2024
HIPAA eManual

HealthFirst
COMPLIANCE SOLUTIONS

10599 v002 11/2023

IMPORTANT MESSAGE

IMPORTANT MESSAGE:
HOW TO ACCESS HIPAA FORMS, REPORTS & TRAINING VIDEO

You will need to follow this link for access to your:

- HIPAA FACILITY CHECKLIST
- HIPAA FORMS
- HIPAA REPORTS
- HIPAA TRAINING VIDEO

https://www.healthfirst.com/ontraq/

Once you are on this link, please follow the SIGN-ON PROMPTS to enter this HIPAA PORTAL

If you have questions or challenges with this, feel free to reach out to us. We are here to help!

HealthFirst
COMPLIANCE SOLUTIONS

Disclaimer

The content is being provided only for educational and informational purposes. HealthFirst attempts to ensure that the content is accurate and obtained from reliable sources, but does not represent that it is error-free.

HealthFirst Compliance Solutions

941.587.2864

2024
HIPAA V-1

EASY-GUIDE

Follow these easy instructions to get the most out of your HIPAA Manual.

Turn to the page listed below & fill-in-the-blanks as explained in the EASY GUIDE instructions:
All forms listed below are accessible via the HIPAA Omnibus Rule Training HIPAA Portal:
https://www.healthfirst.com/ontraq/

Once you are on this link, please follow the SIGN-ON PROMPTS to enter this HIPAA PORTAL

Portal Access Subscription is licensed per location and Digitally Trace Protected to this location only.
If you have additional locations, please sign-up for this HIPAA Annual Update Program at each of your locations

SEE FRONT POCKET	**FAQs on HIPAA & TELEHEALTH DURING PANDEMICS** *Check with your State Regulations regarding Telehealth Rules within your Healthcare Sector.*
Pg 5	**HIPAA COMPLIANCE OFFICER & ADVISORS LISTING** Fill-in-the-Blanks with your: • Facility Name & Address • Name & list a ***HIPAA Compliance Officer*** • Name & list ***HIPAA Advisors*** (these can be Employees or Business Advisors)
Pg 60	**PT. ACKNOWLEDGMENT FORM OF RECEIPT OF NOPP** Each patient to sign & update (ongoing)
Pg 61	**AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION (PHI) & MEDICAL RECORDS to a THIRD PARTY** To be used as needed for patient record release.
Pg 92 & 93	**FAX — E-MAIL SIGNATURE / Privacy Notice of HIPAA Compliance** This is simply a disclaimer/signature you can add to your e-mails & faxes to signify that you are complying with ***HIPAA Omnibus Rule*** Standards.
Pg 96-d –96-j	**Breach Notice Policy & Procedures** • Use to assess Breaches; Customize with your Office Name
Pg 99	**DATA BACK-UP & CONTINGENCY PLAN PLANNING PROCEDURES** On the lower left hand corner of this page, please fill-in the blanks: • ***Primary Location:*** Your City & State • ***Effective Date of Policy:*** Date that you started doing your daily Data Back-Up (it was required since 2008) • ***Date of Policy Review & Update:*** Today's Date ** Make sure to implement ***Secure E-mail Encryption on outgoing email; Discuss this with your IT Tech***** • ***Maintenance of Software & Computers + Data Services Contact Info:*** **Page 101**
Pg 103	**Our Annual Data Back-up, Contingency & Operations Assessment Report (Master)**
Pg 103-A	**Risk Assessment Vulnerabilities Test/ ePHI in Transit or at Rest Report (SAMPLE)**
Pg 103-B	**Risk Assessment Vulnerability Test/ ePhi In transit or at rest Report (Master)**
Pg 104-109	**RED FLAG LAW (ADA Recommended)** This is a review of Fraud prevention for your employees. Read pages 104-109: Employees sign page 109.
Pg 110-120	**HIPAA HITECH LAW PACKET** • Fill-in pages: 114, 117 & 119 *Have Employees sign* ***HITECH LAW EMPLOYEE TRAINING ACKNOWLEDGMENT***
Pg 121-174	**HIPAA WORKBOOK pg 121-174** Use the HIPAA Workbook to follow along with when watching your HIPAA Employee Training Video annually.
Pg 124-125	**HIPAA OMNIBUS RULE CHECKLIST of REQUIREMENTS:** • Follow the ***HIPAA Omnibus Rule Protocol Checklist:*** • Check-off as you complete each task. • Read the training pages as needed • Familiarize yourself with ***(4) Factor Breach Assessment Sheets*** How to use & submit: pages 159
Pg 146-153	**MASTER COPY of HIPAA LAWS: NOTICE OF PRIVACY PRACTICES** First and last page of this document requires you fill in your: Practice Name, Address and Phone Number to make it official. A copy of this is required to be displayed or for patients to have access to read and view. Keep a copy at your reception desk, on a clipboard or lobby copy, for all new patients to read. Copy and provide to patient when requested. If you have a website, a copy must be posted on your website. An electronic version is available on our HIPAA Omnibus Rule Training CD-ROM & HIPAA Portal.
Pg 154-159	**BAA: HIPAA BUSINESS ASSOCIATE AGREEMENT to OMNIBUS RULE STANDARD** Copy and have all businesses that share your ***Patient Health Information (PHI)*** sign a copy & keep it on file in the section provided at the back of this ***HIPAA Manual.*** You are required to keep a signed copy of this agreement from each ***Business Vendor***. Follow these guidelines when presenting this document to vendors: • Use HIPAA BAA Agreement Log (Page 169) to list your current applicable Vendors. **Businesses that are *REQUIRED*** to sign this agreement: (Data Collection Agencies) • Collection Agencies • IT Tech • Consultants • Data Storage Companies • Telephone, Email and Text Confirmation Services • Dental Software & X-Ray Software • After hours Cleaning Service • Bio-Hazard • N20 • Water • Laundry Service Deliveries **Businesses that are *RECOMMENDED*** to sign this agreement: (They see or use your PHI) • Temporary Employees • After Hours Services • Any Vendor who can view PHI **Businesses that are *EXEMPT*** to sign this agreement: (Considered "course of doing business") • Doctor-to-Doctor • Doctor Referral • Insurance Carriers • Pharmacies • Mail Delivery • Labs
Pg 160 or 161	**HIPAA PATIENT ACKNOWLEDGMENT FORM** This is an updated version of a HIPAA PATIENT ACKNOWLEDGMENT FORM that includes: • Authorization of Records Release to Doctor's Offices, Self or Third Parties • How patient wishes to be addressed by name: first name only, or address formally (Mr, Ms, Mrs.) with last name • Cell phone, text & e-mail permissions for contact • Opt-Out-of-Marketing option for Patients • Third Party Remuneration Statement for commissions to your office on products or services you promote **PHARMACIES have their own ***HIPAA PATIENT ACKNOWLEDGMENT FORM*** **Page 161** ** ** Consent to Release Third Party Form will be used occasionally **Page 162****
Pg 163	**HIPAA AFFORDABLE CARE ACT SECTION 1157** Reference this if you take: Medicare, Medicaid or Healthy Kids funded programs. Post this document on your website, on your clip board or in lobby binder and offer to all patients. **WEB & SOCIAL MEDIA & PHOTO RELEASE FORM**
Pg 169 or 176	**BUSINESS ASSOCIATE CONTACT LOG:** Use for tracking your sending and receiving of BAAs. See Business Associate Agreement (pages 154-159); Send to Vendors for signature; Keep on file in this section.
Pg 170 - 172	**HIPAA EMPLOYEE CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT:** All Employees must read the training section of this manual or view the ***HIPAA Omnibus Rule Training Video.*** After reviewing the training section / video, employees should then ***sign this form***. If you prefer ***individual*** Employee HIPAA Confidentiality & Non-Disclosure Agreement, it is assessable via our HIPAA Portal. ** HIPAA EMPLOYEE REPRIMAND FORM is available **Page 80-81**
Pg 173 or 120	**HIPAA HITECH & RISK ASSESSMENT EMPLOYEE TRAINING AGREEMENT:** • Each Employee to sign. • Each employee to sign annually.
Pg 174	**HIPAA EMPLOYEE TECHNOLOGY USE AGREEMENT:** Print a copy for each employee: Fill-out & sign.
	TEXAS HEALTHCARE FACILITIES: Be sure you have completed **Required HB 300 Training & Certification for more info on TX HB300 Certification go to** www.HB300.net Place completed package in this section.
	ANNUAL EMPLOYEE SIGN-IN SHEETS: • All Employees to sign Page: B & C • Make copy of Page E; Each Employee Fill-out & Sign **ANNUAL REPORTS—GET FROM YOUR IT PROVIDER:** • See Template Page: F & H; Store your IT Customized Reports here.
	HOW TO CREATE A RISK ASSESSMENT WRITTEN REPORT: ***Access via our HIPAA Portal; This is a HIPAA Audit requirement!***

HealthFirst
COMPLIANCE SOLUTIONS

IMPORTANT: HIPAA Employee Documents must be saved for 7 consecutive years.

1. **Add this year's Required Employee Documents.**

2. **Add 6 years prior:** Employee Proof of Training & Confidentiality Forms.

Should you have additional questions, please call our HIPAA coaches at **941-587-2864**

HIPAA Omnibus Rule Standard

HIPAA OMNIBUS RULE as set forth by Office for Civil Rights ("OCR")
of the U.S. Department of Health and Human Services ("HHS")

Promulgated January 17, 2013 by HHS ***Effective March 26, 2013***

HealthFirst
COMPLIANCE SOLUTIONS

HIPAA COMPLIANCE TRAINING INFORMATION

The following information is a tool for your office to use, in following HIPAA Omnibus Rule . A HIPAA Officer should be assigned in your office. All team members need to read the training section for understanding of this information. In the front pocket of this manual you will find a (2) page document: EMPLOYEE CONFIDENTIALITY AGREEMENT with DOCUMENTATION OF EMPLOYEE TRAINING. Please have your employees sign after reading and discussing the training section. This will serve as your proof of training. When new employees join the team, they too, will need to review and sign-off on this material. Keep all of these sheets filed at the back of this manual in the appropriate year section for easy access in case of a HIPAA inspection. This information is current as of March 26, 2013 and reflects all changes to the regulations up to that date.

TEXAS STATE HEALTHCARE PROVIDERS: To ensure compliance with Texas State Mandate HB300 Law, effective from September 2012, it is necessary to obtain the required module separately. You can purchase our Texas HB Packet by calling 941-587-2864.

TABLE OF CONTENTS

HIPAA COMPLIANCE OFFICER & ADVISORY COMMITTEE INFORMATION

HIPAA Compliance Officer & Advisory Committee

Office Name _____

Office Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ Email _____

Our HIPAA Compliance Officer is:

_____

Our HIPAA Compliance Committee / Advisors:

The purpose of this committee is to assist the HIPAA Compliance Officer with decisions, implementation and compliance with the program.

Examples of members can be employees, attorneys and professional consultants.

Advisors Name _____

Is an Affiliate of: (Office Name) _____

❑ Address: Same As Above

Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ Email _____

Advisors Name _____

Is an Affiliate of: (Office Name) _____

❑ Address: Same As Above

Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ Email _____

Advisors Name _____

Is an Affiliate of: (Office Name) _____

❑ Address: Same As Above

Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ Email _____

Our HIPAA Compliance Officer's RESPONSIBILITIES:

THIS PERSON TAKES RESPONSIBILITY & SERVES AS THE FOCAL POINT FOR COMPLIANCE ACTIVITIES WITH REGARD TO PLANNING, IMPLEMENTING, AND MONITORING OUR HIPAA OMNIBUS RULES COMPLIANCE PROGRAM

Compliance to HIPAA Omnibus Rule policies is one of the many responsibilities this person has in our office. Our **Compliance Officer** has authority to direct supervised personnel in our office as to the proper procedures to enable compliance with HIPAA Omnibus Rule policies. Our **Compliance Officer** has direct access to management as well as all of our employees.

Our **Compliance Officer** is responsible for the following:

- ✔ The management, monitoring and implementation of our HIPAA Omnibus Rule Compliance Program.
- ✔ Report to management on a regular basis the progress of implementation of HIPAA laws, while assisting management in establishing methods to improve our practice's efficiency and quality of services and to reduce our vulnerability to possible misuse of PHI.
- ✔ Develop, coordinate, and participate in a multifaceted HIPAA Omnibus Rule Educational Training Program that focuses on the elements of the Compliance Program and seeks to ensure that all employees / management are knowledgeable of, and comply with, pertinent HIPAA Federal and State standards.
- ✔ Ensure that all employees of this facility ***sign Employee Training & Confidentiality Agreements,*** then keep them on file.
- ✔ Ensure that Business Associates (independent contractors and agents) who furnish services to our facility ***sign a Business Associate Agreement,*** and are aware of the requirements of this facility's Compliance Program with respect to HIPAA Omnibus Rule and the protection of PHI. The signed copies of the Business Associate Agreement will remain on file within this HIPAA Manual in the section provided.
- ✔ Assist Financial Management and IT Specialist in coordinating internal compliance reviews and monitor activities, including annual or periodic reviews of this facility. ***Conduct annual / regular interval Data-Back Up and Contingency Policy Review & Update***
- ✔ Investigate and act upon matters related to compliance which will include creating and implementing our Breach Occurrence Reporting Plan. Breaches will be documented on our 4-Factor Assessment Sheets and submitted via web, in accordance with HIPAA Omnibus Rule to: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

- ✔ All breaches of more than "low probability will be documented and reported. A copy will reside within this manual, which will be secured and also within the patient's permanent record.
- ✔ Take corrective action with all employees, providers and sub-providers, business associates and agents and, if appropriate, independent contractors.
- ✔ Develop policies and programs that encourage managers and employees to report suspected improprieties without fear of retaliation.
- ✔ Oversee and carry out all requests for electronic copies of records from patients or other parties to see that the request is carried out in accordance with HIPAA Omnibus Rules.

Our **Compliance Officer** has the authority to review all documents and other information that are relevant to compliance activities. This includes, but is not limited to, patient records, billing records, and records concerning the marketing efforts of our clinic and our clinic's arrangements with other parties. This includes: employees, professionals on staff, business associates, subcontractors, conduits and any other agents. This policy enables the **Compliance Officer** to review contracts and obligations (seeking the advice of our legal counsel, where appropriate) that may contain issues that could violate HIPAA Omnibus Rule provisions and other legal or regulatory requirements.

Compliance Committee RESPONSIBILITIES

THE DOCTOR(S)/OWNER(S), EMPLOYEES AND CERTAIN CHOSEN OUTSIDE COUNSEL TO OUR FACILITY COMPRISE OUR "COMPLIANCE REVIEW COMMITTEE" AND WILL ADVISE THE COMPLIANCE OFFICER AND ASSIST IN THE IMPLEMENTATION OF THE COMPLIANCE PROGRAM.

The Committee's functions include:

- ✔ Analyzing the clinic's industry environment, the legal requirements with which it must comply, and specific risk areas with regards to the HIPAA Omnibus Rule.
- ✔ Assessing existing policies and procedures that address these areas for possible incorporation into the Compliance Program.
- ✔ Working with appropriate employees to develop standards of conduct and policies and procedures to promote compliance with our clinic's program.
- ✔ Recommending and monitoring the development of internal systems and controls to carry out the organization's standards, policies, and procedures as part of its daily operations.
- ✔ Determining the appropriate strategy/approach to promote compliance with the program and detection of any potential violations, such as through hotlines and other fraud reporting mechanisms.
- ✔ Developing a system to solicit, evaluate and respond to complaints and problems.
- ✔ Promote proper HIPAA Omnibus compliance and execution of all protocols, including Breach Reporting Protocols.

Our Health Insurance Portability and Accountability Act (HIPAA) Omnibus Rule Compliance Manual

A plan to help our employees comply with the Final HIPAA Omnibus Rule of 2013

Warning: We are serious about following HIPAA rules. Not only because of our desire to comply in order to help patients and the industry, but also because HIPAA calls for severe civil and criminal penalties for noncompliance, including:

Civil monetary penalties

Tier	Penalty
1. Covered entity or individual did not know (and by exercising reasonable diligence would not have known) the act was a HIPAA violation.	$100-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
2. The HIPAA violation had a reasonable cause and was not due to willful neglect.	$1,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
3. The HIPAA violation was due to willful neglect but the violation was corrected within the required time period.	$10,000-$50,000 for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year
4. The HIPAA violation was due to willful neglect and was not corrected.	$50,000 or more for each violation, up to a maximum of $1.5 million for identical provisions during a calendar year

Criminal penalties

Tier	Potential jail sentence
Unknowingly or with reasonable cause	Up to one year
Under false pretenses	Up to five years
For personal gain or malicious reasons	Up to ten years

OUR 5 BASIC HIPAA GOALS

The purpose of this manual is to teach our employees skills that will help them to comply with the Health Insurance Portability and Accountability Act ("HIPAA") and the Privacy Rules and Security Rules issued thereunder. In 2013, the HIPAA Privacy Rules and Security Rules were substantially revised. Those revised rules are known as the "HIPAA Omnibus Rule." The name "Health Insurance Portability and Accountability Act" (HIPAA) does not completely describe what this act is about. In this manual we will try to simplify the key elements of HIPAA. Congress has stated that the goal of HIPAA is to improve the efficiency and effectiveness of the health care system in the United States. To date, HIPAA Omnibus Rule is designed to secure through a far reaching matrix, patient protected health information (PHI).

While there are many facets of HIPAA, in reality all elements of the HIPAA Law revolve around five key sets of standards that will affect our facility. **In summary, here is our program for HIPAA Omnibus Rule Compliance:**

1. *We strive to comply with HIPAA Omnibus Rule guidelines by learning to protect* ***our patient's healthcare privacy and PHI.***

2. *We strive to comply with HIPAA Omnibus Rule guidelines by appropriately* ***maintaining our patient health information (PHI), billing, computer and internet processes, and electronic devices in compliance with national standards.***

3. *We strive to comply with HIPAA Omnibus Rule guidelines by* ***providing appropriate security of our patient PHI records.***

4. *We strive to* ***have every employee understand current, proper protocols and act in accordance with*** *the HIPAA Omnibus Rule whether on or off duty.*

5. *We strive to* ***only affiliate with Business Associates that will comply and uphold*** *these same HIPAA Omnibus Rule,* ***or we shall seek more highly HIPAA educated and compliant Business Associates.***

These five principles are the heart and soul of HIPAA for our practice. If you as an employee will keep these goals in mind as you carry out your duties, we will progressively achieve compliance with the HIPAA Act.

HIPAA OMNIBUS EMPLOYEE TRAINING PROGRAM

A. DEFINITIONS: Terms To Know

In order to make sense of the HIPAA rules, first a few definitions are in order. In the sense that they are used in the HIPAA regulations, privacy and security are closely linked, so it's important for you to understand the difference.

PRIVACY: The Department of Health and Human Services describes privacy as **the patient's right over the use and disclosure of his or her own protected health information.** Privacy includes the right to determine when, how and to what extent protected information is shared with others. During the course of your job, except in connection with patient treatment, always use the "minimum necessary" of the patients' health information, to complete your job. After work hours, do not talk about or communicate electronically about a patient's health information. Do not use their name when speaking about them with regards to their health. You may be social with a patient, but never use their protected health information for personal gain. Keep patient information private. Use it at bare minimum. It is your professional obligation.

The HIPAA Omnibus Rule grants new rights to patients to gain access, and control the use and disclosure of their protected health information. There are many reasons this new need for privacy has come about. Please read the Office Policies Section of this manual and the full details of the Omnibus Rule.

SECURITY: Security refers to the **specific measures a Covered Entity must take to *secure* protected health information (PHI) from unauthorized breaches of privacy,** such as might occur if information is stolen or sent to the wrong person in error. Security also includes measures taken to ensure against the loss of integrity of protected health information (PHI), such as might occur if patient's records are lost or destroyed by accident. HIPAA Omnibus Rule requires general security measures to be put in place. You will learn in the Omnibus Rule Training Section that a 4-factor Assessment must be documented, submitted and kept on file for all breaches not determined to be of "low probable risk."

So as you can see security and privacy are closely related, but we treat them separately. You shall discover by studying this manual that we must keep our records not only secure, but private.

Protected Health Information — PHI

This is a key HIPAA term: **Protected Health Information (PHI)**
It is a common misconception, to think that the ideas of security and privacy apply only to a written document. Throughout this manual, **keep in mind that what you *say* to another person (regarding a patient) needs to be just as protected as what you *write* or *send electronically*.**

This is one acronym worth memorizing: **PHI:** Protected Health Information: any identifiable information which relates to an individual's past, present or future physical or mental health or condition for which there is a reasonable cause to believe it can be used to identify that individual*.

There are 18 Protected Health Identifiers common to business or professional use. These would include:

1. Name
2. Zip Code
3. Birth Date
4. Telephone Number
5. Fax Number
6. Account Number
7. Email Address
8. Social Security Number
9. Medical Record Number
10. Health Plan Number
11. Certificate/license numbers
12. Vehicle Identifiers & Serial Numbers (including license plate numbers)
13. Device Identifiers & Serial Numbers
14. Web Universal Resource Locator (URL)
15. Internet Protocol (IP) Address Number
16. Biometric identifiers (including finger or voice prints)
17. Full-Face Photographic Images (and any Identity Bearing Images)
18. Any other unique identifying number, characteristic or code

***(45 CFR Sec. 164.514 — Code of Federal Regulations)**

EHR Electronic Health Records: patient records that can be transmitted or copied and shared by electronic means: digital, fax, text, phone transmission or via internet.
ePHI: PHI that is stored, maintained or transmitted electronically. This would include fax, phone, text or emails. Similar to EHR but more specifically PHI. (See the 18 Protected Health identifiers listed above).
COVERED ENTITY: under the HIPAA Privacy Rule a Covered Entity refers to three specific groups, including: Health Plans, Health Care Clearinghouses, and Health Care Providers that transmit health information electronically. Here are some examples of Covered Entities:

Healthcare Providers
Doctors
Clinics
Psychologists
Dentists
Chiropractors
Nursing Homs Pharmacies

Health Plans
Medical, Dental, and Vision Plans
HMOs
Medicare and Medicaid
Long Term Care
Veteran Plan

Health Care Clearinghouses
Billing Services
Re-pricing Companies
Community Health Managers
Value Added Networks

See this link for more details:
http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/entityhipaa.html

BUSINESS ASSOCIATE: An entity or person (non-employee) that performs a service for or on behalf of a Covered Entity and in the course of their work will directly / indirectly create, receive, maintain or transmit PHI on behalf of the Covered Entity. The following are some examples of Business Associates under the Omnibus Rule:

Required: (Data Collection Agencies)

- Confirmation Service
- Consultants
- IT Tech
- Data Storage Company

Recommended: (to be safe)

- Temp Employees / Volunteers / Students
- After Hours Services
- Email & Fax Encryption Services
- Dental Suppliers & Dental Repair Services
- Data Back Up Providers
- Landlords
- Other Vendors

The following are examples of persons/entities who are not typically Business Associates:

- Other Doctors
- Doctor Referrals
- Pharmacy
- Insurance Company
- Conduit: UPS Fed Ex USPS
- Dental Labs

Considered Course-of-Doing-Business: Sharing PHI is necessary for patient treatment PHI sharing is to a "minimum necessary" **The Office of Civil Rights declined to specifically define a "Health Information Organization" because this scope of business is still evolving; An entity that does not require access to PHI is not included. These are considered conduits.

It is considered the course-of-doing-business, if the sharing is necessary for patient treatment, and then the PHI sharing is to be of "minimum necessary" rule, when general or specific treatment requires it.

CONDUIT: An entity who temporarily stores PHI either in paper or electronic format or who provides the means of transmission. Conduits are not required to sign Business Associate Agreements.

- EXAMPLE: Mail Courier, Postman, Internet Service Provider ("ISP").

SUB CONTRACTOR: Any entity that contracts with a Business Associate to carry out additional work for the Business Associate involving a Covered Entity's PHI. A signed Business Associate Agreement must be in place between the Business Associate and its Subcontractor to safeguard confidentiality from the subcontractor regarding all PHI handled, processed or viewed. The Business Associate keeps these documents on file for easiest access within their HIPAA Manual.

- EXAMPLE: Doctor hires a Medical / Dental Software Company; That Software Company sub-contracts with a text & e-mail confirmation service.

OCR: The Office for Civil Rights
HHS: The U.S. Department of Health and Human Services

EXAMPLES OF PENALTIES

- Did not know of violation:
  Formerly, $100-$50,000 per violation. Now under Omnibus Rule $50K - $1.5M
- Violator has reasonable cause to know that a violation might occur:
  $1000-$50,000 to a maximum of $1.5 million per year
- Willful neglect in avoiding or responding to violations, if corrected in 30 days:
  $10,000-$50,000 to a maximum $1.5 million per year
- Willful neglect in avoiding or responding to violations without correction:
  $50,000 to a maximum of $1.5 million

B. Introduction To HIPAA: Early History

In 1996, Congress enacted HIPAA which stands for: Health Insurance Portability and Accountability Act, and was originally designed as a means to make health insurance "portable". For instance, if an individual were to move, they could take their existing health insurance policy with them. Limits on how much an insurance company could raise premiums in these situations were also governed and capped. For most Covered Entities, compliance was required by Oct. 16, 2002, for the electronic transaction rule and by April 14, 2003, for the health information privacy rules. We have been abiding by HIPAA rules for a long while.

The original HIPAA ACT also included a series of "administrative simplification" provisions that required the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions. This was about the time offices were beginning to use electronic claims, the internet and email. Uniformity and simplicity needed to be established with regards to patient health information, especially as it was being used over the internet waves.

The intent was to ensure consistency throughout the healthcare industry. It was thought that these national standards would make it easier for health plans, doctors, hospitals, and other health care providers to process claims and other transactions electronically. This consistency was needed due to the countless variations in the way health care companies and individuals processed patient records, claims, services, etc. It was particularly important because the electronic processing age was coming to life.

HIPAA was also created to require security and privacy standards, to secure an individual's protected health information (PHI). HHS issued regulations, with this in mind. The following is a list of those rules and their status as of the fourth quarter 2001:

- Electronic health care transactions (final rule issued);
- Healthcare privacy (final rule issued);
- Security requirements (proposed rule issued; final rule in development);
- Unique identifier for employers (proposed rule issued; final rule in development);
- Unique identifier for providers (proposed rule issued; final rule in development);
- Unique identifier for health plans (proposed rule in development);
- Enforcement procedures (proposed rule in development).

As you can see, many of the HIPAA rules were still evolving. The rules continued to change as the government got feedback from the industry. One of the main objectives of the privacy rules is to help ensure fair and equal health care. Privacy will help everyone attain fair insurance coverage and to avoid discrimination in other areas of our lives. In addition, protecting the privacy of patient health records is an ethical obligation for two reasons: because of the delicate private nature of many disease states, and because patient health identifiers can lead to identify fraud which now plagues this country.

With the implementation of uniform guidelines, congressional researchers concluded that billions of dollars will be saved each year for health care businesses by lowering the costs of developing and maintaining software and reducing the time and expense needed to handle health care transactions. This sounded reasonable, but as time and technology change, HIPAA laws may evolve to become more robust and may actually demand the development or additional software, manpower, money investment and time. Still, we will comply.

C. HIPAA Time Line: Early History 1996-2013

1996—HIPAA is Enacted...

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996 by Congress to protect individual's Right to Privacy about their health. At the time of its passage the information technology boom that occurred in the United States in the late 1990's was just beginning to take hold and it was apparent that the availability of medical information about individuals would increase dramatically in just a short period of time. The importance of legislation to ensure that this trend would not allow any intrusion on the privacy rights of individuals was not lost on Congressional leaders, and thus the protections of HIPAA were set out to allow the information age to transform the health care industry in the most positive way possible.

2003—Privacy Rule-Small Health Providers...

The HIPAA Privacy Rule enactment starting on April 14, 2003 was the most influential step in HIPAA and in the protection of health information privacy rights ever undertaken in this country. Healthcare providers now were required to comply with keeping patient medical information private, and the term "covered entity" was developed to ensure that Protected Health Information (PHI), or any health information that identified an individual within the setting of a treatment facility, was only used for treatment, payment or administrative purposes within a healthcare office. Healthcare offices such as healthcare practices were required to provide paperwork acknowledging those rights and have patients sign forms indicating they understood the details of both a practice's use of PHI and a patient's right to access that information. On October 17, 2003 the Transactions and Code Sets Standards were issued to cover any medical information written, spoken or in electronic form.

2005—Security Rule—Healthcare Offices Subject to Rule Concerning Electronic Information Transfers...

The HIPAA Security Rule enacted on April 21, 2005 was oriented exclusively around the electronic maintenance, storage and transfer of PHI. The Security Rule goes beyond the Privacy Rule in its protection against any reasonably anticipated threats or hazards in the security or integrity of the information that was defined to be protected under the Privacy Rule. Healthcare offices needed to be conscientious of keeping private any medical or identifying information from accessibility by those not necessarily needing that information to continue proper treatment and administration of healthcare offices.

2009—Greater HIPAA Enforcement...

After the election of President Barack Obama in 2008, the American Recovery and Reinvestment Act of 2009 (ARRA) had in it significant provisions for the increased enforcement of both the Privacy Rule and the Security Rule. Most of the important changes to HIPAA are contained in the "HITECH ACT" which is Title XIII of the ARRA, which became law on February 17, 2009. Breaches of confidentiality of information, how to avoid them and how to handle them once detected, has become the primary focus of the HITECH rules. The fast and furious nature of the changes has become evident since that time.

2010—Red Flag Rules

The Federal Trade Commission became involved in the evolution of privacy law as it affects healthcare providers in the enactment of the so called "Red Flag Rules," which were designed as an anti-fraud set of regulations for creditors to recognize and detect the possibility of identity theft among their patients. A great number of scenarios and signs or red flags that such theft might be occurring were laid out by the FTC and now must be recognized by all office staff of health care providers that allow patients to pay not just up front for services but over time or with payments by third parties. This law,

as of now, has not passed as federal standard though it is highly recommended that every healthcare facility have an anti-fraud policy in place to avoid monetary loss.

2011—HITECH LAW

Written and required federal laws for all healthcare offices. HITECH mandates that Covered Entities have written protocol in place regarding their practices with integrating PHI with high technology. Internet interface with routers and firewalls, telephone messaging security, internal computer termi-nal password protection and paper shredding are among the mandates. All employees have to sign a training document stating that they understand that they can be held personally responsible for any malicious conduct either verbally or posted on the internet / electronically. (See HITECH LAW PACKET in the Office Policies Section of this manual for more information).

2012—TEXAS State adds House Bill 300 Law

Governor Rick Perry of Texas mandates a bill for all healthcare facilities to follow stricter handling of PHI & EHR within the healthcare workplace. Employee training is required and must be updated bi-annually. Fines and violations are intense for non–compliance.

2013—Omnibus Rule "The Final Rule"

Omnibus Rule is a 563-page revision to existing HIPAA law that updates and changes many aspects of how we handled PHI, Patient requests for PHI, Marketing and Product/Service dispensing or refer-ring. Omnibus Rule creates a further reaching matrix to protect PHI. This will include holding Busi-ness Associates responsible for confidentiality of PHI use and disclosures to their Subcontractors, plus accountability to report breaches of PHI. All entities will follow a 4-Factor Assessment Protocol to evaluate potential breaches of PHI. Documentation and reporting protocols must be established within the business dwelling. Other Patient Notifications are included in Omnibus Rule, they include but are not limited to:

- The Use and Disclosure of PHI in Marketing & Fundraising
- "Opt Out" Options for these communications for the patient
- Third Party Disclosure Regulations, Selling Products & Services to Patients
- Insurance Notifications for "Out of pocket / Paid in Full" treatment
- Many other protocols.

Read your Omnibus Rule Packet in the Office Policies Section of this manual for full details.

2020—COVID Privacy Updates

Because COVID-19 is a public health threat, employers generally have more discretion on obtaining health information that is usually be limited under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Americans with Disabilities Act (ADA) and other privacy laws (JD Supra, 2020). Labor and employment law experts confirm that employers can legally ask employees for this information. Although HIPAA laws do not apply to most employers, there are privacy requirements regarding employees' health information under the Americans with Disabilities Act (ADA). The EEOC has confirmed that the ADA bans employers from discriminating against employees based on a medical condition, including COVID-19 (2020). The ADA also protects workers by requiring employers to keep the identities of employees who have symptoms, have tested positive for COVID-19 & vaccination status, confidential.

Tele-Health also became popular during COVID-19. Practitioners need to check with their State Board for restrictions and/or guidelines for conducting Tele-Health sessions.

D. HIPAA Omnibus Basic Guidelines & Protocols

As a result of our free market health care system in the United States, health plans, hospitals, pharmacies, doctors, and other health care entities (as all of which are Covered Entities) use a wide array of systems to process and track health care bills and other information. Hospitals and doctor's offices that treat patients with many different types of health insurance understand the vast time and money that is spent ensuring that each claim contains the format, codes and other details required by each insurer. Similarly, health plans spend time and money to ensure their systems can handle transactions from various health care providers, employers and other businesses or entities.

One goal of HIPAA is to provide a wide array of provisions designed to make health insurance more affordable and accessible. With support from health plans, hospitals and other health care businesses, Congress included provisions in HIPAA to require HHS to adopt national standards for certain electronic health care transactions and security.

With the internet age, a newer goal of HIPAA's Omnibus Rule is to create an even further reaching arm to protect our patients' PHI. Now Business Associates will have to sign confidentiality agreements called Business Associates Agreements that will hold them accountable to secure our patients' PHI in the same manner and to the same Federal Standard that we do. (See Omnibus Rule Office Policy for full details in the back of this manual). Similarly, Business Associates will have to have any of their Subcontractors sign Business Associate Agreements for continuity of confidentiality. This manual will clarify our facilities policies in accordance with HIPAA's 2013 Omnibus Rule, combined with all previous volumes of HIPAA Law that apply.

Although at times it may seem tedious for our office to comply with these guidelines, in the long run our interactions with other health care entities / Covered Entities, insurance providers, etc., will benefit from this standardization. Omnibus Rule brings with it many more regulations, but also many obscure definitions. It seems these new guidelines will be more of a means to collect data, especially regarding breaches, the types that occur over time, etc. Then, HIPAA will again change and redefine the HIPAA guidelines to better serve patient protection and uniformity in security efforts. **While HIPAA, may always remain in a "state of flux", because of evolving technology, changes in data set needs and demands of individuals, one thing will remain solid: it's the commitment to HIPAA compliance within our office to show a professional and dedicated effort in valuing security and confidentiality.**

NEW LIMITATIONS FOR MARKETING, FUND RAISING & RESEARCH WITH PHI

Marketing is defined as "a communication about a product or service that encourages the recipient to purchase / use the product or service." In day-to-day practice, we may recommend alternative therapy or products. Going forward we will get patient consent on our ***HIPAA PATIENT ACKNOWLEDGEMENT FORM,*** to inform the patient of possible rebates, remuneration or commissions that we may receive in relation of such endorsements. Recommending products or services (from a third party), for which we, (the covered entity), receives remuneration, must first obtain authorization to use PHI (from the patient) to make any treatment and health care recommendations. This would include: commissions paid to employees on dispensed products. The patient now needs to be aware if commissions exist.

This is acknowledged on our HIPAA Patient Acknowledgement form in the following manner:

> "In signing this **HIPAA Patient Acknowledgement Form,** you acknowledge and authorize, that this office may recommend products or services to promote your improved health. This office may or may not receive third party remuneration from these affiliated companies. We, under current HIPAA Omnibus Rule, provide you this information with your knowledge and consent."

Similarly, our Business Associates who receive remuneration need to get patient authorization, even if we, the covered entity, get no direct remuneration.

There are (4) other important limitations now under Omnibus Rule that may affect us, they are:

1. ***Refill Reminders*** are excluded. Other things considered "Refill Reminders" are:
   - Communications about Generic Equivalents
   - Adherence to Take Medication as Directed
   - Self-Administered Drugs / Biologics, Delivery Systems (i.e. insulin pump)
2. ***Face-to-Face Marketing*** these communications are not subject to the authorization requirement. (i.e.: handing a patient a pamphlet or brochure)
3. ***Promotional Gifts of Nominal Value*** are not subject to the authorization requirement.
4. ***In-Kind Payments*** or payments to implement a disease management program are permissible.

New Fund Raising Rules regarding PHI

Fundraising Rules under Omnibus can be used without the patient having to authorize and know these factors about the fund raising efforts:

- Department of service information
  (the particular department of your facility that is participating)
- Identity of the particular physician
- Health insurance status

We still will note fundraising protocols in their ***Notice of Privacy Practices.*** Patients must be given the oppor-tunity to "opt-out" of receiving future fundraising communications in the ***NOPP.*** You must not be influenced to treat or not treat a patient based on their decision to participate or be included in your fundraising efforts. We have provided this "opt-out" function in both our ***Omnibus Rule NOPP*** and ***HIPAA Patient Acknowledgement*** forms.

Regulations on the Use of PHI in Research

Omnibus Rule changes (2) components with regards to "authorizations for the use or disclosure of PHI for research":

1. ***HHS*** before did not want to authorize use of PHI for ***future*** research, without another authorization being issued, at that later time. Now HHS will consider these valid, if they adequately describe the future uses.
2. Compound authorizations for research have been changed. When used, compound authorizations, must differentiate between conditioned and unconditioned components.

We will consult an attorney specializing in this area of law if we are going to participate in research with PHI to ensure we participate in accordance with HIPAA Omnibus Rules.

SELLING OF PHI UNDER OMNIBUS RULE

Selling PHI without authorization is strictly prohibited. There are some exceptions where remuneration for PHI is allowed under Omnibus Rule, they are for the sale, transfer, merger, or consolidation of all or part of a covered entity/ healthcare facility.

Be cautious with selling PHI even under the above circumstances. **HealthFirst** suggests that you consult with an attorney before doing so, to ensure you are keeping with the Omnibus Rule prescribed standards. We have listed the above as stated in the Omnibus Rules, but will not attempt to advise you on this topic.

Disclosure of PHI for research purposes will not be considered a "sale" if there is only a reasonable PHI transmission fee as payment received. If you, the covered entity, is to sell PHI, an authorization must state remuneration will result.

SOCIAL MEDIA AND HIPAA

Use of social media in the workplace (FaceBook™, Instagram™, Twitter™, etc.) have restrictions under both Omnibus Rule and HITECH Law, especially regarding the posting of patient or employee information. **Employees are held directly responsible for any malicious posting on social networks with civil and criminal penalties including jail time.** Proper security of private employee records and conduct needs to be taken seriously.

A new area of law will emerge as internet/ electronic patient information sharing grows and as professional conduct challenges emerge. While the posting of PHI of patients is strictly prohibited, there is no concise HIPAA rule, regarding the posting of "work related issues" which would include venting or complaining about a workplace.

Healthcare facilities currently are spending thousands of dollars on building social media following and on optimizing their rankings in web space. Just as the physical office has value and can be defaced, so can a health care facility's reputation in web space. When a facility receives negative perfor-mance reviews on social media sites or through other electronic venues, that is malicious in intent, many are seeking legal support and suing for damages. Please be cautious with what you post on social media sites. If our facility suspects slanderous or inappropriate behaviors, we will seek and pursue legal action to the fullest end.

E. Patient Billing And Payments

In order to understand HIPAA as it pertains to patient payments, we first must give the HHS definition of payment. **"Payment"** is a defined term that encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and for a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care. In addition to the general definition, other adjunctive payment examples include, but are not limited to:

- Determining eligibility or coverage under a plan and adjudicating claims
- Risk adjustments
- Billing and collection activities
- Reviewing health care services for healthcare necessity, coverage, justification of charges, and the like
- Utilization review activities
- Disclosures to consumer reporting agencies (limited to specified identifying information about the individual, his or her payment history, and identifying information about the covered entity)

Our practice may use and disclose PHI for payment purposes. We do not need to obtain the patient's authorization to use and disclose PHI for Payment purposes. Payment transactions should always be conducted in a private setting.

Consumer Credit Reporting Agencies

The earlier HIPAA Privacy Rule definition of "payment" includes disclosures to consumer reporting agencies. These disclosures, however, are limited to the following PHI about the individual: name and address, date of birth, social security number, payment history, and account number.

In addition, disclosure of the name and address of the health care provider or health plan making the report is allowed. We can report payment activity directly or we may carry out this function through a third party, such as a collection agency. Note that if the collection agency has access to PHI, we need to enter into a Business Associate Agreement with the collection agency.

Debt Collection Agencies

Our practice may use the services of debt collection agencies. Debt collection is recognized as a payment activity within the "payment" definition. Disclosures of minimum necessary amounts of PHI to collection agencies under a business associate agreement are permitted.

Location information services of collection agencies and the Fair Debt Collection Practices Act

As described above, "payment" is broadly defined as activities by health plans or health care providers to obtain premiums or obtain or provide reimbursements for the provision of health care. The activities specified are by way of example and are not intended to be an exclusive listing. Billing, claims management, collection activities and related data processing are expressly included in the definition of "payment".

HHS has stated that obtaining information about the location of the individual is a routine activity to facilitate the collection of amounts owed and the management of accounts receivable. Therefore, would constitute a payment activity. We would still have to comply with any limitations placed on location information services by the Fair Debt Collection Practices Act.

F. Understanding Our HIPAA Program—An Overview

To comply with the Department of Health and Human Services **(HHS)** HIPAA Omnibus Rule requirements this facility will **provide each new member of our workforce: HIPAA training, HIPAA Updated Training as needed and required by law, Proof of Training & Confidentiality Agreements signed and on-file, A copy of our Notice of Privacy Practices, Review of our Patient HIPAA Acknowledgement form (plus others), Review of HITECH LAW, Our Data Back-Up & Contingency Plan, Omnibus Rules, Breach Reporting Protocols, Our Marketing & Fundraising Policies, Our Product & Services re-selling guidelines, our Patient Contact and Guardian Allow-ances Policies and various other policies and protocols included within the pages of this Manual.** For ease in training, we may provide training through live instruction, video presentations, or interactive software programs.

SUMMARY OF THE HIPAA OMNIBUS RULE

1. It establishes appropriate requirements that Covered Entities must achieve to secure the privacy of protected health information.
2. It holds violators accountable, with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
3. It requires that all employees understand what Major & Minor breaches are and how to respond to them.
4. It measures with a 4-Factor Assessment Plan when a compromise may be considered a breach.
5. It provides a Breach Reporting Headquarters in the US Dept. of Health & Human Services.
6. It strikes a balance when public responsibility requires disclosure of some forms of data – for example, to protect public health.
7. For patients — it means being able to make informed choices when seeking care and reimbursement for care based on how protected health information may be used.
8. It enables patients to find out how their information may be used and what disclosures of their information have been made.
9. It generally limits release of information to the "minimum necessary needed" for the purpose of the disclosure.
10. It gives patients the right to examine and obtain a copy of their own health records and request copies electronically, in a format they desire or one that is available.
11. It provides access to PHI electronic records upon written request within 30 days of receipt.
12. It allows Third Party access to PHI with written request to include: Who receives the PHI, When(Date received request) and Where it will go.
13. It has marketing and fundraising protection to involve PHI. Patients must be offered an "opt out" option for fund raising and this will not be held against them in relation to their treatment.
14. It now allows patients to "pay out of pocket in full" and secure their PHI from insurance plan reporting.
15. It demands attention, focus and respect by all employees and health professionals.
16. It demands that the facility owner keep up on HIPAA changes and updates, to ensure the privacy and security of all PHI.

Our goal in reviewing and updating our privacy standards centers on these components of the final rule. In all that we do in connection with patient records, we should keep in mind the above principles.

G. Our Communication of Privacy & Patient Consent

Prior to HIPAA, many health care providers, for professional or ethical reasons, would routinely obtain a patient's consent for disclosure of information to insurance companies or for other purposes. The HIPAA Privacy Rule expressly allows Covered Entities to use and disclose protected information to carry out **Treatment, Payment, or Health Care Operations. (Hereafter called TPO).**

Under Omnibus Rule, communication permissions that now are directly permissible are: Appointment Reminders, Treatment Information, Benefit Notifications. These are considered the course-of-doing-business.

COMMNUICATION of HIPAA RIGHTS

The HIPAA Privacy Rule establishes a federal requirement that Covered Entities provide their patients with a written description of how they will use and disclose their patients' protected health information. This is why we have new patients sign a **HIPAA PATIENT ACKNOWLEDGEMENT FORM.**

As technology and communication sharing change, we will have all patients sign updated more current **HIPAA Omnibus Rule PATIENT ACKNOWLEDGEMENT FORMS.** With the birth of Omnibus Rule, what results is an overhaul of our current Patient Forms and Confidentiality Agreements. In essence, everyone will re-sign a new HIPAA Omnibus Rule form: Patients will sign the Acknowledgement to the new Omnibus Changes. They will also have access to the new **Omnibus Rule Notice of Privacy Practices** within our facility and on our website (if one is operational). Employees (you) will sign new **Confidentiality Agreements** to the Omnibus Rule standards, and Business Associates and their subcontractors will sign new Business Associate Agreements.

PERMISSABLE COMMUNICATION OF PHI FOR TREATMENT PURPOSES

- Doctors (related to the patient's care or permitted by the patient, including referrals)
- Pharmacy Health Insurance Plans
- Conduit (Postal carrier)

PERMISSABLE COMMUNICATION OF PHI FOR BUSINESS FUNCTIONS

- Appointment Reminders (Patients confirm what type of reminders they prefer)
- Payment for Services
- Business Operations
- Necessary Information for Insurance Providers
- Staff and Service Assessments

WRITTEN COMMUNICATION OF PHI NEEDED FOR:

- Communication of PHI to Family or Others (Emergency, Authority & Communication Barrier Exception)
- Disclosure of PHI to Third Party
- Marketing & Fund Raising / Opt Out Clause
- Product of Services Reimbursement to this Facility Notification

COMMUNICATION OF PHI TO AUTHORITIES OR IN AN EMERGENCY

- In case of incapacity or emergency; Use best professional judgment
- To comply with a court-ordered warrant, or summons
- Healthcare Offices allowance upon detailed written requests from a government agency
- In cases of possible victim of abuse or crimes for the safety and well-being of others

DENIAL OF ACCESS OF PHI

- Access to PHI should be denied if the request is not in writing
- Amendments to medical record not included
- Third Party requests must include in writing and on our HIPAA compliant Authorization Form: Full Name, Date and where to send

SIGN-IN SHEETS

HHS did not intend the Privacy Rule to prohibit the use of a sign-in sheet in doctors' offices. The previous Privacy Rule was ambiguous about this common practice. We will securely conceal our sign in sheet directly after any sign-in and before any patient can view the sheet. If we use sign-in sheets we will only use the type that stay within the permissible guidelines of Omnibus Rule to shield and secure sign-in information.

Here are several key components of our Communication Policies:

1. Patient consent is not required before a covered health care provider that has a direct treatment relationship with the patient may use or disclose protected health information (PHI) for purposes of TPO.
2. Uses and disclosures for TPO may be permitted without prior consent in an emergency, when a provider is required by law to treat the individual, or when there are substantial communication barriers.
3. Health care providers that have indirect treatment relationships with patients (such as laboratories that only interact with doctors and not patients), health plans, and health care clearinghouses may use and disclose PHI for purposes of TPO without obtaining a patient's consent.
4. Our Authorization Form will be written in comprehensible terms to follow HHS guidelines, which will include: how the individual's PHI may be used and disclosed for purposes other than TPO, state the patient's rights to review the provider's privacy notice, to request restrictions and to revoke consent, to request other guardian access, to inform of marketing and fundraising practices, to offer an "opt out" opportunity from such practices, to reveal this facilities involvement in accepting remuneration for health products or services in relation to the individuals care, and be dated and signed by the individual (or his or her representative).
5. Under Omnibus Rule, communication permissions that now are directly permissible are: **Appointment Reminders, Treatment Information, Benefit Notifications.** These are considered Course-of-Doing-Business.

Our patients have individual rights as they pertain to our use and disclosure of their PHI for purposes other than TPO:

- Any of our patients may revoke an Authorization in writing.
- If the patient has previously given Authorization, the patient may not revoke actions that have already taken place which relied on a previously signed Authorization.

- If at some time a patient revokes Authorization in writing, this information should be put in the patient's file attached permanently to the previous Authorization form(s).
- Any patient may request restrictions on uses or disclosures of health information.
- Our practice is not required to agree to the restriction requested, but we are bound by any restriction to which we agree.
- Any such restrictions should be discussed with the HIPAA Compliance Officer and prominently displayed in the patient's files.
- All of our patients must be given a notice of our privacy practices and they should be asked to sign an acknowledgment of receipt.
- All of our patients will receive an "opt out" of marketing and fundraising opportunity.
- All of our patients will be made aware of this facility's practices for accepting remuneration for health products or services in relation to their health care.
- All of our patients will be made aware that they can now "pay out of pocket in full" and request non-disclosure to their insurance carrier.
- All of our patients will be made aware this may or may not influence the insurance carrier's propensity to pay related claims in the future.
- All of our patients will be asked to list by full name and relation, any guardians or other persons who are participating in the patient's care who are allowed to have access to their PHI.

How long do we need to keep patient Authorization forms and Acknowledgment of Receipt of our Notice of Privacy Practices?

We will retain on-file for current patients any written Authorizations as well as signed Acknowledgment of their Receipt of our Notice of Privacy Practices. And signed. We will keep these on file, as law requires, within their patient records. We will retain these records for at least six (6) years.

If you have any questions about time spans for retaining or storing of patient consent forms, contact our HIPAA Compliance Officer.

H. New Additions To Notice Of Privacy Practices

There are some specific changes in the new Omnibus Rule regarding what is required to include or exclude in our offices' **Notices of Privacy Practices (NOPPs)** and how to communicate these to our patients. A newly revised copy of the **Notices of Privacy Practices (NOPPs)** is included in our OMNIBUS RULE PACKET in the Office Policies Section of this manual. Here are the requirements we follow:

- We display this new ***NOPP*** in our facility to make it available for our patients to read.
- We will provide a hard copy to patients should they ask for one.
- We also post this new ***NOPP*** on our website (if functional).

Within this new NOPP, we include:

1. Acknowledgement that the sale of PHI is prohibited.
2. Acknowledgement that the use of PHI in marketing or fundraising is prohibited except with prior authorization or consent from our patients.
3. Our patients have a right to "opt out" of receiving fundraising communications.
4. A statement if you plan to use PHI in marketing or fundraising.
5. An acknowledgement that patients can restrict disclosures to their insurance health plan for services of which they will pay "out of pocket" and in full.

Below are the additional revisions that we include:

Health Insurance plans that underwrite must state in their NOPP that the plan cannot use or disclose genetic information for underwriting purposes (this excludes certain long-term care plans). Health plans that post their NOPPs on their Web sites must post Omnibus Rule changes on their sites by the effective date of Omnibus Rule, as well as by US Mail. Plans that do not post their NOPPs on their Web sites must provide information about Omnibus Rule changes within 60 days of the revision to their clients.
Psychotherapy Notes maintained by a Covered Entity, must state in their NOPPs that "use and disclosure" of such notes require the patient's authorization.
New exclusion / Appointment Reminders, Treatment Info or Health Benefits Notice is ***no longer required***. Omnibus Rule considers this "the course of doing business".

I. Oral Communications

BASIC RULES FOR ORAL COMMUNICATIONS REGARDING PHI

We are required to **reasonably safeguard** protected health information (PHI) — including oral information — from any intentional or unintentional use or disclosure that is in violation of HIPAA Law. The rules of oral communication basically are the same as those of written communication.

We should always use the minimum necessary information for best healthcare. In particular, with oral communications, we act discreetly when talking to or about patients. We stay aware of who is in the area or who could listen in. Because we discuss health care issues all day, it may be easy to be casual with verbal communication. We will never make that assumption. **We will always assume the patient wants privacy when discussing necessary information about their healthcare.** Again, the minimum necessary standard applies to disclosure, including oral disclosures, among providers for treatment purposes.

"Reasonable safeguard" means that we make reasonable efforts to prevent uses and disclosures not permitted by the rule. However, HHS does not expect reasonable safeguards to guarantee the privacy of PHI from any and all potential risks. HHS has said that in determining whether a Covered Entity has provided reasonable safeguards, they will take into account all the circumstances, including the potential effects on patient care and the financial and administrative burden of any safeguards. **We will remember, balance privacy with patient care.**

We will speak quietly and privately when discussing a patient's condition with family members in a waiting room or other public area, and avoid using patients' full name in public hallways or reception areas. Protection of patient identity is an important part of our practice. If the patient or others have **difficulty hearing** or exhibits other communication problems, **we will take them to a private area** when discussing PHI.

TALKING TO OTHER PROVIDERS AND PATIENTS

- Healthcare staff may orally coordinate services at check-out stations.
- Check out stations will be configured with HIPAA privacy in mind.
- Healthcare professionals may discuss a patient's condition over the phone to authorized entities.
- Healthcare professionals may discuss lab tests results with a patient or other provider over the phone or in a private treatment area.
- Healthcare professionals may discuss a patient's condition during training rounds in an academic or training institution if applicable.

CALLING OUT PATIENT NAMES

HHS has not provided specific instructions regarding calling out patient names in waiting rooms. They have said that they will **"propose regulatory language to reinforce and clarify that this and similar oral communications are permissible".** This becomes tricky from the standpoint of managing and respecting our patients. Many adult patients prefer to be called by their Surname. Common first names also increase the chances that several individuals may be seated in one reception area with that same name. With these factors considered, **we will generally call for patients by first name unless asked to do otherwise.** Should a Surname be requested we will document this both in the patient's chart (paper and/or software). We will confirm last name as soon as patient interacts with us at a close, personal distance to avoid escorting the incorrect patient to treatment areas. If we use sign-in sheets, we will not request any information concerning the patient's specific complaint; we will request only the patient's first and last name.

J. Parents And Minors

It is our policy to work closely and cooperatively with our patients to ensure that they understand their health conditions at all times. We encourage questions and give answers that are clear and understandable to our patients. HIPAA Omnibus Rule provides individuals with certain rights to access their PHI, including the right to obtain access to and to request amendment of health information about themselves, also to give Third Parties these rights when requested properly in a written Authorization (see the Third Party Authorization Form These rights rest with that individual, or their "personal representative".

The concepts below will provide exceptional guidance for you, regarding confidential relationships and parents or guardians. If you find yourself in a situation where you are not sure as to the PHI you should divulge to a parent, guardian, or child, please check with our Compliance Officer.

Because a parent usually has authority to make health care decisions about his or her minor child, a parent is generally a "personal representative" of his or her minor child and has the right to obtain access to health information about his or her minor child. This would also be true in the case of a guardian or other person acting in loco parentis of a minor.

There are exceptions in which a parent might not be the "personal representative" with respect to certain health information about a minor child. In the following situations, the Privacy Rule defers to determinations under other law that the parent does not control the minor's health care decisions, and, thus, does not control the PHI related to that care.

- When state or other law does not require consent of a parent or other person before a minor can obtain a particular health care service, and the minor consents to the health- care service, the parent is not the minor's personal representative under the Privacy Rule. For example, when a state law provides an adolescent the right to consent to mental health treatment without the consent of his or her parent, and the adolescent obtains such treatment without the consent of the parent, the parent is not the personal representative under the Privacy Rule for that treatment. The minor may choose to involve a parent in these healthcare decisions without giving up his or her right to control the related health information. Of course, the minor may always have the parent continue to be his or her personal representative even in these situations.
- When a court determines or other law authorizes someone other than the parent to make treatment decisions for a minor, the parent is not the personal representative of the minor for the relevant services. For example, courts may grant authority to make healthcare decisions for the minor to an adult other than the parent, to the minor, or the court may make the decision(s) itself. In order to not undermine these court decisions, the parent is not the personal representative under the Privacy Rule in these circumstances.

State Laws

In addition to the provisions (described above) tying the right to control information to the right to control treatment, the Privacy Rule also established and still holds true that it does not preempt state laws that specifically address disclosure of health information about a minor to a parent (§160.202). This is true whether the state law authorizes or prohibits such disclosure. Thus, if a doctor believes that disclosure of information about a minor would endanger that minor, but a state law requires disclosure to a parent, the doctor may comply with the state law without violating this HIPAA Rule. Similarly, a provider may comply with a state law that requires disclosure to a parent and would not have to accommodate a request for confidential communications that would be contrary to state law.

Parents and their Children's Healthcare Records

The Privacy Rule allows parents, as their minor children's personal representatives, to have access to information about the health and well-being of their children. This occurs when state or other underlying law allows parents to make treatment decisions for the child.

There are two exceptions to the above statement:

1. When the parent agrees that the minor and the healthcare provider may have a confidential relationship, the provider is allowed to withhold information from the parent to the extent of that agreement. If a parent agrees to this, the person giving the care should make an easily identifiable record of this agreement in the patient chart.
2. When the provider reasonably believes in his or her professional judgment that the child has been or may be subjected to abuse or neglect, or that treating the parent as the child's personal representative could endanger the child, the provider is permitted not to treat the parent as the child's personal representative with respect to health information.

Parental Consent

The Privacy Rule established access to health information, not the underlying treatment. The rule does not address consent to treatment, nor does it preempt or change state or other laws that address consent to treatment.

Emergency healthcare without a parent's (See: Consent to Treat Laws)

Even though a parent does not provide consent to treatment in an emergency healthcare situation, since established under the Privacy Rule, the parent would still be the child's personal representative. This would not be so only when the minor provided consent (and no other consent is required) or the treating doctor suspects abuse or neglect or reasonably believes that releasing the information to the parent will endanger the child.

K. Uses and Disclosures of PHI Without a Patient's Written Authorization

The Privacy Rules (45 CFR 164.506(a)) list three situations in which we may use or disclose PHI without obtaining written authorization from the patient. A Covered Entity may use or disclose PHI for its own treatment, payment or health care operations.

1. **TREATMENT** means the provision, coordination or management of health care and related services, including the coordination or management of health care with a third party, consultation between health care providers or the referral of a patient form one health care provider to another.
2. **PAYMENT** means activities undertaken by a health care provider to obtain reimbursement for the provision of health care and includes billing, collection activities, determining medical necessity, and determination whether a service is covered under a health plan.
3. **HEALTH CARE OPERATIONS** is defined very broadly to include conducting quality assessment and improvement activities; patient safety activities; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the covered entity; the sale, merger or consolidation of all or part of the covered entity with another covered entity.

See 45 CFR 164.501.

Under Omnibus Rules a patient must be informed of our intent to use their PHI in Marketing, Fund Raising or Research. The patient must be offered an "opt out" clause for future incidences and our facility must not discriminate in terms of treating the patient who does "opt out". In this case, a patient may choose to "opt out", but would sign the remainder of their HIPAA PATIENT ACKNOWLEDGEMENT FORM.

Another mandate under Omnibus Rule is to inform the patient of our involvement in receiving commissions or remuneration for products or services we may recommend to them. We must obtain written permission prior to discussing any such products or services with the patient. We must honor that choice, not discriminate against them during our course of treatment. In this case, a patient may choose to "opt out", but would sign the remainder of their HIPAA PATIENT ACKNOWLEDGEMENT FORM.

L. To Treat… or Not to Treat

Doctors and other providers may be exposed to serious liability if they provide treatment to patients who have not signed consent forms. "Consent to Treat" is not a HIPAA topic, please reference "Consent to Treat" laws of your jurisdiction. If you need more guidance in understanding "Consent to Treat" Forms, please see Management.

Incapacity Governed by State Law

HIPAA law largely defers to state law in incapacity situations. Sec 164.502(g) states that a "personal representative under applicable law" (generally meaning state law) "who has the authority to make healthcare decisions for another person of any age, also has the authority to make healthcare information decisions, such as those that involve granting consent for TPO of the other person".

In many contexts, particularly emergencies and hospital care, whether an adult patient is able to knowledgeably grant consent on healthcare and information issues is a determination that doctors or even ambulance staff must make. Once the doctor says a hospital patient is incapacitated, health information decisions should be made under policies and procedures developed in light of privacy laws for the particular state.

Most States Have Legal Hierarchy

Most states provide roughly similar legal hierarchies for determining who the personal representative of an adult is for health purposes. The approximate order they suggest—which is not necessarily the law in any one state—is as follows:

1. Legal guardians ordered by courts or recognized in state-mandated forms. Many states now have a state mandated "health care proxy" or "living will" form that patients fill out and sign when admitted to hospitals. The forms designate not only personal representatives, but also certain care decisions. Court-ordered guardianships are helpful, because without one, there are sometimes conflicts in determining the patient's choice on healthcare or information. For instance, two adult children of an elderly patient may disagree on what treatment to authorize.
2. "Durable" powers of attorney DPOA/ guardianships may also be in effect, for healthcare only. These typically must be "activated" by the signatures of two doctors. Ordinary powers of attorney are only for financial uses.
3. Family hierarchy is used when there is nothing in writing. The hierarchy is sometimes set forth in state "substituted judgment" statutes, and sometimes merely set in healthcare facility policies or by common assent. Usually the order for an incapacitated adult patient is: spouse, parents, adult children, siblings, and then more distant relatives such as cousins and nieces/nephews.

M. Using the "Minimum Necessary" Benchmark When Disclosing Our Patient's Health Care Information

As a general rule our practice feels that the term is self-explanatory. Whenever you are dealing with patient health-care information always review and/or disclose the minimum necessary to accomplish your task.

HHS has declared that healthcare workers must take reasonable steps to limit the use or disclosure of, and requests for Protected Health Information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

- Disclosure to or requests by a healthcare provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an authorization requested by the individual.
- Uses or disclosures required for compliance with the standardized HIPAA Omnibus Rule transactions.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
- Uses or disclosures that are required by other law.

If you ever have any questions regarding your access to patient information, please ask our HIPAA Compliance Officer

When is too much information too much?

What if you are in a situation where you believe that a request for patient information is seeking more than the minimum necessary PHI? If this occurs, the Omnibus Rule requires you to limit the disclosure to the minimum you think is necessary using a reasonable effort to limit patient information. The rule actually does permit you to rely on the judgment of the person requesting the information. But it says that the reliance must be reasonable. It even says that despite your concerns you may make the disclosure as requested, again, if it is reasonable.

Keep in mind that nothing in the Omnibus Rule prevents you from discussing concerns with the person making the request, and negotiating an information exchange that meets the needs of both parties. If you have real concern about a request, contact our HIPAA Compliance Officer.

The most difficult situations are when a non-routine disclosure is needed. As a general rule, these special situations should be discussed with our HIPAA Compliance Officer. In these cases, we want to be especially vigilant that we determine and limit disclosure to only the minimum amount of PHI necessary to accomplish the purpose of the non-routine disclosure.

HHS has said that in certain circumstances, the Omnibus Rule permits a Covered Entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed (emergencies, communication barriers, etc.). Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency for a disclosure permitted under §164.512 of the rule.
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

We must make "*Reasonable Efforts*" to limit Use and Disclosure of PHI

HHS has said that each healthcare entity must determine its own set of standards for minimum necessary use and disclosure of patient information. The Omnibus Rule continues support of previous statutes that requires a Covered Entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the **minimum necessary to accomplish the intended purpose.** To allow Covered Entities the flexibility to address their unique circumstances, the rule requires us to make our own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of business and workforce. Best practices will have us limiting and protecting information uses or disclosures to those that are absolutely needed to serve the purpose and to be consistent with this approach.

We consistently will evaluate our practice and enhance protections as needed to prevent unnecessary or inappropriate access to PHI. If you have any suggestions as to how we can better limit access to and disclosure of our patient information, please bring this information to our HIPAA Compliance Officer. The minimum necessary standard is intended to reflect and be consistent with, not override, professional judgment and standards. We want to appropriately limit access to protected health information without sacrificing the quality of healthcare that we offer.

There are some who worry that the minimum necessary restrictions impede the delivery of quality healthcare by preventing or hindering necessary exchanges of PHI among healthcare providers involved in treatment. HIPAA rules provide our practice with substantial discretion as to how to implement the minimum necessary standard, and appropriately and reasonably limit access to the use of the health information concerning our patients. The rule recognizes that we are in the best position to know and determine who in our workforce needs access to protected health information to perform their jobs. Keep this in mind when interacting with other authorized entities in the course of your job.

Remember the Concept of "Reasonable Efforts"

HHS was asked if healthcare practices are required to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, in order to comply with the minimum necessary requirements. They said "no". The Rule says that the basic standard for minimum necessary use requires that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the Covered Entity. The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary use. At this time, the Omnibus Rule does not directly require this. Things may change in the future.

On the other hand, HHS has said that healthcare providers may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, for securing protected information. If you have any suggestions for situations in our offices where you feel that our patient information is not secure, please contact our HIPAA Compliance Officer. All security measures will follow our HITECH Law protocols as listed prior and also in our HITECH Packet in the OFFICE POLICIES section of this manual. HHS encourages actions towards configuring our record systems to limit access to some PHI fields in a patient's record through our practice management software. Or to partition our software systems, when possible, to create limited access to PHI. HHS understands that for a small healthcare facility with a largely paper-based records system, limited access to employees may be more challenging. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the rule. This is what is meant by reasonable efforts.

Healthcare Residents, Healthcare Students, Trainees, Temps and Volunteers

The minimum necessary requirements do not prohibit healthcare residents, healthcare students, nursing students, and other healthcare trainees from accessing patients' healthcare information in the course of their training. The definition of "healthcare operations" in the rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health- care learn under supervision to practice or improve their skills as healthcare

providers." See 45 CFR Sec. 164.501. These entities will however, have signed Business Associate Agreements or Employee Confidentiality Agreement (if on our payroll) on file with our facility prior to having exposure to PHI.

Third Parties

The minimum necessary concept need not be applied to third parties that are authorized by the patient him or herself. This includes written authorizations whereby the patient expressly permits us to provide PHI to third parties, such as: life, disability, or health. For example, if a covered healthcare provider receives an individual's written authorization to disclose healthcare information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of the HIPAA Omnibus Rule.

Disclosure to Federal and State Agencies

We are not required to make a minimum necessary determination to disclose to Federal or State agencies, such as the Social Security Administration (SSA) or its affiliated state agencies, or for individual applications for Federal or State benefits. These disclosures must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements. HHS has said further that use of the provider's authorization form is not required. Providers can accept an agency's authorization form as long as it meets the requirements of §164.508 of the rule.

Disclosure of an Entire Healthcare Record

HHS has said that use, disclosure, or requests of an entire healthcare record is allowed. The patient under Omnibus Rule is entitled to their desired electronic format. If it is not available, a similar electronic format must be delivered, all within 30 days of written request.

HHS has also said that a covered entity may use, disclose, or request an entire healthcare record without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire healthcare record is reasonably necessary for certain purposes. For this reason, it is important that you are aware of those in our workforce that are authorized to see the entire healthcare record and the conditions. Our HIPAA Compliance Officer can help identify our policies and procedures for routine disclosure and requests, as well as the criteria used for non-routine disclosure that would identify the circumstance under which disclosing or requesting the entire healthcare record is reasonably necessary. Our Compliance Officer can clarify criteria to assist you in determining when to request or release the entire healthcare record. With this in mind, it is clear that HIPAA Privacy Rule does not require that a justification be provided with respect to each distinct healthcare record. Keep in mind that no justification is needed in instances where the minimum necessary standard does not apply, such as disclosures to or requests by the healthcare provider for treatment, or disclosures to the individual, or authorized Third Parties.

Regarding Patient Healthcare Charts at Point-of-Care, Empty Prescription Vials, X-ray Displays

HHS has indicated that specific workplace practices need to remain as they have been developed over the years in order to maintain proper patient care and reasonable workflow. The minimum necessary standards do not prohibit us from maintaining patient healthcare charts at point of care (chair side or bedside), nor do they require that we shred empty prescription vials, or require that X-ray monitor displays be remounted, so long as patient names or other PHI are shielded to obscured patient identity whenever possible.

We must, in accordance with other provisions of the HIPAA Law, take reasonable precautions to prevent inadvertent or unnecessary disclosures. For example, while HIPAA law does not require that X-ray boards be totally isolated from all other functions, it does require us to take **reasonable precautions** to protect X-rays from being accessible to the public. We will try to keep secure, using the best means possible, visual and auditory PHI from discovery without disrupting our work duties. Should you have ideas to improve this aspect of our work environment, please bring it to the attention of management.

Minimum Necessary Disclosure and Transaction Standards

HHS has set uniform transaction standards for keeping coding and insurance submission standardized. These formally were ICD-9-CM codes changing to ICD-10 codes under the HIPAA 5010 ruling. HHS believes that the *"minimum necessary standard"* does not conflict with the "transactions standards". There are some areas here where the "minimum necessary standards" are exempt. This includes all data elements that are required or required-by-situation in certain cases. In a way, the Transactions Standards guide you to give the right information. However, in many cases, covered entities have significant discretion as to the information included in these transactions.

N. Secure vs. Unsecure PHI

It is important to differentiate between secured vs. unsecured PHI. Please review the following to understand the distinction:

Breaches occur when our PHI becomes unsecured and falls into unknown or unauthorized hands. PHI is secured if it is unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology that has been approved by HHS. PHI is unsecured if it has not been rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology that has been approved by HHS. Therefore, hard-copy or paper records containing PHI are, by definition, UNSECURED.

With respect to Electronic PHI ("EPHI"), the following applies:
Electronic data at rest, which includes data that resides in databases, file systems, flash drives, memory, and any other structured storage methods, is unsecured unless it is encrypted consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
Electronic data in motion, which includes, for example, data that is moving through a network, including wireless transmission, whether by e-mail, e-claims, e-radiographs, e-charts or structured electronic interchange is unsecured **unless** it is encrypted in compliance, as appropriate Federal Information Processing Standards (FIPS) 140-2 validated. In addition, encryption keys should be kept on a separate device from the data that they encrypt or decrypt.
Data disposed, which includes discarded paper records or recycled electronic data. To be considered "Secured", the PHI must be destroyed in one of the following ways:

1. Paper, film, x-ray or other hard copy will be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.
2. Electronic data will be cleared, purged, or destroyed so that PHI cannot be retrieved.

Unsecured PHI

Notification is required if there is a breach and PHI is "unsecured."
Creating an unsecured situation or compromising PHI can occur by verbal indiscretions, mistakenly releasing paper correspondence, email, fax, phone or written contact of PHI, malicious misuse of said information, or technical mishaps. Employees who witness, suspect or discover that that PHI has been accessed, used or disclosed in a way that violates the HIPAA Omnibus Rules, should immediately report such information to our HIPAA Compliance Officer so we can keep in accordance HIPAA Omnibus Rule Breach Reporting Compliance Standards.

Personnel who discover that PHI has been compromised and is unsecure will need to know our Breach Reporting Protocol and proceed with an evaluation of the situation (this process is explained in detail in the next training section). A breach has occurred if PHI is accessed, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules as set forth in the Omnibus Rule.

Employees who are determined to have failed to adhere to the policies and procedures regarding reporting of breach of unsecured PHI will be subject to the disciplinary policies of our office and it will be documented in your employee record. Unreported, unsecured breaches also come with very serious HIPAA fines. Reporting breaches is a way for the HHS to discover over the next several years what type of breach activity is occurring in the healthcare arena. Please note that it is far better to report a breach, especially since the HHS wants to know even moderate breach occurrences. Taking the time and effort to report breaches will help our government determine better ways to qualify and quantify the breaches that are occurring within the United States.

O. Our Breach Reporting Plan

The HITECH ACT, now incorporated into the Omnibus Rule, requires notice to affected individuals, HHS and, in certain circumstances, the media, when there is a breach of unsecured PHI. A "breach" is defined as the acquisition, access, use or disclosure of unsecured PHI in violation of the Privacy Rule that compromises the security or privacy of the PHI. An impermissible use or disclosure of unsecured PHI is ***presumed*** to be a breach unless we demonstrate that there is a low probability that the PHI has been compromised. In this context, the word "compromised" means "to reveal or expose to an unauthorized person." There are three exceptions to this definition of "breach." There is no "breach":

1. if the acquisition, access or use of PHI is by a workforce member, in good faith, and without further use or disclosure not permitted by the Privacy Rule;
2. if there is an inadvertent disclosure to a person authorized to access PHI, without further use or disclosure not permitted by the Privacy Rule;
3. where there is a good faith belief that the unauthorized person would not be able to retain the information.

Apart from the those three exceptions, we must determine whether there is a low probability that the unsecured PHI has been compromised. If there is a low probability that the PHI has been compromised, then we do not have a breach and no reporting is required. The HIPAA Omnibus Rule requires all suspected breaches to be evaluated by using a "4-Factor Formula." to determine if a breach should be reported to HHS. We will use our **4-Factor Breach Assessment Forms** to document and track all breach incidents at our facility. These forms are located in the **BREACH ASSESSMENT** section of this manual. If a breach or potential breach is discovered, we will fill out a **4-Factor Breach Assessment Form** and proceed with actions to mitigate the breach. If the **4-Factor Breach Assessment Form** determines that there is more than just a "low probability" that the PHI was compromised, we will proceed to report the breach to the HHS and to all involved parties. We will complete documentation of the **4-Factor Breach Assessment Form**. All forms will be retained in securely in this HIPAA Manual and within patient charts.

While the forms are relatively straight forward, the determinants set forth by Omnibus Rule are not. Previously we were to report HIPAA breaches if they would potentially pose a *"significant risk"* of financial or reputational harm to the individual.

Under the Omnibus Rule, breach reporting changes to: *"presume a breach unless **low probability** that the PHI was compromised is proven"*. Because it is difficult to prove a low probability that PHI was compromised, **we will be reporting most breaches and documenting each situation.**

We report breaches to this web link:

Breaches affecting less than 500 people, will be submitted on a different eForm than
Breaches affecting more than 500 people, submit form at:
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

4-Risk Factor Assessment

At the back of this manual, you will find (2) **Breach Assessment Sections.** One should hold a *blank* Master Breach Assessment Sheet and the other is for *documented* Breach Assessment Sheets. These Breach Assessment Sheets will serve as an objective, user-friendly breach occurrence test. They will focus on whether PHI has been "compromised" for each situation you evaluate. Finally, they will demonstrate accordance with HIPAA Omnibus Rule standards for assessing various breaches. Here are some examples of possible breaches:

- Theft of an office computer
- You determine your computer data has been "hacked into"
- You dial the wrong phone number and leave a message using PHI
- You stuff an envelope with an incorrect patient invoice
- You notice a patient has walked off with your patient sign-in sheet
- You forgot to shred all documents and your cleaning crew has discarded them
- You accidently fax or email the wrong doctor's office PHI

While some of these occurrences may seem harmless, please use caution, as there is no "quantifying protocol" for this low probability measuring factor that Omnibus Rule imposes. And because the Omnibus Rule does not define the term "compromise" or explain what it means for PHI to be compromised, we must assume the standard dictionary definition, which is "to reveal or expose to an unauthorized person." Please be mindful to *document and report, first to management, all breach occurrences.* Our HIPAA Compliance Officer will help you determine if the breach will have a ranking above "low probability of risk", and will help you in the HHS reporting process. To avoid costly HIPAA fines toward our facility, we will be opting to report most breaches. We may in some situations also consult an attorney who specializes in this area of law should a situation prove to be serious or highly questionable in scope. Theft or hacking of PHI would require an attorney's attention.

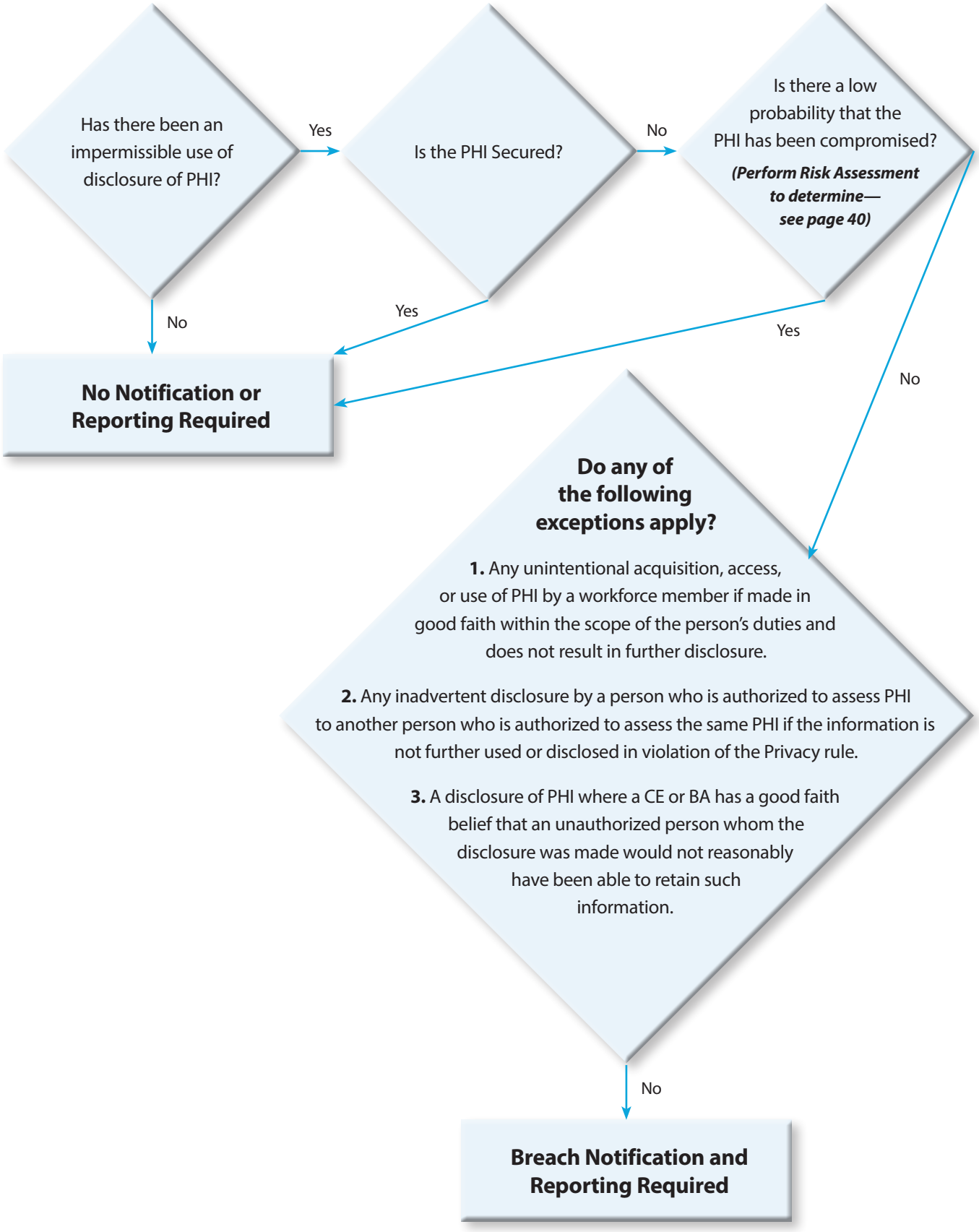
For now, let's look at how to use our **4-Factor Breach Assessment Sheets** provided in this manual:

How To Use the (4)-Factor Breach Assessment Sheet for PHI Breach Determination:

1. Determine / Discover that a potential breach situation has occurred.
2. Locate the **(4)-Factor Breach Assessment Sheets** provided in the back of this manual.
3. Fill-out the **(4)-Factor Breach Assessment Sheet**. Provide a brief description of the breach occurrence in the space provided and circle the answers that best fit the breach situation you are assessing to report. Share this information with our HIPAA Compliance Officer to determine if HHS reporting will be necessary. Keep a copy of the report in the back of this HIPAA Manual in the BREACH ASSESSMENT SHEETS (documented) sec-tion. Place a copy in the appropriate patient charts.
   If it is determined that there is more than a "low probability" that the PHI has been compromised, it is a breach that must be reported. Report the breach incident to: ***The Secretary of U. S. Department of Human Health Services*** using this electronic link: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html **(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)**
4. If a breach incident involves a group of patients we may need to notify **(OCR)** Office of Civil Rights, media, or other parties. Check immediately with the U.S. Dept. of Health & Human Services **(HHS)** or a legal professional specializing in this area of law for guidance in these matters. **HealthFirst** provides useful introductions and overviews to the law but will not consult or advise in matters of breach occurrences.

During the assessment process, if you feel you can mitigate the potential breach by contacting the end recipient of the PHI, please take measures to do so.

Breach Notification Flow Chart



HIPAA Breach Notification Risk Assessment

Risk Assessment Factors	Circumstances of the Incident (Circle)			
		Elements	Score	
1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. For example, if a file of known abuse victims is breached that includes the victims' addresses, then you will probably want to rank the breach of this data as a high probability of causing harm to the person(s) impacted by the breach. However, under other circumstances just the release of an address may be considered a low risk of harm to the person(s) impacted by the breach.	Elements at the top of the list are less likely to indicate compromise. Elements at the bottom of the list are ***more*** likely to indicate compromise.	**Clinical Information** • Non-Diagnostic Information • Limited Data Set • Name • Address • Room# • Email • DOB • Provider • Date of Service • SSN • Sensitive Diagnosis Information • *Sensitive Protected Health Information* which may include information about sensitive diagnosis such as HIV, Substance Abuse, and/or Mental Health. • STD • Medications that indicate sensitive diagnosis	Low Probability of Compromise ↕ High Probability of Compromise	The greater the number of elements the more likely there is high probability of compromise.
2. The unauthorized person who used the PHI or to whom disclosure was made. If the information impermissibly used or disclosed is not immediately identifiable, entities should determine whether the unauthorized person who received the protected health information has the ability to re-identify the information. For example, if information containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may be more than a low probability that the protected health information has been compromised. (78 F .R. 5643). Does recipient have confidentiality obligations? (5643)		• Your Business Associate • Another Covered Entity • Internal Workforce • Wrong Payor (not the patient's) • Unauthorized family member • Other	Low Probability of Compromise	
		• Non-covered entity • Media • Unknown/Lost/Stolen • Member of the general public • Patient employer • Other	High Probability of Compromise	

<table>
<tr><td rowspan="2">3. Whether the PHI was actually acquired or viewed.
For example, there is likely a low risk if a misdirected letter is returned unopened or a lost computer is recovered and it is confirmed that PHI was not accessed. Conversely, there is a higher risk where the recipient opens and reads a misdirected letter even though she reports the letter to the covered entity.</td><td rowspan="2"></td><td>• Unauthorized internal acquisition, access and/or use without disclosure outside of organization Extent to which PHI was in fact accessed (5643)
• Verbal Disclosure
• View only
• Other</td><td>Low Probability of Compromise</td></tr>
<tr><td>• Paper I Fax
• Electronic
• Other</td><td>High Probability of Compromise</td></tr>
<tr><td>4. Whether the risk to the PHI has been mitigated.
For example, there may be a lower risk if a fax is directed to the wrong number, but the recipient confirms that they returned or destroyed the PHI; the PHI has not been and will not be further used or disclosed; and the recipient is reliable. (/d.). This factor highlights the need for covered entities and business associates to immediately identify and respond to potential breaches to reduce the probability that PHI is compromised and the necessity of breach reporting.

If risk has been mitigated, then low risk of compromise.

If risk has not been mitigated, then high risk of compromise.</td><td>Disposition (What happened to the information after the initial disclosure) Has the risk to the PHI been mitigated?

Did we get it back? Certification/attestation of destruction? Reliability of attestation? Unreadable/undecipherable? Other impact? Controls in place to influence ability to compromise? Flag records Like red flags? Value of Data? (insurance number vs. other types)</td><td>• Visual—viewed only with no further disclosure or retention
• Obtained reliable assurances that the use or disclosure was very limited
• Obtained reliable assurances that the PHI will not be further used or disclosed?
• Information returned complete
• Information properly destroyed and attested to
• Information properly destroyed (unattested)
• Electronically Deleted (unsure of backup status)
• Other</td><td></td></tr>
<tr><td>5. Other Factors</td><td colspan="3">Additional Controls
• Electronic Data Wiped
• Information/Device Encrypted, but does not meet compliance with NIST Standards
• Hardcopy or electronic media destroyed, but does not meet compliance with NIST Standards
• Encrypted—Encryption keys not secured
• Password Protected
• No Controls
Safeguards listed in the DHHS Breach reporting form:
• Firewalls, Packet Filtering (router based)
• Secure Browser Sessions
• Strong Authentication
• Encrypted Wireless, Physical Security
• Logical Access Control
• Anti-virus software, Intrusion Detection
• Biometrics
• Other</td></tr>
</table>

Additional information considered in your determination:

- Analysis Points/Narrative
- Ensure Mitigation or Process Correction within 30 days for reoccurrence

SCORING

If the entity concludes that the risk assessment demonstrates a low probability that the PHI has been compromised, the entity should document its analysis and may forego breach notification. On the other hand, if the risk assessment fails to demonstrate a low probability that the PHI has been compromised, the entity is required to report the breach unless one of the regulatory exceptions applies.

The scoring is meant to serve only as a guide in decision making and not designed to make the notification decision for you. There are a variety of factors and mitigations that may be involved in your incident that this tool may not foresee or predict. An attempt was made to develop this is a way that would help you in documenting your actions, consider risk factors and circumstances and then aid in your final decision of making a breach notification or not making a breach notification. There is no "scoring" element for factors #4 and #5 as they were considered mitigation factors as opposed to risk factors.

The scoring is designed to be subjective enough so that each entity can consider their own policies, technical safeguards/constraints, mitigation strategies, interpretation and details specific to the specific incident they are reviewing.

The risk factors carry a possible outcome of "Low Probability" or "High Probability."

Probability Compromised Information

Low Probability		**High Probability**
Notification Unlikely	Articulate and Document Decision To Notify or Not	Notification Likely

Breach notification is necessary in all situations except those in which the covered entity demonstrates that there is a low probability that the protected health information has been compromised.

An example of our (4)-Factor Breach Assessment Sheet is on the following page.

(4)-Factor Breach Assessment Sheet
for HIPAA Omnibus Rule PHI Breach Determination

(This file is also available on your training HIPAA On-Line Portal in the **Omnibus Rule eForms** folder)

Date of Incident: _____

Name of Patient at Risk: _____

Type of PHI breached:

❑ paper / mail ❑ email ❑ fax ❑ phone ❑ conversation ❑ visual ❑ theft ❑ hacking

❑ other, describe: _____

Brief description of incident: _____

_____

_____

Check "**Yes**" or "**No**" for the breached situation you are evaluating:

RISK FACTORS		
#1 PHI INVOLVED—Is this PHI likely to be identified and linked easily to the patient?		
SENSITIVE / HIGH RISK PHI: Includes any of these…	**Yes**	**No**
Name Address Email Address Full Fa[illegible] Note Nam[illegible]ith Lab Results	Phone Number Credit Card Number Web Address Finger P[illegible]	Social Security Number License Number Vehicle ID M[illegible]ice ID
#2 RE[illegible]IENT of the PH[illegible]—Is r[illegible]ipient au[illegible]ori[illegible]d to rec[illegible]ve [illegible]I? Example[illegible] ***afe Recip[illegible]nts:*** D[illegible]tor or H[illegible]lth [illegible]ility, [illegible]sura[illegible]e Carr[illegible] of Pati[illegible], Phar[illegible]acy, Authorized Le[illegible] Repr[illegible] [illegible]ur Emp[illegible]yee, [illegible]ur B[illegible]ines[illegible]ssocia[illegible] Business A[illegible]ociates Subcontractor, [illegible]r Pa[illegible]ent	Y[illegible]	N[illegible]
UNS[illegible]E REC[illegible]ENT / HIGH RISK: [illegible]clud[illegible]s any o[illegible]ese… Un Known Stolen Hacked-Into Known but not Business Associate Known but not Patient	Y[illegible]	
#3 PHI ACQUIRED / VIEWED—Was the PHI acquired & viewed?	**Yes**	**No**
Unsafe recipient received PHI	**Yes**	**No**
Safe recipient received & viewed PHI	**Yes**	**No**
#4 PHI MITIGATION **UNSAFE PHI: Includes any of these…** Not Traceable Not Retrievable UNABLE to mitigate Lost Stolen Hacked-Into	**Yes**	**No**
If the PHI *can be located and suppressed* it will be considered *diffused*. Locate by a: phone call, email, letter, text to confirm correspondence; PHI needs to be destroyed!	**Yes**	**No**

Since there are no "quantifiable parameters", we advise you to Report most everything

1 Yes = **Report this Breach**
2 Yes = **Report this Breach**
3 Yes = **Report this Breach**
4 Yes = **Report this Breach**
5 Yes = **Report this Breach**

Breaches of PHI need to be reported to:

The ***Secretary of U. S. Department of Human Health Services*** using this electronic link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

There are (5) of these sheets at the back of this packet for you to print and keep on file for easy access in your HIPAA Manual. Label with a tab: Breach Assessment Sheets

Our Business Associates are now responsible to discover and report breaches of PHI to Government Agencies, to us, and to the patients involved per HIPAA Omnibus Rules and per our Business Associate Agreement.

Steps to follow if a Breach must be reported

If we need to report a breach, we will use this web link:

Breaches affecting less than 500 people, will be submitted on a different eForm than Breaches affecting more than 500 people, submit form at:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

As soon as possible, but no later than 60 days after we discover a breach, the patient or involved entity should be issued a written notice deliverable by registered or return receipt mail to the last known address of that individual, or we may provide written notice by electronic mail, if the individual agrees to receive electronic notice, and such agreement has not been withdrawn. If the affected individual is a minor or otherwise lacks legal capacity, the notification may be sent to the individual's personal representative. If the individual is deceased, the notice may be sent to the deceased individual's next of kin or personal representative if the address of the decedent's next of kin or Personal Representative is known.

If there is insufficient contact information for some or all affected individuals, individuals will be sent a substitute notice. If sufficient contact information is unavailable for fewer than ten (10) affected individuals, substitute notice may be provided through an alternative form of written notice, such as electronic mail, telephone or other means. If no current contact information is available for the individuals, notice may be posted in their current chart. We will also notify the HHS and all involved parties/authorities of the breach, or any breaches of unsecured PHI made by our personnel, immediately upon discovery.

Under the direction of the HIPAA Compliance Officer, we will maintain records of all breaches within our HIPAA documentation. We will also maintain this breach information and documentation regarding breach of unsecured PHI for six years. We are not required to submit information for breaches that occurred before September 23, 2009.

SAFEGUARDS AFTER BREACH OCCURS

- Debriefing with management regarding Breach Situation
- Additional Employee Training and Development of Breach Mitigation Policies

P. Our HITECH Security Policies

The healthcare industry has experienced sweeping change. Internet infor-mation sharing has made Private Health Information (PHI) vulnerable to many indiscretions. From theft of PHI and malicious posting of it on the internet by disgruntled employees, to hackers stealing insurance ID infor-mation and misusing social security numbers, the breaches are serious and astounding. The federal government has recognized that health records needed to be managed more securely with criminal and civil fines for mis-use. The Health Information Technology for Economic and Clinical Health Act (HITECH or "The Act" effective February 17, 2010) and (ARRA) of 2009, allowed a number of incentives to *encourage* the adoption of health infor-mation technology use.

The **HITECH Act** expanded the activities covered by HIPAA in the scope of electronic privacy and security to protect Patient Health Information (PHI) by taking various precautionary measures. It defines what incidents con-stitute a privacy breach and requires business associates and employees to comply with the Security Rule's administrative, physical, and technical safeguard requirements. The Act also required accounting of disclosures to patients upon their request. Penalties for HIPAA violations under HITECH extended from the employer to include the employee for misconduct. Currently, the Omnibus Rule increases these fines from $25,000 to $1.5 million. Penalties for malicious conduct with posting PHI on the internet (for example: on Facebook™ or Instagram™) will also result in jail time if traced back to the employee. Employers are no longer responsible for the misconduct of employees with regard to foul play on the internet.

In accordance with HITECH Law, we will handle PHI in the following manner at this facility:

- Confidential Information (PHI) must be protected from other patients.
- Computerized Information will use screen savers or software protection to block viewing range of anyone other than screen operator.
- We will avoid asking Sensitive Information—or do so privately.
- Communication with other team members must at all times be restrictive.
- Patient Charts should not be left for others to view or handle.
- No communication about patient's identities or conditions outside of the office.
- Terminated or Separated Employees. Eliminate all access.

USE CAUTION UNDER OMNIBUS RULE

Consider having a Business Associates Agreement in place for vendors who may "see or use" your patient PHI: Cleaning Crews, Plant Watering Service, Aquarium Maintenance, Healthcare Vendors, Volunteers, Temps, etc. It makes good business sense to have a BAA signed and on file for all vendors who may come into contact with your PHI.

STANDARDIZATION AND TRANSFER OF PHI

- Encryption for the Security of Electronic Transfer of PHI
- Protection against reasonably anticipated threats, hazards—Ensures compliance by workers
- Deliver PHI within 30 Days of written request in an electronic format patient desires (if available)
- Deliver PHI to Third party with proper Written Request
- Date of Request, Full Name of Party, Where to send

HITECH ENFORCEMENT OF SECURITY RULE SAFE GUARD REQUIREMENTS FOR

- Administrative Safeguards
- Technical Safeguards
- Physical Safeguards

Administrative Safeguards

- A Privacy Officer is designated
- Written set of privacy procedures reside in the OFFICE POLICIES / HITECH Section of this manual
- The procedures state who has access to PHI
- The procedures state how data is properly stored and secured
- The procedures state train on HITECH procedure for employees new /existing
- The procedures in DATA RECOOVERY & CONTINGINCY PLAN state our protocol response for emergency
- The procedures in our BREACH ASSESSMENT section state protocols for Breach Situations

Technical Safeguards

- This area is set up with Federal Standards by our computer networking advisors
- There is encryption over open networks, routers and firewalls
- Wireless routers are isolated from primary network & Ensure default to secure settings
- Anti-spyware software is up-to-date and used regularly
- Staff is trained and advised to use only secure and trusted web sites
- Software is able to prevent against erasure or change
- Password Protection is required for each employee to use terminals
- We Log in and out of practice management software
- Levels of Security are set for Managerial Access only
- There exists double checking data corroboration by double-keying passwords and authenticating digital signatures
- Authentication of communication is checked from other entities via in ports
- Configuration of records is secure
- We "lock down" access to computers / end of day to prevent access to anyone
- Daily Back-Up is Encrypted, Off-Site and Secured to Federal Standard
- Risk analysis and management programs are in place (see Office Policies section of this manual

Physical Safeguards

- PHI is protected from non-employees
- PHI access is monitored and detailed by password protection and protocols
- There are private workstations
- Business Associates Agreements are to Omnibus Standard
- Hardware and software is secure at all times
- Office is secured when we are not working

For our complete HITECH Protocols please see our HITECH PACKET in the Office Policies Section of this manual.

Q. Our Annual Data Back Up & Contingency Plan

We complete an Annual **Data Back-Up & Contingency Plan** to recover our patient PHI and our important business data to ensure we continue functioning as a business during or after any emergency situations.

Because Health Information is continually being shared over internet and digital devices from remote locations, we will ensure our business practices are functioning regardless of emergency times and in accordance with HIPAA Federal Standards. We will update these on a regular basis to keep up with advancing technology in the work force.

Our plan entails the steps each team member, management and our technology crew will take to secure: patient PHI, our back-up and data storage, ePHI (electronic Protected Health Information* and EHR** (Electronic Health Records). This is our contingency plan for the protection of our PHI and business data. We have designed the plan to ensure it will interface to another location while remaining safe, yet live-streaming.

We do this in accordance with the HIPAA Security Rule 45 CFR § 164.306The Security Rule was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), that requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information. See our DATA BACK UP & CONTINGENCY PLAN document located in the Office Policies section of this manual.

R. Our Business Associates Guidelines for Vendor Confidentiality

The Omnibus Rule allows us to share PHI with Business Associates. See Part II, Subsection (a) for the definition of "Business Associate/ Vendor (non-employees who may directly or indirectly be exposed to our PHI). Under the Omnibus Rule, Business Associates will need to sign a **new Business Associate Agreement ("BAA") that will replace any BAA** signed prior to the Omnibus Rules' approval since September 2013. All new, signed Omnibus Rule Business Associate Agreements should have been in place by:
New Associates = sign by Sept 23, 2013
Please update any that you have signed and on file, prior to this date

Omnibus Rule mandates that Business Associates will now be subject to the same stringent HIPAA Privacy Rule and Security Rule requirements, use and disclosure limitations as we are (the Covered Entity). They will be subject to audit and fines by HHS. Business Associates will need Business Associate Agreements from their subcontractors who may receive, create, or transmit PHI on their behalf. Our Business Associates will need to:

1. *Implement and maintain Information Security Policies* that comply with the HIPAA Security Rule [1]
2. *Enter into Business Associate Agreements with Subcontractors* with whom they exchange our PHI
3. These have to be written, signed & on-file in the Business Associate's workplace

   Respond to Breaches of PHI in accordance with new Omnibus Rule HHS regulation. Breaches of PHI need to be reported by the Business Associate to us, as the covered entity. We must then report the breach to the Secretary of U. S. Department of Human Health Services using this electronic link: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html ***(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)***
4. *Report the Breach to the Covered Entity/ Healthcare Facility and the source patient.*

Business Associates under the Omnibus Rule include:

- Health Information Organizations
- E-prescribing Gateways
- Data Collection Agencies (Vendors who store or use your PHI)
  - Software Company
  - IT Tech
  - Collection Agency
  - Confirmation Service (email or text confirmations)
  - Phone Answering Service
  - Consultants
  - Temporary Employees
  - Volunteers

Business Associates may also include, as a precaution, but not required:

- After Hours Services
- Cleaning Crews
- Confirmation Services
- Collection Agencies
- Software Companies, if they have access to PHI in the course of providing their services
- IT Techs, Other Entities—if they have access to PHI in the course of providing their services
- Consultants, if they have access to PHI in the course of providing their services

Non-Business Associates or entities *not required to have a signed Business Associates agreement on file.* These are chosen by the patient or affiliated with by choice. Such will be:

- Doctor-to-Doctor business
- Healthcare Providers
- Insurance Company business
- Pharmacies
- Labs

Understand that the new Omnibus HIPAA regulations are far reaching. They will now start with our facility, you the employee and penetrate all of our Business Associates and their Subcontractors to protect our patient's (PHI) Protected Health Information. Basically no one is to mishandle PHI or share it with marketers, advertisers or others for professional gain. The new Omnibus Rule helps prevent the "ripple effect" with regards to PHI. Now all entities that come into contact with PHI, directly or indirectly will need to respect PHI to the fullest degree of the law. This new protection is a massive effort on the part of the US government to decrease and mitigate identity fraud and malicious conduct.

PHI may be disclosed to a Business Associate only to enable them to help us carry out our health care functions—not for independent use by the Business Associate. Because many businesses touch our business and may inadvertently see or gain access to our patient files or our computer terminals, we now regard all service help and after-hours contractors with access to our facility. These entities will also sign a in most instances, order to do business with us. If you have any questions about whether a contractor of ours is or is not a business associate, or if you have any questions whether one of our Business Associates has signed our most up-to-date Business Associate Agreement, please contact the Compliance Officer. We have a "Business Associate Agreement" that should be used in all situations where required.

S. Our Omnibus Rule Protocols

***OMNIBUS* is defined as…**
noun: A volume containing several novels or previously published parts.
adjective: comprising several items.

As of January 17, 2013, HIPAA regulations have had a massive update and overhaul to protect patients. The new laws more extensively hold second and third party businesses responsible to keep patient health information (PHI) private! *Protected Health Information* is defined as any identifiable information which relates to an individual's past, present or future physical or mental health or condition for which there is a reasonable cause to believe it can be used to identify that individual. There are 18 identifiers listed in the Privacy Rule that, if found with any health information, are sufficient to make the health information "identifiable." ***(45 CFR Sec. 164.514 --Code of Federal Regulations)***

In the ***Office Policies Section*** of this HIPAA manual you will learn the details of *HIPAA's Omnibus Rule*. It brings massive change to the way we manage HIPAA duties and patient's Protected Health Information (PHI) within the healthcare workplace. It is important that each employee has a detailed understanding of the HIPAA Omnibus Rules of 2013. Please read this brief synopsis below, but study the entire ***HIPAA Omnibus Rule Training Packet*** (located in the ***Office Protocols Section*** of this manual).

The Office for Civil Rights (**"OCR"**) of the U.S. Department of Health and Human Services (**"HHS"**) adopted this update to the USA's existing volumes of HIPAA Law and HITECH Law. The Final Rule or final HIPAA omnibus rule **(78 Fed. Reg. 5566)** has some important modifications to HIPAA as we know it. They are required to begin functioning within your workplace, beginning March 26, 2013. Though you are allowed time to attain signatures from Business Associates for compliance. Below we have listed requirements of the new Omnibus Rule law and what is required of you:

1. New Business Associate Agreements must be signed; Old ones become obsolete: **A new version of the Business Associates Agreement is required to be signed & on-file in this HIPAA manual. New Associates, sign by Sept 23, 2013 & Existing Associates, sign new by Sept 22, 2014.**
2. New Compliance Obligations & Liability: Business Associates to their Subcontractors **Business Associate must have Subcontractor Confidentiality signatures on-file in their HIPAA manual.**
3. Breach Notification for Unsecured Protected Health Information (PHI) **New Breach Assessment Protocols are required. Forms are included in the BREACH ASSESSMENT SHEETS (blank) Section of this HIPAA manual for easy-access as you may need them.**
4. New Marketing & Fund Raising Protocols **Explained within the Omnibus Rules Packet in the Office Protocols Section of this manual; Also listed on the updated Notice of Privacy Practices (NOPP) within this HIPAA manual.**

THERE ARE 18 ...

Protected Health Information Identifiers

1. Names
2. Zip Codes
3. Bithdates All elements of dates (except year, unless individual is > 89 years)
4. Telephone numbers
5. FAX numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers (including license plate numbers)
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URL)
15. Internet protocol (IP) addresses
16. Biometric identifiers (including finger or voice prints)
17. Full face photos and comparable images
18. Any other unique identifying number, characteristic or code

5. New Additions to Notice of Privacy Practices (NOPP) for Patients' Right-to-Know **Updated Revision included within this manual; Keep as your new office copy of (NOPP / Omnibus Rule).**

Read ***HIPAA Omnibus Rule Workbook*** **in the back of this manual** for full details.

Within the remainder of this manual are:

SAMPLE FORMS THAT COMPLY WITH FEDERAL HIPAA LAW FOLLOW

For legal purposes, your Facility name and address should appear at the top of every form. Make sure you dispense these forms with this in mind. You should customize these forms. Many of these forms, you will rarely use. The one you will use most often are the:

- ✔ PATIENT ACKNOWLEDGEMENT OF RECEIPT OF PRIVATE PRACTICES
- ✔ NOTICE OF PRIVACY PRACTICES
- ✔ THIRD PARTY MEDICAL RELEASE FORM
- ✔ 4-FACTOR RISK ASSESSMENT FORM
- ✔ EMPLOYEE TRAINING & CONFIDENTIALITY AGREEMENT
- ✔ HITECH LAW ACKNOWLEDGEMENT
- ✔ EMPLOYEE TECHNOLOGY USE FORM
- ✔ BUSINESS ASSOCIATE AGREEMENT
- ✔ ANNUAL DATA BACK-UP & CONTINGINCY REPORT

PATIENT FORMS

All forms are updated to reflect the HIPAA Omnibus Rule Standards of 2013.

Notice of Privacy Practices to Omnibus Standard

- Must be displayed for patient viewing; Copy for patient if requested
- If you have a website, a copy must be posted on your site
- eFrom copies
- Optional Rules for NOPP

Patient HIPAA Acknowledgement of Receipt of Private Practices

- Every patient must sign a new copy to comply with Omnibus Rule; Keep in Patient Chart
- (2) Versions Doctors Office Version & Pharmacy / Treatment Facility Version (shorter)

Patient HIPAA Acknowledgement of Receipt of Private Practices for Pharmacy

Authorization for Release of Medical Records to a Third Party

- Have patient sign when requesting x-rays or copies of their records

Request for Alternative Communications

- This form is useful for situations where patients require alternative means of communication

Records Release to Patient: Authorization for Use and Disclosure of Protected Health Information

- Used when a patient wants copies of their own records
- Used when these specific health issues need to be disclosed:
  - HIV & Sexually Transmitted Disease Records
  - Alcohol & Substance Abuse
  - Psychotherapy Records

Request to Inspect, Copy or Summarize

- Typically used for auditors and attorneys consent to inspect your records.

Request for Amendment / Correction

- Used with litigation when records may not have been accurate

Request for Restrictions on Use / Disclosure

- When patient requests additional restrictions on their records. This may or may not be granted and could last only for a certain length of time

Request for Accounting of Disclosures

- Used to release personal patient accounting information

Prohibition on Re-Disclosure (HIV Information)

Prohibition on Re-Disclosure (Substance Abuse / Psychotherapy Information)

Limited Healthcare Power Of Attorney

Patient HIPAA Complaint Form / Information

To be provided to a patient if they ask for this form.
FIND THE OFFICIAL FORM AT: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf
Find Regional Addresses at: www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
(Google search HHS HIPAA Complaint Form if these links are broken)

HIPAA OMNIBUS Rule
NOTICE OF PRIVACY PRACTICES
for the Facility of:

Name of Facility: _____

Address: _____

_____

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION under the HIPAA Omnibus Rule of 2013.

PLEASE REVIEW IT CAREFULLY

For purposes of this Notice "us" "we" and "our" refers to the Name of this Healthcare Facility: _____ _____ and "you" or "your" refers to our patients (or their legal representatives as determined by us in accordance with state informed consent law). When you receive healthcare services from us, we will obtain access to your medical information (i.e. your health history). We are committed to maintaining the privacy of your health information and we have implemented numerous procedures to ensure that we do so.

The Federal Health Insurance Portability & Accountability Act of 2013, HIPAA Omnibus Rule, (formally HIPAA 1996 & HITECH of 2004) require us to maintain the confidentiality of all your healthcare records and other identifiable patient health information (PHI) used by or disclosed to us in any form, whether electronic, on paper, or spoken. HIPAA is a Federal Law that gives you significant new rights to understand and control how your health information is used. Federal HIPAA Omnibus Rule and state law provide penalties for covered entities, business associates, and their subcontractors and records owners, respectively that misuse or improperly disclose PHI.

Starting April 14, 2003, HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow when you first come into our office for health-care services. If you have any questions about this Notice, please ask to speak to our HIPAA Privacy Officer.

Our doctors, clinical staff, employees, Business Associates (outside contractors we hire), their subcontractors and other involved parties follow the policies and procedures set forth in this Notice. If at this facility, your primary caretaker / doctor is unavailable to assist you (i.e. illness, on-call coverage, vacation, etc.), we may provide you with the name of another healthcare provider outside our practice for you to consult with. If we do so, that provider will follow the policies and procedures set forth in this Notice or those established for his or her practice, so long as they substantially conform to those for our practice.

OUR RULES ON HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

Under the law, we must have your signature on a written, dated Consent Form and/or an Authorization Form of Acknowledgement of this Notice, before we will use or disclose your PHI for certain purposes as detailed in the rules below.

Documentation—You will be asked to sign an Authorization / Acknowledgement form when you receive this Notice of Privacy Practices. If you did not sign such a form or need a copy of the one you signed, please contact our Privacy Officer. You may take back or revoke your consent or authorization at any time (unless we already have acted based on it) by submitting our Revocation Form in writing to us at our address listed above. Your revocation

will take effect when we actually receive it. We cannot give it retroactive effect, so it will not affect any use or disclosure that occurred in our reliance on your Consent or Authorization prior to revocation (i.e. if after we provide services to you, you revoke your authorization / acknowledgement in order to prevent us billing or collecting for those services, your revocation will have no effect because we relied on your authorization/ acknowledgement to provide services before you revoked it).

General Rule—If you do not sign our authorization/ acknowledgement form or if you revoke it, as a general rule (subject to exceptions described below under "Healthcare Treatment, Payment and Operations Rule" and "Special Rules"), we cannot in any manner use or disclose to anyone (excluding you, but including payers and Business Associates) your PHI or any other information in your medical record. By law, we are unable to submit claims to payers under assignment of benefits without your signature on our authorization/ acknowledgement form. You will however be able to restrict disclosures to your insurance carrier for services for which you wish to pay "out of pocket" under the new Omnibus Rule. We will not condition treatment on you signing an authorization / acknowledgement, but we may be forced to decline you as a new patient or discontinue you as an active patient if you choose not to sign the authorization/ acknowledgement or revoke it.

Healthcare Treatment, Payment and Operations Rule
With your signed consent, we may use or disclose your PHI in order:

- To provide you with or coordinate healthcare treatment and services. For example, we may review your health history form to form a diagnosis and treatment plan, consult with other doctors about your care, delegate tasks to ancillary staff, call in prescriptions to your pharmacy, disclose needed information to your family or others so they may assist you with home care, arrange appointments with other healthcare providers, schedule lab work for you, etc.
- To bill or collect payment from you, an insurance company, a managed-care organization, a health benefits plan or another third party. For example, we may need to verify your insurance coverage, submit your PHI on claim forms in order to get reimbursed for our services, obtain pre-treatment estimates or prior authorizations from your health plan or provide your x-rays because your health plan requires them for payment; Remember, you will be able to restrict disclosures to your insurance carrier for services for which you wish to pay "out of pocket" under this new Omnibus Rule.
- To run our office, assess the quality of care our patients receive and provide you with customer service. For example, to improve efficiency and reduce costs associated with missed appointments, we may contact you by telephone, mail or otherwise remind you of scheduled appointments, we may leave messages with whomever answers your telephone or email to contact us (but we will not give out detailed PHI), we may call you by name from the waiting room, we may ask you to put your name on a sign-in sheet, (we will cover your name just after checking you in), we may tell you about or recommend health-related products and complementary or alternative treatments that may interest you, we may review your PHI to evaluate our staff's performance, or our Privacy Officer may review your records to assist you with complaints. If you prefer that we not contact you with appointment reminders or information about treatment alternatives or health-related products and services, please notify us in writing at our address listed above and we will not use or disclose your PHI for these purposes.
- New HIPAA Omnibus Rule does not require that we provide the above notice regarding Appointment Reminders, Treatment Information or Health Benefits, but we are including these as a courtesy so you understand our business practices with regards to your (PHI) protected health information.

Additionally, you should be made aware of these protection laws on your behalf, under the new HIPAA Omnibus Rule:

- That **Health Insurance plans** that underwrite cannot use or disclose genetic information for underwriting purposes (this excludes certain long-term care plans). Health plans that post their NOPPs on their web sites must post these Omnibus Rule changes on their sites by the effective date of the Omnibus Rule, as well as notify you by US Mail by the Omnibus Rules effective date. Plans that do not post their NOPPs on their Web sites must provide you information about Omnibus Rule changes within 60 days of these federal revisions.
- **Psychotherapy Notes** maintained by a healthcare provider, must state in their NOPPs that they can allow "use and disclosure" of such notes only with your written authorization.

Special Rules

Notwithstanding anything else contained in this Notice, only in accordance with applicable HIPAA Omnibus Rule, and under strictly limited circumstances, we may use or disclose your PHI without your permission, consent or authorization for the following purposes:

- When required under federal, state or local law
- When necessary in emergencies to prevent a serious threat to your health and safety or the health and safety of other persons
- When necessary for public health reasons (i.e. prevention or control of disease, injury or disability, reporting information such as adverse reactions to anesthesia, ineffective or dangerous medications or products, suspected abuse, neglect or exploitation of children, disabled adults or the elderly, or domestic violence)
- For federal or state government health-care oversight activities (i.e. civil rights laws, fraud and abuse investigations, audits, investigations, inspections, licensure or permitting, government programs, etc.)
- For judicial and administrative proceedings and law enforcement purposes (i.e. in response to a warrant, subpoena or court order, by providing PHI to coroners, medical examiners and funeral directors to locate missing persons, identify deceased persons or determine cause of death)
- For Worker's Compensation purposes (i.e. we may disclose your PHI if you have claimed health benefits for a work-related injury or illness)
- For intelligence, counterintelligence or other national security purposes (i.e. Veterans Affairs, U.S. military command, other government authorities or foreign military authorities may require us to release PHI about you)
- For organ and tissue donation (i.e. if you are an organ donor, we may release your PHI to organizations that handle organ, eye or tissue procurement, donation and transplantation)
- For research projects approved by an Institutional Review Board or a privacy board to ensure confidentiality (i.e. if the researcher will have access to your PHI because involved in your clinical care, we will ask you to sign an authorization)
- To create a collection of information that is "de-identified" (i.e. it does not personally identify you by name, distinguishing marks or otherwise and no longer can be connected to you)
- To family members, friends and others, but only if you are present and verbally give permission. We give you an opportunity to object and if you do not, we reasonably assume, based on our professional judgment and the surrounding circumstances, that you do not object (i.e. you bring someone with you into the operatory or exam room during treatment or into the conference area when we are discussing your PHI);

we reasonably infer that it is in your best interest (i.e. to allow someone to pick up your records because they knew you were our patient and you asked them in writing with your signature to do so); or it is an emergency situation involving you or another person (i.e. your minor child or ward) and, respectively, you cannot consent to your care because you are incapable of doing so or you cannot consent to the other person's care because, after a reasonable attempt, we have been unable to locate you. In these emergency situations we may, based on our professional judgment and the surrounding circumstances, determine that disclosure is in the best interests of you or the other person, in which case we will disclose PHI, but only as it pertains to the care being provided and we will notify you of the disclosure as soon as possible after the care is completed. **As per HIPAA law 164.512(j) (i)… (A) Is necessary to prevent or lessen a serious or imminent threat to the health and safety of a person or the public and (B) Is to person or persons reasonably able to prevent or lessen that threat.**

Minimum Necessary Rule

Our staff will not use or access your PHI unless it is necessary to do their jobs (i.e. doctors uninvolved in your care will not access your PHI; ancillary clinical staff caring for you will not access your billing information; billing staff will not access your PHI except as needed to complete the claim form for the latest visit; janitorial staff will not access your PHI). All of our team members are trained in HIPAA Privacy rules and sign strict Confidentiality Contracts with regards to protecting and keeping private your PHI. So do our Business Associates (and their Subcontractors). Know that your PHI is protected several layers deep with regards to our business relations. Also, we disclose to others outside our staff, only as much of your PHI as is necessary to accomplish the recipient's lawful purposes. Still in certain cases, we may use and disclose the entire contents of your medical record:

- To you (and your legal representatives as stated above) and anyone else you list on a Consent or Authorization to receive a copy of your records
- To healthcare providers for treatment purposes (i.e. making diagnosis and treatment decisions or agreeing with prior recommendations in the medical record)
- To the U.S. Department of Health and Human Services (i.e. in connection with a HIPAA complaint)
- To others as required under federal or state law
- To our privacy officer and others as necessary to resolve your complaint or accomplish your request under HIPAA (i.e. clerks who copy records need access to your entire medical record)

In accordance with HIPAA law, we presume that requests for disclosure of PHI from another Covered Entity (as defined in HIPAA) are for the minimum necessary amount of PHI to accomplish the requestor's purpose. Our Privacy Officer will individually review unusual or non-recurring requests for PHI to determine the minimum necessary amount of PHI and disclose only that. For non-routine requests or disclosures, our Privacy Officer will make a minimum necessary determination based on, but not limited to, the following factors:

- The amount of information being disclosed
- The number of individuals or entities to whom the information is being disclosed
- The importance of the use or disclosure
- The likelihood of further disclosure
- Whether the same result could be achieved with de-identified information
- The technology available to protect confidentiality of the information
- The cost to implement administrative, technical and security procedures to protect confidentiality

If we believe that a request from others for disclosure of your entire medical record is unnecessary, we will ask the requestor to document why this is needed, retain that documentation and make it available to you upon request.

Incidental Disclosure Rule
We will take reasonable administrative, technical and security safeguards to ensure the privacy of your PHI when we use or disclose it (i.e. we shred all paper containing PHI, require employees to speak with privacy precautions when discussing PHI with you, we use computer passwords and change them periodically (i.e. when an employee leaves us), we use firewall and router protection to the federal standard, we back up our PHI data off-site and encrypted to federal standard, we do not allow unauthorized access to areas where PHI is stored or filed and/or we have any unsupervised business associates sign Business Associate Confidentiality Agreements).

However, in the event that there is a breach in protecting your PHI, we will follow Federal Guide Lines to HIPAA Omnibus Rule Standard to first evaluate the breach situation using the Omnibus Rule, 4-Factor Formula for Breach Assessment. Then we will document the situation, retain copies of the situation on file, and report all breaches (other than low probability as prescribed by the Omnibus Rule) to the US Department of Health and Human Services at: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html ***(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)***

We will also make proper notification to you and any other parties of significance as required by HIPAA Law.

Business Associate Rule
Business Associates are defined as: an entity, (non-employee) that in the course of their work will directly / indirectly use, transmit, view, transport, hear, interpret, process or offer PHI for this Facility.

Business Associates and other third parties (if any) that receive your PHI from us will be prohibited from re-disclosing it unless required to do so by law or you give prior express written consent to the re-disclosure. Nothing in our Business Associate agreement will allow our Business Associate to violate this re-disclosure prohibition. Under Omnibus Rule, Business Associates will sign a strict confidentiality agreement binding them to keep your PHI protected and report any compromise of such information to us, you and the United States Department of Health and Human Services, as well as other required entities. Our Business Associates will also follow Omnibus Rule and have any of their Subcontractors that may directly or indirectly have contact with your PHI, sign Confidentiality Agreements to Federal Omnibus Standard.

Super-confidential Information Rule
If we have PHI about you regarding communicable diseases, disease testing, alcohol or substance abuse diagnosis and treatment, or psychotherapy and mental health records (super-confidential information under the law), we will not disclose it under the General or Healthcare Treatment, Payment and Operations Rules (see above) without your first signing and properly completing our Consent form (i.e. you specifically must initial the type of super-confidential information we are allowed to disclose). If you do not specifically authorize disclosure by initialing the super-confidential information, we will not disclose it unless authorized under the Special Rules (see above) (i.e. we are required by law to disclose it). If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with state and federal law that requires us to warn the recipient in writing that re-disclosure is prohibited.

Changes to Privacy Policies Rule
We reserve the right to change our privacy practices (by changing the terms of this Notice) at any time as authorized by law. The changes will be effective immediately upon us making them. They will apply to all PHI we create or receive in the future, as well as to all PHI created or received by us in the past (i.e. to PHI about you that we had

before the changes took effect). If we make changes, we will post the changed Notice, along with its effective date, in our office and on our website. Also, upon request, you will be given a copy of our current Notice.

Authorization Rule
We will not use or disclose your PHI for any purpose or to any person other than as stated in the rules above without your signature on our specifically worded, written Authorization / Acknowledgement Form (not a Consent or an Acknowledgement). If we need your Authorization, we must obtain it via a specific Authorization Form, which may be separate from any Authorization / Acknowledgement we may have obtained from you. We will not condition your treatment here on whether you sign the Authorization (or not).

Marketing and Fund Raising Rules

Limitations on the disclosure of PHI regarding Remuneration
The disclosure or sale of your PHI without authorization is prohibited. Under the new HIPAA Omnibus Rule, this would exclude disclosures for public health purposes, for treatment / payment for healthcare, for the sale, transfer, merger, or consolidation of all or part of this facility and for related due diligence, to any of our Business Associates, in connection with the business associate's performance of activities for this facility, to a patient or beneficiary upon request, and as required by law. In addition, the disclosure of your PHI for research purposes or for any other purpose permitted by HIPAA will not be considered a prohibited disclosure if the only reimbursement received is "a reasonable, cost-based fee" to cover the cost to prepare and transmit your PHI which would be expressly permitted by law. Notably, under the Omnibus Rule, an authorization to disclose PHI must state that the disclosure will result in remuneration to the Covered Entity.

Limitation on the Use of PHI for Paid Marketing
We will, in accordance with Federal and State Laws, obtain your written authorization to use or disclose your PHI for marketing purposes, (i.e.: to use your photo in ads) but not for activities that constitute treatment or healthcare operations. To clarify, ***Marketing*** is defined by HIPAA's Omnibus Rule, as "a communication about a product or service that encourages recipients . . . to purchase or use the product or service." A communication is not considered "marketing" if it is in writing and if we do not receive direct or indirect remuneration from a third party for making the communication.

Under Omnibus Rule we will obtain your written authorization prior to using your PHI for making any treatment or healthcare recommendations, should financial remuneration for making the communication be involved from a third party whose product or service we might promote (i.e.: businesses offering this facility incentives to promote their products or services to you). This will also apply to our Business Associate who may receive such remuneration for making a treatment or healthcare recommendations to you.

We must clarify to you that financial remuneration does not include "in-kind payments" and payments for a purpose to implement a disease management program. Any promotional gifts of nominal value are not subject to the authorization requirement.

The Privacy Rule expressly excludes from the definition of "marketing" refill reminders or other communications about a drug or biologic that is currently being prescribed for you, provided that the financial remuneration received by us in exchange for making the communication, if any, is reasonably related to our cost of making the communication. Face-to-face marketing communications, such as sharing with you, a written product brochure or pamphlet, is permissible under current HIPAA Law.

Flexibility on the Use of PHI for Fundraising
Under the HIPAA Omnibus Rule, covered entities were provided more flexibility concerning the use of PHI for fund raising efforts. However, we will offer the opportunity for you to "opt out" of receiving future fundraising

communications. Simply let us know that you want to "opt out" of such situations. There will be a statement on your ***HIPAA Patient Acknowledgement Form*** where you can choose to "opt out". Our commitment to care and treat you will in no way effect your decision to participate or not participate in our fund raising efforts.

Improvements to Requirements for Authorizations Related to Research
Under HIPAA Omnibus Rule, we may seek authorizations from you for the use of your PHI for future research. However, we would have to make clear what those uses are in detail.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

If you received this Notice via email or website, you have the right to get, at any time, a paper copy by asking our Privacy Officer. Also, you have the following additional rights regarding PHI we maintain about you:

To Inspect and Copy
You have the right to see and get a copy of your PHI including, but not limited to, medical and billing records by submitting a written request to our Privacy Officer. Original records will not leave the premises, will be available for inspection only during our regular business hours, and only if our Privacy Officer is present at all times. You may ask us to give you the copies in a format other than photocopies (and we will do so unless we determine that it is impractical) or ask us to prepare a summary in lieu of the copies. We may charge you a fee not to exceed state law to recover our costs (including postage, supplies, and staff time as applicable, but excluding staff time for search and retrieval) to duplicate or summarize your PHI. We will not condition release of the copies on summary of payment of your outstanding balance for professional services if you have one). We will comply with Federal Law to provide your PHI in an electronic format within the 30 days, to Federal specification, when you provide us with proper written request. Paper copy will also be made available. We will respond to requests in a timely manner, without delay for legal review, or, in less than thirty days if submitted in writing, and in ten business days or less if malpractice litigation or pre-suit production is involved. We may deny your request in certain limited circumstances (i.e. we do not have the PHI, it came from a confidential source, etc.). If we deny your request, you may ask for a review of that decision. If required by law, we will select a licensed health-care professional (other than the person who denied your request initially) to review the denial and we will follow his or her decision.

To Request Amendment / Correction
If you think PHI we have about you is incorrect, or that something important is missing from your records, you may ask us to amend or correct it (so long as we have it) by submitting a **"Request for Amendment / Correction"** form to our Privacy Officer. We will act on your request within 30 days from receipt but we may extend our response time (within the 30-day period) no more than once and by no more than 30 days, or as per Federal Law allowances, in which case we will notify you in writing why and when we will be able to respond. If we grant your request, we will let you know within five business days, make the changes by noting (not deleting) what is incorrect or incomplete and adding to it the changed language, and send the changes within 5 business days to persons you ask us to and persons we know may rely on incorrect or incomplete PHI to your detriment. We may deny your request under certain circumstances (i.e. it is not in writing, it does not give a reason why you want the change, we did not create the PHI you want changed (and the entity that did can be contacted), it was compiled for use in litigation, or we determine it is accurate and complete). If we deny your request, we will (in writing within 5 business days) tell you why and how to file a complaint with us if you disagree, that you may submit a written disagreement with our denial (and we may submit a written rebuttal and give you a copy of it), that you may ask us to disclose your initial request and our denial when we make future disclosure of PHI pertaining to your request, and that you may complain to us and the U.S. Department of Health and Human Services.

To an Accounting of Disclosures
You may ask us for a list of those who got your PHI from us by submitting a **"Request for Accounting of Disclosures"**

form to us. The list will not cover certain disclosures (i.e. PHI given to you, given to your legal representative, given to others for treatment, payment or health-care-operations purposes). Your request must state in what form you want the list (i.e. paper or electronically) and the time period you want us to cover, which may be up to but not more than the last six years. If we maintain your PHI in an electronic health record, then we must provide you with routine disclosures of PHI, including disclosures of treatment, payment or healthcare operations, for the 3-year period prior to the date of the request. If you ask us for this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee to respond, in which case we will tell you the cost before we incur it and let you choose if you want to withdraw or modify your request to avoid the cost.

To Request Restrictions

You may ask us to limit how your PHI is used and disclosed (i.e. in addition to our rules as set forth in this Notice) by submitting a written **"Request for Restrictions on Use, Disclosure"** form to us (i.e. you may not want us to disclose your surgery to family members or friends involved in paying for our services or providing your home care). If we agree to these additional limitations, we will follow them except in an emergency where we will not have time to check for limitations. Also, in some circumstances we may be unable to grant your request (e.g. we are required by law to use or disclose your PHI in a manner that you want restricted).

To Request Alternative Communications

You may ask us to communicate with you in a different way or at a different place by submitting a written **"Request for Alternative Communication"** Form to us. We will not ask you why and we will accommodate all reasonable requests (which may include: to send appointment reminders in closed envelopes rather than by postcards, to send your PHI to a post office box instead of your home address, to communicate with you at a telephone number other than your home number). You must tell us the alternative means or location you want us to use and explain to our satisfaction how payment to us will be made if we communicate with you as you request.

To Complain or Get More Information

We will follow our rules as set forth in this Notice. If you want more information or if you believe your privacy rights have been violated (i.e. you disagree with a decision of ours about inspection / copying, amendment / correction, accounting of disclosures, restrictions or alternative communications), we want to make it right. We never will penalize you for filing a complaint. To do so, please file a formal, written complaint within 180 days with:

The U.S. Department of Health & Human Services
Office of Civil Rights
200 Independence Ave., S.W.
Washington, DC 20201
877.696.6775

Or, submit a written Complaint form to us at the following address:

Our Privacy Officer: _____ Office Name: _____
Office Address: _____
Office Phone: _____ Ext.:_____ Office Fax: _____
Email Address: _____

You may get your **"HIPAA Complaint"** form by calling our privacy officer.

These privacy practices are in accordance with the original HIPAA enforcement effective April 14, 2003, and undated to Omnibus Rule effective September 23, 2013 and will remain in effect until we replace them as specified by Federal and/or State Law.

OPTIONAL RULES FOR NOPP

NOTICE OF PRIVACY PRACTICES

Faxing and Emailing Rule
When you request us to fax or email your PHI as an alternative communication, we may agree to do so, but only after having our Privacy Officer or treating doctor review that request. For this communication, our Privacy Officer will confirm that the fax number or email address is correct before sending the message and ensure that the intended recipient has sole access to the fax machine or computer before sending the message; confirm receipt, locate our fax machine or computer in a secure location so unauthorized access and viewing is prevented; use a fax cover sheet so the PHI is not the first page to print out (because unauthorized persons may view the top page); and attach an appropriate notice to the message. Our emails are all encrypted per Federal Standard for your protection.

Practice Transition Rule
If we sell our practice, our patient records (including but not limited to your PHI) may be disclosed and physical custody may be transferred to the purchasing healthcare provider, but only in accordance with the law. The healthcare provider who is the new records owner will be solely responsible for ensuring privacy of your PHI after the transfer and you agree that we will have no responsibility for (or duty associated with) transferred records. If all the owners of our practice die, our patient records (including but not limited to your PHI) must be transferred to another healthcare provider within 90 days to comply with State & Federal Laws.

Inactive Patient Records
We will retain your records for a minimum of six years from your last treat-ment or examination (unless a longer period is required by state law), at which point you will become an inactive patient in our practice and we may destroy your records at that time (but records of inactive minor patients will not be destroyed before the child's eighteenth birthday). We will do so only in accordance with the law.

Collections
If we use or disclose your PHI for collections purposes, we will do so only in accordance with the law.

For the Office of:

_____

PATIENT ACKNOWLEDGEMENT FORM FOR RECEIPT OF NOTICE OF PRIVACY PRACTICES CONSENT

You may refuse to sign this acknowledgement & authorization. In refusing we may not be allowed to process your insurance claims.

Date: _____ Patient Name: _____

HOW DO YOU WANT TO BE ADDRESSED WHEN SUMMONED FROM RECEPTION AREA:

❑ First Name Only ❑ Proper Surname ❑ Other _____

PLEASE LIST ANY OTHER PARTIES WHO ARE ACTIVELY INVOLVED IN YOUR HEALTH CARE AND WHO CAN HAVE ACCESS TO YOUR HEALTH INFORMATION: (This includes step parents, grandparents and any care takers who can have access to this patient's records):

Name: _____ Relationship: _____

Name: _____ Relationship: _____

I AUTHORIZE CONTACT FROM THIS OFFICE TO **CONFIRM MY APPOINTMENTS, TREATMENT & BILLING INFORMATION** VIA:

❑ Cell Phone Confirmation
❑ Text Message to my Cell Phone
❑ Home Phone Confirmation
❑ Email Confirmation
❑ Work Phone Confirmation
❑ **Any of the Above**

I AUTHORIZE **INFORMATION ABOUT MY HEALTH** BE CONVEYED VIA:

❑ Cell Phone Confirmation
❑ Text Message to my Cell Phone
❑ Home Phone Confirmation
❑ Email Confirmation
❑ Work Phone Confirmation
❑ **Any of the Above**

I APPROVE BEING CONTACTED ABOUT **SPECIAL SERVICES, EVENTS, FUND RAISING EFFORTS or NEW HEALTH INFO** on behalf of this Healthcare Facility via:

❑ Phone Message
❑ Text Message
❑ Email
❑ **Any of the Above**
❑ **None of the Above** (opt out)

In signing this HIPAA Patient Acknowledgement Form, you acknowledge and authorize, that this office may recommend products or services to promote your improved health. This office may or may not receive third party remuneration from these affiliated companies. We, under current HIPAA Omnibus Rule, provide you this information with your knowledge and consent.

The undersigned acknowledges receipt of a copy of the currently effective Notice of Privacy Practices for this healthcare facility. A copy of this signed, dated document shall be as effective as the original.

_____ _____

Please ***print*** name of Patient Please ***sign*** Patient / Guardian of Patient

_____ _____

Legal Representative / Guardian Relationship of Legal Representative / Guardian

OFFICE USE ONLY

As Privacy Officer, I attempted to obtain the patient's (or representatives) signature on this Acknowledgement but did not because:

❑ It was emergency treatment
❑ I could not communicate with the patient
❑ The patient refused to sign
❑ The patient was unable to sign because
❑ Other (please describe)_____

Signature of Privacy Officer _____

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION (PHI) & MEDICAL RECORDS to a THIRD PARTY

Date: _____ Name of patient making Request: _____

Name of Designated Party to receive records: _____

COMPLETE AS APPLICABLE:

1. Please send a copy of my records for the period from _____ [insert date] to _____ [insert date] (including information from other health-care providers that it may contain) to:

Name_____

Address _____

City _____ State _____Zip_____

The purpose of this Authorization is: _____

I understand that my records may be subject to re-disclosure by recipient(s) and will no longer be protected by the HIPAA Privacy Rules.

2. Please allow _____ to pick up a copy of my records (including information from other healthcare providers that it may contain).

- ❑ My entire Medical Record
- ❑ My recent Radiographs
- ❑ My recent Test Results
- ❑ Other _____

I specifically authorize this Healthcare Facility to disclose verbally, by mail, fax, encrypted or unencrypted email, the following types of PHI, if it is included in the records described in paragraph 1, above (initial where appropriate):

- ❑ HIV records (including HIV test results) and sexually transmissible diseases
- ❑ Alcohol and substance abuse diagnosis and treatment records
- ❑ Psychotherapy records / this serves as my signature release under Federal law
- ❑ Other / Specify: _____

This Authorization permits our Facility to use or disclose your Protected Health Information for purposes other than your treatment, payment to our Facility or the health care operations of our Facility. You have the right to revoke this Authorization by providing our Facility with written notice of revocation. The revocation will be effective upon receipt, except with respect to uses or disclosures made prior to receipt and in reliance upon this Authorization.

Our Facility cannot require you to sign this Authorization as a condition to the provision of services.

This Authorization shall expire on _____, 20_____, or one year after its effective date, whichever is sooner or unless it is revoked prior to the expiration date.

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

REQUEST FOR ALTERNATIVE COMMUNICATIONS

Return completed form to: Privacy Officer [insert address] _____

_____

Please note that we will not ask you why you are requesting alternative communications. Also, we may be unable to agree to accommodate your request (i.e. it is unreasonable, we do not have the technology, in an emergency). We may deliver your electronic request in the format you request, or if we do not have the software to accommodate that, in a similar electronic format. If we agree to your request, we will follow the instructions stated below until such time as you instruct us otherwise in writing. A signed, dated copy of this Request shall be as effective as the original.

COMPLETE AS APPLICABLE:

1. This request pertains to the records of _____
2. I am requesting the following alternative communications:
   - ❑ Appointment Reminder
   - ❑ Address
   - ❑ Telephone Contact
   - ❑ Email ContactFax Contact
   - ❑ Other _____

Send all written communications only to the following address:

_____

_____

_____

During business hours, contact me by telephone only at the following phone number(s):

Cell: _____

Home: _____

Other: _____

Please communicate with me only by: _____

Please communicate with me only at the following address:

_____

_____

_____

Change in Payment (explain): _____

Additional request(s): _____

Please accept this as a formal request for communication.

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

Describe what alternative communications were denied this _____ day of _____, 20 _____

_____

Describe what alternative communications were accepted this _____ day of _____, 20 _____

_____

RECORD RELEASE TO PATIENT

AUTHORIZATION FOR DISCLOSURE OF PROTECTED HEALTH INFORMATION (PHI) TO INCLUDE ***SUPER CONFIDENTIAL PHI*** DIRECTLY TO THE PATIENT

I,_____, [Name of Patient making Request], hereby request a copy of my health records for services provided from _____ [insert date] to _____ [insert date] and authorize _____, (hereafter collectively referred to as "this Healthcare Facility") to disclose a copy of my health records to me.

I prefer my records be sent to me in the following format, but understand that by law, the records can be sent in any electronic format similar if the format I desire is not available. I know this Healthcare Facility will supply me these records within 30 days of this request and will contact me should there be any reason they need to extend this time frame. I understand, by law this Healthcare Facility and request an extension for more time but, can only request an extension, once for an additional 30 days. The format which I prefer to receive my electronic records in is:

❑ Email a word document to (email address): _____

❑ Email a PDF copy to (email address): _____

❑ Fax a copy to (fax number): _____

❑ Send a hard copy to (address):_____

❑ I will pick up a copy on or after (date):_____

I specifically authorize this Healthcare Facility to disclose verbally, by mail, fax or unencrypted email, the following types of **super-confidential information** as stated in the NOPP (initial where appropriate):

❑ HIV records (including HIV test results) and sexually transmissible diseases _____

❑ Alcohol and substance abuse diagnosis and treatment records _____

❑ Psychotherapy records _____

❑ Not Applicable

A copy of this signed, dated Authorization shall be as effective as the original.

By Patient:_____ Date: _____
(Print name and sign)

Or

By Patient's Representative:_____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

Describe what alternative communications were denied this _____ day of _____, 20 _____

_____

Describe what alternative communications were accepted this _____ day of _____, 20 _____

_____

REQUEST TO INSPECT, COPY OR SUMMARIZE

Return completed form to: Name: _____
Address: _____
City, State: _____

Please note that we may deny your request to inspect, copy or summarize records if you are not the patient or the patient's legal representative, if we do not have the records, or in other circumstances. If we deny your request, you may ask us to review that decision. A signed, dated copy of this Request shall be as effective as the original.

COMPLETE AS APPLICABLE:

1. This request pertains to the records of _____.

2. ❑ I want to INSPECT IN PERSON the **entire medical record** (including clinical and billing information) from _____ [insert date] to _____ [insert date]

   ❑ I want to INSPECT IN PERSON **only the following** type of records _____ pertaining to dates of service from _____ [insert date] to _____ [insert date]

   - I wish to inspect the records from _____ am/pm to _____ am/pm on (date): _____
   - I will bring with me the following persons: _____ and I will provide a written authorization for release of PHI to such persons.
   - I agree that original records will not leave the premises and that Practice's Privacy Officer will be present at all times during the inspection. ❑ yes ❑ no.

3. I want a COPY of: ❑ entire medical record ❑ only the following records _____

   _____

   - I want the copy in the following format: ❑ hardcopies ❑ emailed copies ❑ other_____
   - The copy will be ready for pick up at _____, on (date): _____
   - I acknowledge I will pay costs in the amount of $_____ before the copy is released.

4. I want a SUMMARY of: ❑ entire medical record ❑ only the following records _____

   - The summary will be ready for pick up at _____ on _____.
   - I acknowledge I will pay costs in the amount of _____ before the summary is released.

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

1. Request denied because records were:
- ❑ Not in our possession (and we advised the patient where they were, if known)
- ❑ From a confidential source that would be revealed if records were disclosed to patient
- ❑ Other (describe) _____

2. Patient requested a review of the denial on _____. We have selected Dr. _____ to review our denial. If the reviewer is outside the practice, we have obtained a Business Associate agreement.

3. Upon review of our denial, Dr. _____'s recommendation was _____ .

4. Copy of records in format requested not provided because:
- Inappropriate Authorization
- Patient refused payment of copying charge
- Patient failed to pick up
- Other (describe) _____

5. Records released: to _____ on _____.
❑ In Person ❑ Summary ❑ Copy

REQUEST FOR AMENDMENT / CORRECTION

Return completed form to: Name: _____

Address: _____

City, State: _____

Please note that we may be unable to accommodate your request for amendment / correction under certain circumstances (e. g., you do not give a reason why you want the change, we did not create the record you want changed, it was compiled for use in litigation, or we find it is accurate and complete). A signed, dated copy of this Request shall be as effective as the original.

If we grant your request, we will let you know within 5 working days, make the changes by noting (not deleting) what is incorrect or incomplete and adding to it the changed language, and send the changes within 5 working days to persons you ask us to and persons we know may rely on (or already have) incorrect or incomplete information to your detriment.

If we deny your request, we will (in writing within 5 business days) tell you why and how to file a complaint with us or the U.S. Department of Health and Human Services if you disagree. Also, you may submit a written disagreement and instruct us to disclose this (as well as our rebuttal, if any) when we make future disclosures of your PHI.

COMPLETE AS APPLICABLE:

1. This request pertains to the records of _____.
2. The following records (list by date and describe) are incorrect:
3. The following language in the records described above is incorrect (state specific language you want changed):
4. The language is incorrect because:
5. The language should be changed to read as follows (state specific language you want added):
6. The records are missing the following important information:
7. State specific records and/or language you want added:
8. The following previously have received the incorrect records (state name, address and phone number):
9. Do you want us to give them a copy of the information after it is changed and an explanation of why you wanted it changed?
   - ❑ Yes
   - ❑ Yes, but not to (indicate name): _____
   - ❑ No

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

Changes that were accepted this _____ day of _____ , 20 _____

_____

Changes that were denied this _____ day of _____ , 20 _____

_____

REQUEST FOR RESTRICTIONS ON USE / DISCLOSURE

This form should be used only if you are requesting limitations on how we use and disclose your protected health information that are in addition to our rules as set forth in our Notice of Privacy Practices.

Return completed form to: Name: _____
Address: _____
City, State: _____

Please note that we may be unable to agree to additional limitations (i.e. if required or in emergency situations where it may be necessary). In signing this Request for Restrictions form, you understand the exceptions. If we agree to your request, we will follow the parameters of current HIPAA law and the limitations stated below until such time as you instruct us otherwise in writing. A signed, dated copy of this Request shall be as effective as the original.

COMPLETE AS APPLICABLE:

1. This request pertains to the records of _____.
2. Please do not disclose: _____
   (list type of information)
3. Please list to whom the limitation should apply: _____
   (list persons or entities prohibited)
4. Additional limitation(s) requested:_____

_____

By Patient:_____Date: _____
(Print name and sign)
Or
By Patient's Representative:_____Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

Date: _____ Describe what limitations were denied:_____

_____

Date: _____ Describe what limitations were accepted: _____

_____

Date: _____ Name of Business Associates notified of accepted limitations: _____

_____
_____
_____
_____

REQUEST FOR ACCOUNTING OF DISCLOSURES

Return completed form to: Name: _____

Address: _____

City, State: _____

Please note that we may deny your request for accounting of disclosures for the following reasons: If you are not the patient or the patient's legal representative. Please note that, unless we maintain your PHI in an electronic database, the accounting that we provide will not include disclosures made to you or your legal representative, made for purposes of treatment, payment or health-care-operations purposes, or as required by law. We do this in accordance with current HIPAA Law. A signed, dated copy of this Request shall be as effective as the original.

COMPLETE AS APPLICABLE:

1. Please provide me with an accounting of disclosures pertaining to the records of Patient Name: _____

   _____

2. Please include disclosures from these dates: Date from: _____ Date to: _____

3. Please provide me with the accounting in the following format:
   ❑ hardcopies ❑ CD-ROM ❑ email ❑ fax ❑ eCloud drop copy

4. Pick up is preferred. Date that I can pick up copies in the above listed format,
   On or after (date): _____

5. I acknowledge I will pay costs in the amount of $ _____ before the accounting will be released.

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

1. Request for accounting denied because of the following:

- ❑ Disclosures occurred more than six years before the date of the request
- ❑ Disclosures occurred prior to April 14, 2003
- ❑ Disclosures were for treatment, payment or health-care purpose
- ❑ Disclosures were made to patient or patient's legal representative
- ❑ Requesting party lacks legal authority
- ❑ Patient refused to pay costs

Please note that Federal law requires that all patient requests for PHI Requests made in writing must be delivered electronically within 30 days of receipt.

- ❑ Other: _____

2. Date: _____ List of disclosures released to patient: _____

Date: _____ Name of Business Associates notified of accepted limitations:

_____

_____

_____

_____

PROHIBITION ON RE-DISCLOSURE (HIV INFORMATION)

This information has been disclosed to you from records whose confidentiality is protected by HIPAA Law and applicable state law which prohibits you from making any further disclosure of such information without the specific written consent of the person to whom such information pertains, or as otherwise permitted by specific state law.

The individual must specifically authorize disclosure of super-confidential information; we will not disclose it unless authorized by the patient. If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with State and Federal Law that requires us to warn the recipient in writing that re-disclosure is prohibited.

PROHIBITION ON RE-DISCLOSURE (SUBSTANCE ABUSE / PSYCHOTHERAPY INFORMATION)

This information is confidential under state and federal law. Federal regulations (42 CFR §2.1 et seq.) prohibit any further disclosure without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations.

The individual must specifically authorize disclosure by initialing super-confidential information, we will not disclose it unless authorized by the patient. If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with state and federal law that requires us to warn the recipient in writing that re-disclosure is prohibited.

LIMITED HEALTH-CARE POWER OF ATTORNEY

— get notarized —

KNOW ALL MEN BY THESE PRESENTS, that _____ (Name of Mother) & _____ (Name of Father), (hereafter collectively referred to as Parents) are natural or adoptive parents of _____ (Name of Child), an un-emancipated minor (hereafter "Child") and do hereby jointly nominate, constitute and appoint: _____ (Name of Attorney) as their attorney in fact for the limited purpose of making health-care decisions (including but not limited to providing informed consent for medical treatment, surgical and diagnostic procedures and records privacy decisions) on behalf of Child.

Parents do hereby jointly give and grant unto said attorney in fact full power and authority to do and perform every act necessary, requisite or proper to be done in and about the premises as fully as they might or could do were they personally present, with full power of substitution and revocation, hereby ratifying and confirming all that said attorney shall lawfully do or cause to be done by virtue hereof, with the following limitations:

1. This limited power of attorney shall be effective only if:
   a) Parents are unable to make health-care decisions regarding Child; or
   b) neither parent can be immediately located by telephone at their places of residence or businesses, as follows: _____
2. Parents fully understand that this designation will permit the attorney in fact to make health-care treatment and informational privacy decisions on behalf of Child, and to provide, withhold, or withdraw consent on Child's behalf; to apply for public benefits to defray the cost of health care; and to authorize Child's admission to or transfer from a health-care facility.
3. If the attorney in fact is unwilling or unable to perform his or her duties, Parents designate as alternate attorney in fact:
   _____
4. This limited power of attorney is not intended to and shall not pre-empt the provisions of Federal HIPAA Omnibus Rule 2013, pertaining to, respectively, consent for emergency care and other persons who may consent to medical care or treatment of a minor.
5. This limited power of attorney shall remain in full force and effect until revoked in writing, dated and signed by Parents.
6. A copy of this signed, dated power of attorney shall be as valid as the original.

IN WITNESS WHEREOF, the undersigned have issued this limited power of attorney, effective stated below,

_____ _____

(Print Name of Parent) (Signature of Parent)

_____ _____

(Print Name of Parent) (Signature of Parent)

On this _____ day of _____, 20_____, before me personally appeared _____ and _____, to me personally known and known to me to be the persons described in and who executed the foregoing instrument and they duly acknowledged that they executed same.

_____

(Notary Public)

My Commission Expires:_____

PRIVACY COMPLAINT FORM INFORMATION

We will never penalize you for filing a complaint. Nor will we ever ask you to waive your right to complain. You are entitled to a copy of this form.

If you think we are not following our Notice of Privacy Practices in accordance with Omnibus Rule or the current HIPAA Federal and/or State Laws, or you disagree with a decision of ours about inspection, copying, amending and correcting, accounting of disclosures, or requests for restrictions and alternative communications, please ask to speak with our HIPAA Privacy Officer; file a formal written complaint within 180 days to: U.S. Department of Health & Human Services:

FIND THE OFFICIAL FORM & REGIONAL ADDRESSES AT:

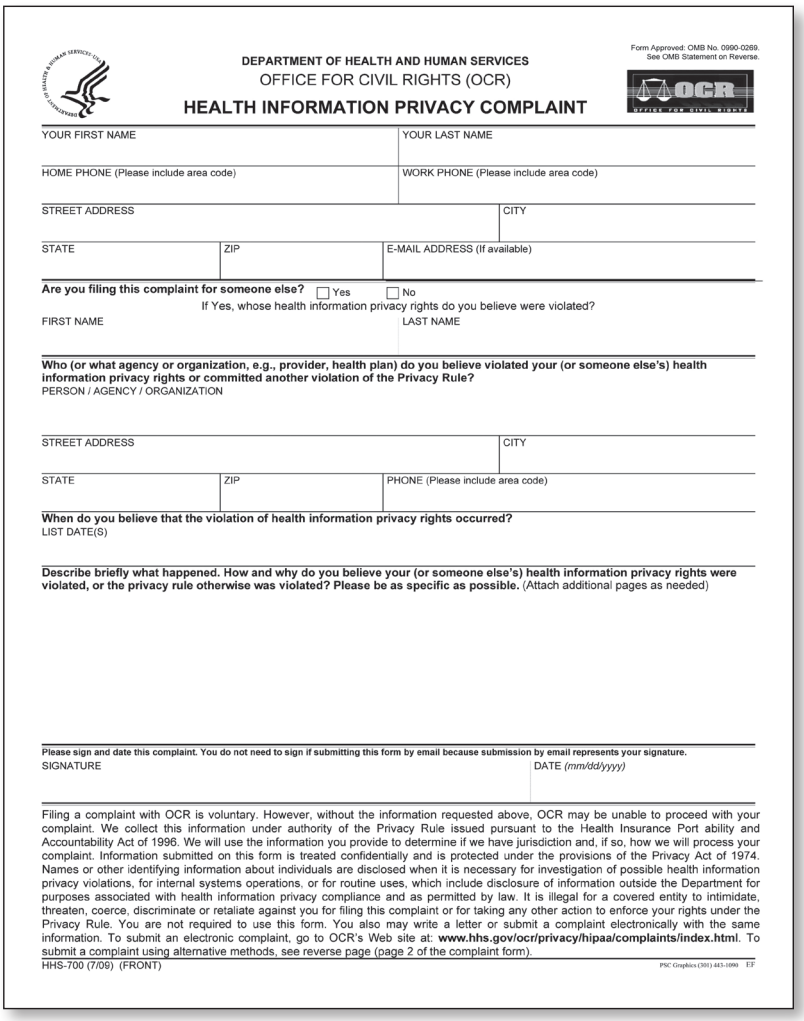
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

For more information you can also contact:

Office of Civil Rights
200 Independence Ave
S. W., Washington, D.C. 20201
877.696.6775

THIS IS A SAMPLE of the OFFICIAL FORM:



DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS (OCR)
HEALTH INFORMATION PRIVACY COMPLAINT

Form Approved: OMB No. 0990-0269.
See OMB Statement on Reverse.

YOUR FIRST NAME | YOUR LAST NAME

HOME PHONE (Please include area code) | WORK PHONE (Please include area code)

STREET ADDRESS | CITY

STATE | ZIP | E-MAIL ADDRESS (If available)

Are you filing this complaint for someone else? ☐ Yes ☐ No
If Yes, whose health information privacy rights do you believe were violated?
FIRST NAME | LAST NAME

Who (or what agency or organization, e.g., provider, health plan) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?
PERSON / AGENCY / ORGANIZATION

STREET ADDRESS | CITY

STATE | ZIP | PHONE (Please include area code)

When do you believe that the violation of health information privacy rights occurred?
LIST DATE(S)

Describe briefly what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the privacy rule otherwise was violated? Please be as specific as possible. (Attach additional pages as needed)

Please sign and date this complaint. You do not need to sign if submitting this form by email because submission by email represents your signature.
SIGNATURE | DATE *(mm/dd/yyyy)*

Filing a complaint with OCR is voluntary. However, without the information requested above, OCR may be unable to proceed with your complaint. We collect this information under authority of the Privacy Rule issued pursuant to the Health Insurance Port ability and Accountability Act of 1996. We will use the information you provide to determine if we have jurisdiction and, if so, how we will process your complaint. Information submitted on this form is treated confidentially and is protected under the provisions of the Privacy Act of 1974. Names or other identifying information about individuals are disclosed when it is necessary for investigation of possible health information privacy violations, for internal systems operations, or for routine uses, which include disclosure of information outside the Department for purposes associated with health information privacy compliance and as permitted by law. It is illegal for a covered entity to intimidate, threaten, coerce, discriminate or retaliate against you for filing this complaint or for taking any other action to enforce your rights under the Privacy Rule. You are not required to use this form. You also may write a letter or submit a complaint electronically with the same information. To submit an electronic complaint, go to OCR's Web site at: **www.hhs.gov/ocr/privacy/hipaa/complaints/index.html**. To submit a complaint using alternative methods, see reverse page (page 2 of the complaint form).
HHS-700 (7/09) (FRONT)

EMPLOYEE FORMS

Job Description for Privacy Officer

Job Description for Employees with Patient Health Information Access

Confidentiality and Non-Disclosure Agreement & Employee HIPAA Training Document (Team Sign-In Sheet)

- TO BE SIGNED BY EACH EMPLOYEE AND KEPT IN THEIR PERMANENT RECORD
- ALSO KEEP A COPY

Confidentiality and Non-Disclosure Agreement & Employee HIPAA Training Document (Individual Sign-In Sheet)

Employee Reprimand

Record of Disclosure Regarding Employee Behavior, Situation or Circumstances

- Signed by employee and HIPAA officer when HIV, Alcohol / Substance Abuse or Psycho- therapy information is disclosed

(Group Form) Employee Confidentiality Agreement of PHI in Accordance with OMNIBUS RULES *PLUS* EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAININ*G*

- This is a GROUP SIGN IN SHEET TO BE SIGNED BY EACH EMPLOYEE, THEN KEPT IN THE BACK OF THIS MANUAL BY APPROPRIATE YEAR OF TRAINING
- ALSO KEEP A COPY IN THE EMPLOYEES RECORD

(Individual Form) Employee Confidentiality Agreement of PHI in Accordance with OMNIBUS RULES

- This is an Individual Employee Form: YOU MAY CHOOSE TO HAVE SEPARATE CONFIDENTIALITY AGREEMENTS PER EACH EMPLOYEE. IF SO, KEEP ACOPY IN THEIR PERMANENT RECORD

HITECH Law Policy

Employee Technology Use Agreement

- Print and give each employee a form.
- As a team, place “checkmarks” in the top portion for the appropriate technology that you have operational in your dental office.
- Then, each employee should choose their “job title” then fill out that row of the table from left-to-right with checkmarks that apply to their job.
- Sign and date the form.
- Keep on file

JOB DESCRIPTION FOR PRIVACY OFFICER

- Acts as HIPAA Privacy Officer for this facility.
- Stays current on HIPAA Law and updates our privacy policies.
- Develops and implements privacy policies and procedures for the management of protected health information (PHI) in compliance with federal, state and local law, including but not limited to preparing the Notice of Privacy Practices to be distributed to patients and changes to the Notice.
- Ensures that all required *Employee Confidentiality Agreements* & *Proof of HIPAA Employee Training Sheets* are signed by employees and kept on file.
- Ensures that all Business Associates sign *Business Associates Agreements* to HIPAA Omnibus Standards. (Stored on file, in the Business Associate Agreement section of this manual)
- Trains employees who have access to protected health information (PHI) on privacy policies.
- Provides strategic guidance and periodically reports on privacy policies, to our employees and management.
- Designs a complaint system and resolves disputes over privacy violations.
- Assures the effectiveness of the privacy program, including but not limited to, monitoring and evaluating its implementation, making periodic revisions to meet practice needs, enforcing the policies when employees have access to PHI, investigating violations of the privacy standards, recommending appropriate discipline of employees and Business Associates.
- Monitors the activities of employees and Business Associates and promptly appraises our management of anticipated or actual violations of the privacy program.
- On a day-to-day basis, accepts overall responsibility to oversee compliance with the privacy policies.
- Ensures that proper documentation is created (i.e. acknowledgement, authorizations, revocations, amendments and corrections) and properly retained as necessary under HIPAA Records Retention Law.
- Analyzing possible breaches of confidentiality and carrying out appropriate notifications to patients and governmental agencies.

JOB DESCRIPTION FOR EMPLOYEES WITH PHI ACCESS

- Complies with this facilities' privacy policies and procedures for the management of protected health information (PHI).
- Understands the meaning and all verbiage on our Notice of Privacy Practices, HIPAA Patient Acknowledgement and other commonly used HIPAA Forms.
- Is able to explain and discuss with patients, the meaning of the top-ics covered within our Notice of Privacy Practices, HIPAA Patient Acknowledgement and other commonly used HIPAA Forms.
- Promptly contacts the Privacy Officer to resolve disputes over privacy violations or to address questions regarding compliance with privacy policies.
- Understands when PHI might be compromised and brings these situ-ations promptly to the attention of our HIPAA Compliance Officer.
- Understands how to initiate a breach inspection using the 4-Factor Breach Assessment Sheets located at the back of this manual. This will be managed by our HIPAA Compliance Officer.
- Understands that ignoring situations where PHI may have been potentially compromised comes with severe legal ramifications to both the practice and themselves.
- Is annually, or as needed updated with regard to compliance with privacy policies.
- Completes training on privacy policies within 30 days after being hired, or before being assigned new duties involving protected health information (PHI), or changes to the practices' privacy policies.
- Signs off on the employee documentation of HIPAA Privacy Training upon initial training and with each update.
- Signs off on HITECH Law training and complies when processing PHI, ePHI or ERH within the office while on the internet or with any other electronic communication.

HIPAA CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT *PLUS* EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAINING

THIS AGREEMENT entered into this_____ day of _____ , 20_____ , by and between _____ (name of Healthcare Facility), hereafter this "Healthcare Facility" and _____ (name of Employee), hereafter"Employee",sets forth the terms and conditions under which information created or received by or on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under state law and the Health Insurance Portability and Accountability Act of 1996 and updated through HIPAA Omnibus Rule of 2013 and will also uphold regulations enacted there under (hereafter "HIPAA").

THEREFORE, in consideration of the premises and the covenants and agreements contained herein, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. All parties acknowledge that meaningful employment may or will necessitate disclosure of confidential information by this Healthcare Facility to the Employee and use of confidential information by the Employee. Confidential information includes, but is not limited to, PHI, any information about patients or other employees, any computer log-on codes or passwords, any patient records or billing information, any patient lists, any financial information about this Healthcare Facility or its patients that is not public, any intellectual property rights of Practice, any proprietary information of Practice and any information that concerns this Healthcare Facility's contractual relationships, relates to this Healthcare Facility's competitive advantages, or is otherwise designated as confidential by this Healthcare Facility.

2. Disclosure and use of confidential information includes oral communications as well as display or distribution of tangible physical documentation, in whole or in part, from any source or in any format (e.g., paper, digital, electronic, internet, social networks like Facebook™ or social network posting, magnetic or optical media, film, etc.). The parties have entered into this Agreement to induce use and disclosure of confidential information and are relying on the covenants contained herein in making any such use or disclosure. This Healthcare Facility, not the Employee, is the records owner under state law and the Employee has no right or ownership interest in any confidential information.

3. Confidential information will not be used or disclosed by the Employee in violation of applicable law, including but not limited to HIPAA Federal and State records owner statute; this Agreement; the Practice's Notice of Privacy Practices, as amended; or other limitations as put in place by Practice from time to time. The intent of this Agreement is to ensure that the Employee will use and access only the minimum amount of confidential information necessary to perform the Employee's duties and will not disclose confidential information outside this Healthcare Facility unless expressly authorized in writing to do so by this Healthcare Facility. All Confidential information received (or which may be received in the future) by Employee will be held and treated by him or her as confidential and will not be disclosed in any manner whatsoever, in whole or in part, except as authorized by this Healthcare Facility and will not be used other than in connection with the employment relationship.

4. The Employee understands that he or she will be assigned a log-on code or password by Practice, which may be changed as this Healthcare Facility, in its sole discretion, sees fit. The Employee will not change the log-on code or password without this Healthcare Facility's permission. Nor will the Employee leave confidential information unattended (e.g., so that it remains visible on computer screens after the Employee's use). The Employee agrees that his or her log-on code or password is equivalent to a legally-binding signature and will not be disclosed to or used by anyone other than the Employee. Nor will the Employee use or even attempt to learn another

person's log-on code or password. The Employee immediately will notify this Healthcare Facility's privacy officer upon suspecting that his or her log-on code or password no longer is confidential. The Employee agrees that all computer systems are the exclusive property of Practice and will not be used by the Employee for any purpose unrelated to his or her employment. The Employee acknowledges that he or she has no right of privacy when using this Healthcare Facility's computer systems and that his or her computer use periodically will be monitored by this Healthcare Facility to ensure compliance with this Agreement and applicable law.

5. Immediately upon request by this Healthcare Facility, the Employee will return all confidential information to this Healthcare Facility and will not retain any copies of any confidential information, except as otherwise expressly permitted in writing signed by this Healthcare Facility. All confidential information, including copies thereof, will remain and be the exclusive property of this Healthcare Facility, unless otherwise required by applicable law. The Employee specifically agrees that he or she will not, and will not allow anyone working on their behalf or affiliated with the Employee in any way, use any or all of the confidential information for any purpose other than as expressly allowed by this Agreement. The Employee understands that violating the terms of this Agreement may, in this Healthcare Facility's sole discretion, result in disciplinary action including termination of employment and/or legal action to prevent or recover damages for breach. Breach reporting is imperative.

6. The parties agree that any breach of any of the covenants or agreements set forth herein by the Employee will result in irreparable injury to this Healthcare Facility for which money damages are inadequate; therefore, in the event of a breach or an anticipatory breach, Practice will be entitled (in addition to any other rights and remedies which it may have at law or in equity, including money damages) to have an injunction without bond issued enjoining and restraining the Employee and/or any other person involved from breaching this Agreement.

7. This Agreement shall be binding upon and ensure to the benefit of all parties hereto and to each of their successors, assigns, officers, agents, employees, shareholders and directors. This Agreement commences on the date set forth above and the terms of this Agreement shall survive any termination, cancellation, expiration or other conclusion of this Agreement unless the parties otherwise expressly agree in writing.

8. The parties agree that the interpretation, legal effect and enforcement of this Agreement shall be governed by the laws of the State in which the Healthcare Facility is located and by execution hereof, each party agrees to the jurisdiction of the courts of such State. The parties agree that any suit arising out of or relation to this Agreement shall be brought in the county where this Healthcare Facility's principal place of business is located.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have executed this Agreement on the date first above written, when signing below and after training on HIPAA Law with full understanding this agreement shall stand.

EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE PRIVACY TRAINING

The Health Insurance Portability Act of 1996 (HIPAA) requires our privacy officer to train employees on our health information privacy policies and procedures to the HIPAA Omnibus Standards of 2013 which also includes HITECH and Protected Health Information (PHI), Electronic Protected Health Information (ePHI) and Electronic Health Records (EHR). All employees with treatment, payment or healthcare operations responsibilities, which allow access to protected health information, are trained with updates periodically as State and Federal mandates require. HIPAA also requires that we keep this documentation (that the training was completed) for six years after the training.

I, the undersigned do hereby certify that I have received, read, understood and agree to abide by this Healthcare Facilities HIPAA Policies and Operating Procedures.

PRINTED NAME	SIGNATURE	DATE

HIPAA CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
TO HIPAA OMNIBUS RULE STANDARD

THIS AGREEMENT entered into this_____ day of _____ , 20_____ , by and between _____ (name of Healthcare Facility), hereafter this "Healthcare Facility" and _____ (name of Affiliate Person), hereafter "Affiliate Person", sets forth the terms and conditions under which information created or received by or on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under state law and the Health Insurance Portability and Accountability Act of 1996 and updated through HIPAA Omnibus Rule of 2013 and will also uphold regulations enacted there under (hereafter "HIPAA").

THEREFORE, in consideration of the premises and the covenants and agreements contained herein, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. All parties acknowledge that meaningful employment may or will necessitate disclosure of confidential information by this Healthcare Facility to the Affiliate Person and use of confidential information by the Affiliate Person. Confidential information includes, but is not limited to, PHI, any information about patients or other employees, any computer log-on codes or passwords, any patient records or billing information, any patient lists, any financial information about this Healthcare Facility or it's patients that is not public, any intellectual property rights of Practice, any proprietary information of Practice and any information that concerns this Healthcare Facility's contractual relationships, relates to this Healthcare Facility's competitive advantages, or is otherwise designated as confidential by this Healthcare Facility.

2. Disclosure and use of confidential information includes oral communications as well as display or distribution of tangible physical documentation, in whole or in part, from any source or in any format (e.g., paper, digital, electronic, internet, social networks like Facebook™ or social network posting, magnetic or optical media, film, etc.). The parties have entered into this Agreement to induce use and disclosure of confidential information and are relying on the covenants contained herein in making any such use or disclosure. This Healthcare Facility, not the Affiliate Person, is the records owner under state law and the Employee has no right or ownership interest in any confidential information.

3. Confidential information will not be used or disclosed by the Affiliate Person in violation of applicable law, including but not limited to HIPAA Federal and State records owner statute; this Agreement; the Practice's Notice of Privacy Practices, as amended; or other limitations as put in place by Practice from time to time. The intent of this Agreement is to ensure that the Affiliate Person will use and access only the minimum amount of confidential information necessary to perform the Affiliate Person's duties and will not disclose confidential information outside this Healthcare Facility unless expressly authorized in writing to do so by this Healthcare Facility. All Confidential information received (or which may be received in the future) by Affiliate Person will be held and treated by him or her as confidential and will not be disclosed in any manner whatsoever, in whole or in part, except as authorized by this Healthcare Facility and will not be used other than in connection with the Affiliate relationship.

4. The Affiliate Person understands that he or she will be assigned a log-on code or password by Practice, which may be changed as this Healthcare Facility, in its sole discretion, sees fit. The Affiliate Person will not change the log-on code or password without this Healthcare Facility's permission. Nor will the Affiliate Person leave confidential information unattended (e.g., so that it remains visible on computer screens after the Affiliate Person's use). The Affiliate Person agrees that his or her log-on code or password is equivalent to a legally-binding signature and will not be disclosed to or used by anyone other than the Affiliate Person. Nor will the Affiliate Person use or even attempt to learn another person's log-on code or password. The Affiliate Person immediately will notify this Healthcare Facility's privacy officer upon suspecting that his or her log-on code or password no longer is confidential. The Affiliate Person agrees that all computer systems are the exclusive property of Practice and will not be used by the Affiliate Person for any purpose unrelated to his or her employment. The Affiliate Person acknowledges that he or she has no right of privacy when using this Healthcare Facility's computer systems and that his or her computer use periodically will be monitored by this Healthcare Facility to ensure compliance with this Agreement and applicable law.

5. Immediately upon request by this Healthcare Facility, the Affiliate Person will return all confidential information to this Healthcare Facility and will not retain any copies of any confidential information, except as otherwise expressly permitted in writing signed by this Healthcare Facility. All confidential information, including copies thereof, will remain and be the exclusive property of this Healthcare Facility, unless otherwise required by applicable law. The Affiliate Person specifically agrees that he or she will not, and will not allow anyone working on their behalf or affiliated with the Affiliate Person in any way, use any or all of the confidential information for any purpose other than as expressly allowed by this Agreement. The Affiliate Person understands that violating the terms of this Agreement may, in this Healthcare Facility's sole discretion, result in disciplinary action including termination of Affiliation and/or legal action to prevent or recover damages for breach. Breach reporting is imperative.

6. The parties agree that any breach of any of the covenants or agreements set forth herein by the Affiliate Person will result in irreparable injury to this Healthcare Facility for which money damages are inadequate; therefore, in the event of a breach or an anticipatory breach, Practice will be entitled (in addition to any other rights and remedies which it may have at law or in equity, including money damages) to have an injunction without bond issued enjoining and restraining the Affiliate Person and/or any other person involved from breaching this Agreement.

7. This Agreement shall be binding upon and ensure to the benefit of all parties hereto and to each of their successors, assigns, officers, agents, employees, shareholders and directors. This Agreement commences on the date set forth above and the terms of this Agreement shall survive any termination, cancellation, expiration or other conclusion of this Agreement unless the parties otherwise expressly agree in writing.

8. The parties agree that the interpretation, legal effect and enforcement of this Agreement shall be governed by the laws of the State and by execution hereof, each party agrees to the jurisdiction of the courts of the State. The parties agree that any suit arising out of or relation to this Agreement shall be brought in the county where this Healthcare Facility's principal place of business is located.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have executed this Agreement on the date first above written, when signing below and after training on HIPAA Law with full understanding this agreement shall stand.

Date: _____

Print Witness Name: _____

_____

(Signature of Witness of Management / Healthcare Facility)

I, the undersigned do hereby certify that I have received, read, understood and agree to abide by this Healthcare Facilities HIPAA Policies and Operating Procedures.

Date: _____

Print Affiliate Person's Name: _____

_____

(Signature of Affiliate Person to Healthcare Facility)

EMPLOYEE HIPAA BREACH / REPRIMAND NOTICE

Employee Name: _____ Date of Notice: _____

Position Held: _____ Date of Hire: _____

TYPE of VIOLATION:

- ❑ Damage to Company Property / PHI
- ❑ Improper Behavior with PHI
- ❑ Unauthorized Performance / PHI
- ❑ Insubordination
- ❑ OSHA Violation endangering PHI
- ❑ HIPAA Violation
- ❑ Other _____

DESCRIPTION OF INCIDENT

Date: _____ Time: _____ ❑ am ❑ pm

Description: _____

_____

_____

_____

EMPLOYEE STATEMENT

- ❑ I agree with the described violation
- ❑ I disagree with the described violation

Explain _____

_____

_____

ACTIONS TO BE TAKEN

- ❑ Warning
- ❑ Probation
- ❑ Suspension
- ❑ Discharge
- ❑ Explain _____

_____

_____

Consequences should occurrence happen again

_____

I HAVE READ AND UNDERSTAND THIS EMPLOYEE WARNING NOTICE

_____ _____

Signature of Employee Date Signature of HIPAA Officer Date

RECORD OF DISCLOSURE REGARDING EMPLOYEE BEHAVIOR, SITUATION or CIRCUMSTANCES FOR COMPLETION AS APPLICABLE BY PRIVACY OFFICER ONLY

Date: _____

1. This accounting pertains to the records of _____
2. On the date stated above, the following records were disclosed (describe the information disclosed):

   _____

   _____

   _____

   _____
3. Check one: ❑ By Privacy Officer ❑ Business Associate
4. Name of Business Associate making disclosure:
   Name of Individual making disclosure: _____
5. Address, if known, of recipient: _____

   _____
6. For the purpose of: _____
7. This disclosure included the following type of super-confidential information and written prohibition on re-disclosure was provided to recipient(s) on this date:_____

   Check all that apply:

   ❑ HIV records (including HIV test results) and sexually transmissible diseases
   ❑ Alcohol and substance abuse diagnosis and treatment records
   ❑ Psychotherapy records
8. This disclosure was authorized under the Patient's Acknowledgement, Consent & Authorization. That authorization accompanies this form (See corresponding date).
9. This disclosure was authorized under the following State or Federal law.

   Check all that apply:

   ❑ Emergency
   ❑ Sexual or needle-sharing partner
   ❑ Research
   ❑ Crime, missing person, medical examiner
   ❑ Domestic violence
   ❑ Communicable disease / public health agency
   ❑ Malpractice defense
   ❑ Workers' compensation
   ❑ Other litigation
   ❑ Collections
   ❑ Marketing
   ❑ Other

List statute _____

Are Statues still in effect? ❑ yes ❑ no (IF NO, DO NOT MAKE DISCLOSURE)

Describe underlying circumstances:

_____

_____

_____

_____

10. Format of disclosure was:

_____

_____

_____

_____

- ❑ Hand delivery to: _____
- ❑ Postal service: Name of Service _____
- ❑ CD-ROM
- ❑ Jump Drive
- ❑ Email (with privacy notice)
- ❑ Facsimile (with privacy notice)
- ❑ Verbal

11. If Business Associate made unauthorized disclosure, describe discipline / mitigation and indicate date taken:

_____

_____

_____

_____

12. Accounting of disclosure—a copy of this form was given to _____ ,
❑ the patient ❑ the patient's legal representative (check one), as part of a requested accounting of disclosures, on:

(insert each date an accounting was provided):

Date: _____
Date: _____
Date: _____
Date: _____
Date: _____

HITECH LAW Policy
Risk Management Analysis
EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document I declare that I have been fully trained understand the materials and steps necessary to carry out and enforce the Risk Management Analysis Policies (HITECH LAW of 2010) and Practices for this facility. I will fully abide by these practices in accordance with our Administrator and Federal Law.

DATE	PRINT NAME	SIGNATURE

EMPLOYEE TECHNOLOGY USE AGREEMENT

EMPLOYEE TRAINING OPERATIONS, MAINTENANCE & PROTECTION for

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) & ELECTRONIC HEALTH RECORDS (EHR)

HIPAA ePHI is protected as follows at this location: (check ✓ the appropriate boxes below)

1. ***Electronically printed PHI*** (patient routing slips, daily schedules, credit card & payment receipts, insurance claims) will be protected by: ☐ **We Use a** SHREDDER ☐ NOT APPLICABLE ☐ We have a SHREDDING SERVICE
2. ***Electronic Insurance Claims*** will be protected by: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
3. ***Credit Card Transmitting of PHI***: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
4. E-mail ***Transmitting of digital radiographs & PHI***: ☐ We have Email Encryption Software in place: **Name of Software:** _____ ☐ Pre-Encryption Service in place ☐ NOT APPLICABLE
5. ***E-Tronic Confirmations*** to patients (text or email): ☐ We use an *eTronic Confirmation Service* that has ROUTER & FIREWALL with ENCRYPTION ☐ We call to confirm appointments and do not use the patients full name when confirming
6. ***Computer Terminals*** from which we enter PHI: ☐ Terminals have *Unique Passwords* (protected) ☐ We can initiate *HIPAA Privacy Mode in our Software* to obscure the Pt. "last name" when patients are present ☐ Microsoft Cor[illegible]t updated to ***OWS Ve[illegible]*** on a[illegible]mputers ☐ W[illegible]icrosoft.
7. **Telephone Answering [illegible]stem** is managed by: ☐ We have a Li[illegible]wering Servic[illegible] a signe[illegible] *HIPAA Bu[illegible]ss Asso[illegible]tes Agreement* [illegible] confidentiality ☐ [illegible]mployees To[illegible] F[illegible]warded Ca[illegible] Af[illegible] Hours; [illegible] employee[illegible]ave H[illegible]A training & sign[illegible] Confidentiality Agreement ☐ [illegible]e have a P[illegible]ne [illegible]mpany o[illegible]oic[illegible] Over IP[illegible]vice (VoIP) [illegible] We[illegible]e an Answering M[illegible]chine
8. Individuals ***cell phones*** [illegible] business conversations and/or[illegible]ng: ☐ [illegible]en texting[illegible]e *do[illegible]t use p[illegible]ents[illegible]l name* ☐ W[illegible]have an [illegible]crypt[illegible] Texti[illegible] Softw[illegible]e on al[illegible]
9. ***Faxed Documents***: ☐ W[illegible]se an[illegible]*ax-Encrypte[illegible]Fax Serv[illegible]e* with [illegible]ign[illegible] HIPAA[illegible]usiness [illegible]ociates Agreement[illegible] confidentiality ☐ W[illegible]do n[illegible]"Fax out" & o[illegible]ax ma[illegible]ine is u[illegible]e[illegible]anage[illegible]nt Supe[illegible]sion

HIPAA MAINTEN[illegible]CE & [illegible]OTECTIO[illegible] ELECTRO[illegible]C PHI fo[illegible]pecific JOB TITLE at [illegible]

Job Title: _____ Name: _____ Signature: _____ Date: _____

☐ I have been trained for my job-specific Texas HB 300 HIPAA PHI & ePHI requirements

IN THE COURSE OF MY JOB, I UNDERSTAND MY RESPONSIBLITIES FOR PROPERLY EXECUTING, MAINTAINING AND PROTECTING THE FOLLOWING:
(check ✓ the appropriate boxes below that pertain to your job):

MY JOB TITLE: ↓	I use Computer Terminal for Electronic Patient Chart / Treatment Entry	I use the Office Telephone re: Patient Info	I Use a Credit Card Payment Terminal	I use my Cell Phone for Texts, Emails & Calls Involving Pt. Info	I transmit Electronic Faxes w/ Patient info	I use Office Email Account w/: Patient info	I deploy Text Confirmations w/ Pt. Info	I discard Paper w/ Patient PHI via Shredder	I submit Electronic Insurance Claims via email or fax	I update Office Internet & Software
Doctor										
Dentist										
Pharmacist										
Chiropractor										
Dental Hygienist										
Dental Assistant										
Nurse										
Physical therapist										
Massage Therapist										
Physicians Assistant										
Office Manager										
Receptionist										

New Employees: Complete this employee document within **60 days** of hire. **Existing Employees**: should update document **once every (2) years**. Completion of this form fulfills our obligation for our Technology Use Agreement and how we handle our **ELECTRONIC HEALTH RECORDS (EHR)** & **PROTECTED HEALTH INFORMATION (PHI)** withinr this office, Please see our **HITECH PACKET** for more information **HIPAA OMNIBUS RULE CHANGES NEED TO BE TRAINED ON WITH YOUR TEAM IN A SEPARATE MODULE** REFERENCES: h p://www.nixonpeabody.com/publications_detail3.asp?ID=3915 www.HIPAA.org

OFFICE FORMS

Business Associate Agreement

Response to Records Request

Privacy Notice Fax Cover Sheet

Privacy Notice Email Cover Sheet

Prohibition of Re-Disclosure HIV

- Prohibits repeat disclosure

Prohibition of Re-Disclosure Alcohol, Substances & Psychotherapy

- Prohibits repeat disclosure

TAB: MEDICARE, MEDICAID & HEALTHY KIDS PROGRAMS

Affordable Care Act / Section 1557

- Healthcare Reimbursement Requirements

Non-Discrimination Notice for Medicaid / Medicare / Healthy Kids

15 Language Translation Statement for Section 1557 Medicaid Medicare

- Use this form for patients that require language translation by calling the HIPAA 800 # that has has translators "on-call" for translating treatment needs.

TAB: BREACH NOTICE POLICY & PROCEDURE

- Use to assess Breaches; Customize with your Office Name

TAB: BREACH ASSESSMENT FORMS (BLANK)

4-Factor Risk Assessment Forms

- Use to report breaches to HSS at: The Secretary of U. S. Department of Human Health Services using this electronic link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Major Breach Protocols also requires: *Report to Media:* Newspaper, Radio & TV; Notify media as a Press Release; This notice must be within 60 days of discovery of a Major HIPAA Breach & must include the same information required for the individual notice.

TAB: BREACH ASSESSMENT FORMS (DOCUMENTED)

HIPAA Omnibus Rule
BUSINESS ASSOCIATE AGREEMENT
"A Business Vendor Confidentiality Agreement"

This document is required to be signed by the Business Associate and maintained on file by Covered Entity to comply with Omnibus Rule of 2013, and Effective March 26, 2013. Signatures need to be made by:

September 23, 2013 for new Business Associates Agreements.
or, if after this date, at inception of the business date.
September 22, 2014 for Business Associate Agreements currently on-file. This new version needs to be signed and kept on-file.

BUSINESS VENDORS ARE URGED TO GET AND USE THEIR OWN SUB CONTRACTORS AGREEMENTS.

Term

The Term of this Agreement shall be effective as of _____**(Today's Date)**, and shall terminate upon the date that Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Healthcare Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. ***"Business Associate"*** shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean

_____ (Name of Business Vendor).

(b) Covered Entity. ***"Covered Entity"*** at 45 CFR 160.103, shall generally have the same meaning as the term "Our Office" in reference to the parties that sign this agreement,

_____ (Name of Covered Entity).

(c) HIPAA Rules. ***"HIPAA Rules"*** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate _____ **(Name of Business Vendor)** agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to Covered Entity any use or disclosure of PHI protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; The Business Associate, *will report these immediately or not more than 5 business days after such a discovery.*

The Business Associate *will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media*, on behalf of the Covered Entity *as its own breach*. Reporting is made to: HHS at this link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Make available PHI (protected health information) in a designated record set to the "Covered Entity" as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;

The Business Associate will respond to a request for access that the Business Associate receives directly from an individual for responsive business purpose, this will be either ***via email, (read-receipt option) and /or via registered mail, within 5 business days of a request.***

(f) The Business Associate will make any amendment(s) to PHI protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526; and:

The Business Associate will respond to a ***request for amendment*** when received directly from the individual either ***via email, (read-receipt option) and /or via registered mail, within 5 days*** of a request and the Business Associate will forward the individual's request to the Covered Entity ***with any amendments*** to the information in the designated record set will be incorporated.

(g) Maintain and make available the information required to provide an **accounting of disclosures** to the Covered Entity and also to the Individual, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;

The Business Associate will respond to a request for accounting of disclosures when received directly from the individual either via ***email, (read-receipt option) and /or via registered mail, either, within 5 days*** of a request ***and*** the Business Associate will ***forward the individual's request to the Covered Entity*** with any **Accounting of Disclosures** to the information in the designated record set will be incorporated.

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

(i) The Business Associate will make its internal practices, books, and records available to legal inspectors, The HHS and Covered Entity for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business Associate may only use or disclose PHI protected health information pertaining only to situations that deem it necessary to perform the services set forth in the Business Associates & Covered Entities governing Service Agreement/ Contract, as permitted by current HIPAA law.

In addition to other permissible purposes, the Business Associate is authorized to use PHI protected health information to ***de-identify the information*** in accordance with 45 CFR 164.514(a)-(c). The Business Associate may de-identify the information, permitted uses and disclosures by means legal and necessary to formulate this identity.

(b) Business Associate may use or disclose PHI protected health information as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI protected health information in timely and legal fashion consistent with Covered Entity's ***minimum necessary policies*** and procedures, which are defined as: the *least* use of information disclosure necessary to complete this task.

(d) Business Associate may not use or disclose PHI protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below:

(e) Business Associate may use PHI protected health information for the proper management and administration to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law and that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed. Notifications will be made to the all effected parties and required government offices of any instances in which the confidentiality of the PHI information has been breached.

(f) Business Associate may provide data aggregation services relating to the healthcare operations of the Covered Entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered Entity may notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI protected health information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI protected health information, to the extent that such changes may affect Business Associate's use or disclosure of PHI protected health information.

(c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI protected health information.

Permissible Requests by Covered Entity

Covered Entity ***shall not request*** Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity. The exception would be if the Business Associate will use or disclose PHI protected health information for, data aggregation or management and administration and legal responsibilities of the Business Associate.

Termination

(a) *Termination for Cause.* Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement (and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity).

(b) *Obligations of Business Associate Upon Termination.*

Business Associate shall retain no copies of the protected health information except to use or disclose PHI protected health information for its own management and administration or to carry out its legal responsibilities and the Business Associate needs to retain PHI protected health information for such purposes after termination of the agreement.

Upon termination of this Agreement for any reason, Business Associate, with respect to PHI protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that PHI protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity or destroy the remaining PHI protected health information that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information to prevent use or disclosure of the PHI protected health information, other than as provided for in this Section, for as long as Business Associate retains the PHI protected health information;
4. Not use or disclose the PHI protected health information retained by Business Associate other than for the purposes for which such PHI protected health information was retained and subject to the same conditions set in the *Permitted Uses and Disclosures By Business Associate sections (e) and (f) of this document*, applied prior to termination; and
5. Return to Covered Entity or destroy the PHI protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The Business Associate may be asked by the Covered Entity to transmit the PHI protected health information to another Business Associate of the Covered Entity at termination. The Business Associate would comply, confirm the transfer and then ensure the destruction of PHI protected health information created, received, or maintained by subcontractors.

(c) *Survival.* The obligations of Business Associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) *Amendment*. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law or law changes.

(b) *Interpretation*. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules by the Business Associates legal counsel.

This document was replicated from The Omnibus Rule model form is available at:
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
or
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html

BUSINESS ASSOCIATES
SIGNATURE PAGE—(RETAIN ON FILE)

THIS SIGNATURE PAGE—ADDENDUM (hereafter "Addendum") is entered into this _____ day of _____, 20_____, by and between _____ (hereafter "Business Associate") and _____ (hereafter "Healthcare Facility / Covered Entity), for themselves and their respective successors and assigns.

WHEREAS, the parties hereto desire to modify the aforementioned Agreement to set forth the terms and conditions under which information created or received by Business Associate on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under the Health Insurance Portability and Accountability Act "Omnibus Rule" of 2013 and regulations enacted thereunder (hereafter "HIPAA");

THEREFORE, both parties, for valuable consideration from each party to the other, the receipt and sufficiency of which is hereby acknowledged, do hereby mutually agree that the Agreement shall continue in full force and effect with the following modifications and additions, to wit: (additions or modifications state below, must comply with HIPAA Omnibus Rules):

_____

_____

_____

_____

_____

_____

_____

1. Except as amended by this Addendum, all terms, conditions and covenants of the Agreement are valid, shall remain in full force and effect, and hereby are ratified and confirmed.
2. Any inconsistencies between this Addendum and the Agreement shall be governed by this Addendum.
3. A copy of this Addendum shall be as effective as the original.

IN WITNESS WHEREOF, the parties hereto have entered into this Agreement as of the date first written above.

Name of Practice

_____
Signature

_____
Print name and title

Name of Business Associate (Vendor)

_____
Signature

_____
Print name and title

RESPONSE TO RECORDS REQUEST

Sent to:

Date: _____
Name: _____
Address: _____
City, State: _____

On _____(date), you submitted a request to us pertaining to the records of _____ (name of patient).

COMPLETE AS APPLICABLE:

1. We are ready to prepare the ❑ entire chart copy ❑ summary (check one) you requested in ❑ hardcopies ❑ emailed copies ❑ other _____ (check one). The cost for this service is $_____. Upon receipt of this charge, we will provide the requested records. Please contact our HIPAA Privacy Officer, _____ _____, to arrange a time to pick up the records. If you prefer, we will mail them to you. Please call to determine the additional postage cost and let us know where you want us to mail the records.
2. We are ready to provide you with access to inspect the records as you requested. Your appointment time if from _____ am/pm to _____ am/pm on _____ at _____. Please contact our HIPAA Privacy Officer at least 24 hours in advance if you will unable to make this appointment.
3. We are denying ❑ all ❑ some (check one), of your request as indicated below because:
   - ❑ We do not have the following records: _____
   - ❑ We believe you may obtain those records by contacting: _____
   - ❑ We do not know where you may obtain the records.
   - ❑ We cannot produce the copy or summary in the format you requested. Format we can deliver is: _____. Please contact our privacy officer if you would like paper copies.
   - ❑ We cannot give you access to the records because:
     - ❑ You lack authority under state law to access these records (i.e. the patient has not given you authority in writing, the written authority has been revoked, the records are super-confidential and you have only a general authority).
     - ❑ The information was given to us on a confidential basis and revealing the record would disclose the source of the information.
     - ❑ The information has been compiled in anticipation of litigation
     - ❑ The information is protected by the Clinical Laboratory Improvement Amendments of 1988 (42 U.S.C. 263a) or the Privacy Act (5 U.S.C. 552a).
     - ❑ A licensed health-care provider has determined, in the exercise of his or her professional discretion that disclosing the records would endanger the health or safety of you or another person.
     - ❑ Other: _____

If you disagree with our decision, you have the right to file a formal written complaint within 180 days with the ***U.S. Department of Health & Human Services.***

FIND THE OFFICIAL FORM AT: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf
Find Regional Addresses at: www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
Office of Civil Rights, 200 Independence Ave., S.W., Washington, D.C. 20201, 877.696.6775

Thank You,

_____
HIPAA Privacy Officer

PRIVACY NOTICE FOR FAX COVER SHEET

The documents accompanying this message may contain information that is privileged, proprietary, confidential or otherwise legally exempt from disclosure. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to protect the confidentiality of the information after its stated use has been fulfilled.

If you are not the intended recipient, you are hereby notified that any retention, disclosure, copying, distribution or action taken in reliance on the contents of these documents is strictly prohibited. If you have received these documents in error, please notify with a returned fax or call to our office and request to speak to our HIPAA Privacy Officer. Please arrange to return or destroy all copies of this message as per HIPAA Omnibus Rule. Federal Law demands the full cooperation of all parties involved in mitigating any breach of Protected Health Information (PHI).

If you have received this fax in error, please contact us at:

Office Name: _____
HIPAA Privacy Officer: _____
Phone Number: _____
Email Address: _____

PRIVACY NOTICE FOR EMAIL MESSAGES

Attach one of these to all of your office signature emails. . . .

DISCLOSURE:
This message is not intended to be a legally binding or legally effective electronic signature. The documents accompanying this message may contain information that is privileged, proprietary, confidential or otherwise legally exempt from disclosure. This information is intended only for the use of the individual or entity named above. The authorized recipient of this information is prohibited from disclosing this information to any other party and is required to protect the confidentiality of the information after its stated use has been fulfilled. If this is an email message that contains a forwarded message or is a reply to a prior message, some or all of the contents of this message or its attachments may not have been produced by the sender.

If you are not the intended recipient, you are hereby notified that any retention, disclosure, copying, distribution or action taken in reliance on the contents of these documents strictly is prohibited. If you have received these documents in error, please notify the sender immediately at the phone number, fax number or email address (as applicable and listed above) to arrange for their return and delete all copies of this message. This message is provided in accordance with the HIPAA Omnibus Rule of 2013.

Shorter version:

DISCLOSURE:
This message is intended only for the use of the individual(s) to whom it is addressed and contains information that is privileged, confidential, and exempt from disclosure under applicable law. Any further dissemination or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone or email as listed in our signature above. This message is provided in accordance with the HIPAA Omnibus Rule of 2013.

PROHIBITION OF RE-DISCLOSURE (HIV INFORMATION)

This information has been disclosed to you from records whose confidentiality is protected by HIPAA Law which prohibits you from making any further disclosure of such information without the specific written consent of the person to whom such information pertains, or as otherwise permitted by specific state law. A General Authorization for the release of medical or other information is NOT sufficient for this purpose.

The individual must specifically authorize disclosure by initialing super-confidential information; We will not disclose it unless authorized by the patient. If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with State and Federal Law that requires us to warn the recipient in writing that re-disclosure is prohibited.

PROHIBITION ON RE-DISCLOSURE (SUBSTANCE ABUSE / PSYCHOTHERAPY INFORMATION)

This information is confidential under state and federal law. Federal regulations (42 CFR §2.1 et seq.) and state law prohibit any further disclosure without the specific written consent of the person to whom it pertains, or as otherwise permitted by such regulations.

A General Authorization is NOT sufficient for this purpose.

The individual must specifically authorize disclosure by initialing super-confidential information; We will not disclose it unless authorized by the patient If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with state and federal law that requires us to warn the recipient in writing that re-disclosure is prohibited.

HIPAA HHS
Affordable Care Act: Section 1557
Healthcare Reimbursement Requirements

If your Healthcare facility gets government reimbursement for **Medicaid, Medicare Part C / Medicare Advantage** or **State Funded Healthy Kids Programs,** www.hhs.gov requires that you **post & use (2) Notices** within your practice:

- ✔ **A Non-Discrimination Notice**
- ✔ **Taglines: That reference Free Language Translation Assistance**

The US Department of Health & Human Services provides a free resource for you and translation in 15 languages. They list a **free phone number for each language** that may need translation.

You can search for this link by using the key words: **HHS—Language Assistance Services** or by following this link: http://www.hhs.gov/civil-rights/for-individuals/language-assistance/index.html

These NON-DISCRIMINIATION & TRANSLATION TAGLINES must Appear:

- ✔ **In your Office**
- ✔ **On your Website**
- ✔ **On Office Postcards & Brochures as a shorter version** (referencing your State's Top (2) Languages)

Sample materials are also available on HHS website: http://www.hhs.gov/civil-rights/for-individuals/section-1557/trainingmaterials/index.html

For more information, visit the OCR's website and search Section 1557

Please see pages 96A – 96C for:
15 Language Translation Statement for Section 1557 Medicaid Medicare

_____ (***Healthcare Facility Name***) complies with applicable Federal Civil Rights Laws and does not discriminate on the basis of race, color, national origin, age, disability, or sex.
_____ (***Healthcare Facility Name***) does not exclude people or treat them differently because of race, color, national origin, age, disability, or sex. We provide free aids and services to people with disabilities to communicate effectively with us, such as: HIPAA interpretation in written format, written information in large print, audio-accessible formats via www.HHS.gov 800#, electronic formats & hard copies.

We also comply with HIPAA Law to provide free HIPAA Translation to people whose primary language is not English. For language translation, in the top 15 common languages we will have you call: **800-752-0093**. Or please contact our **HIPAA Officer** for additional guidance on these translation links or other fore mentioned communication aids at the phone number listed below.

If you believe that _____ (***Healthcare Facility Name***) has failed to provide these services or discriminated in another way on the basis of race, color, national origin, age, disability, or sex, you can file a grievance with:

HIPAA Officer: _____
Office Name: _____
Office Address: _____
_____
Office Phone: _____
Office Fax: _____

You can also file a civil rights complaint with the U.S. Department of Health and Human Services, Office for Civil Rights, electronically through the Office for Civil Rights Complaint Portal, available at https://ocrportal.hhs.gov/ocr/portal/lobby.jsf , or by U.S. mail or telephone:

U.S. Department of Health and Human Services
200 Independence Avenue, SW Room 509F
HHH Building Washington, D.C. 20201
Phone: 800-368-1019 Fax: 800-537-7697
Language Translation Phone: 800-752-0093

Complaint forms are available at http://www.hhs.gov/ocr/office/file/index.html

Language Assistance Services for Individuals with Limited English Proficiency

Section 1557 Of The Affordable Care Act

We will take reasonable steps, in accordance with current HIPAA requirements, to provide free language assistance services to people who speak common languages that we are likely to hear within our practice and who don't speak English well enough to talk to us about the healthcare service we provide.

Translation of the above statement in:

Spanish: Tomaremos medidas razonables, de acuerdo con los requisitos actuales de HIPAA, para proporcionar servicios de asistencia lingüística gratuitos a las personas que hablan idiomas comunes que probablemente escuchemos en nuestra práctica y que no hablen el inglés lo suficientemente bien como para hablarnos sobre la atención médica. Servicio que brindamos.

French: Nous prendrons des mesures raisonnables, conformément aux exigences actuelles de la loi HIPAA, pour fournir des services d'assistance linguistique gratuits aux personnes qui parlent des langues communes que nous sommes susceptibles d'entendre dans notre cabinet et qui ne parlent pas suffisamment l'anglais pour nous parler des soins de santé. service que nous fournissons.

Italian:
Adotteremo misure ragionevoli, in conformità con gli attuali requisiti HIPAA, per fornire servizi di assistenza linguistica gratuiti a persone che parlano lingue comuni che probabilmente sentiremo all'interno della nostra pratica e che non parlano inglese abbastanza bene da parlarci della sanità servizio che forniamo.

French Creole (Haitian Creole):
Nou pral pran mezi rezonab pou bay sèvis asistans lang gratis pou moun ki pale lang nou pagen ide deyo ak ki pa pale angle byen ase pou pale ak nou sou swen nou ap bay.

German: In Übereinstimmung mit den aktuellen HIPAA-Anforderungen werden wir angemessene Schritte unternehmen, um Menschen, die gängige Sprachen sprechen und die wir wahrscheinlich in unserer Praxis hören werden, kostenlose Sprachassistenzdienste anzubieten, die nicht gut genug Englisch sprechen, um mit uns über die Gesundheitsversorgung zu sprechen Service, den wir anbieten.

Portegues: Tomaremos medidas razoáveis, de acordo com os requisitos atuais da HIPAA, para fornecer serviços gratuitos de assistência em idiomas para pessoas que falam idiomas comuns que provavelmente escutaremos em nossa prática e que não falam inglês o suficiente para conversar conosco sobre os cuidados de saúde. serviço que prestamos.

Croatian: Poduzimat ćemo razumne korake, u skladu s trenutnim zahtjevima HIPAA-e, pružiti besplatne usluge jezične pomoći osobama koje govore zajedničke jezike koje ćemo vjerojatno čuti u našoj praksi i koji ne govore dovoljno dobro engleski jezik da razgovaraju s nama o zdravstvenoj zaštiti usluge koje pružamo.

Greek:
Θα λάβουμε εύλογα μέτρα, σύμφωνα με τις ισχύουσες απαιτήσεις της HIPAA, για να παρέχουμε δωρεάν υπηρεσίες γλωσσικής βοήθειας σε άτομα που μιλούν κοινές γλώσσες που πιθανόν να ακούσουμε μέσα στην πρακτική μας και που δεν μιλούν αρκετά καλά αγγλικά για να μας μιλήσουν για την υγειονομική περίθαλψη υπηρεσιών που παρέχουμε.

Korean: 우리는 현재의 HIPAA 요구 사항에 따라 합리적인 조치를 취하여 우리가 실제로 듣고 싶어하는 공통 언어를 사용하는 사람들에게 무료 언어 지원 서비스를 제공 할 것이며 건강 관리에 관해 우리에게 충분히 이야기 할 수있는 영어를하지 못합니다 우리가 제공하는 서비스.

.

Albanian:
Ne do të ndërmarrim hapa të arsyeshëm, në përputhje me kërkesat e tanishme të HIPAA, për të ofruar shërbime të asistencës gjuhësore falas për njerëzit që flasin gjuhë të zakonshme që ne mund të dëgjojmë brenda praktikës sonë dhe që nuk flasin anglisht mjaft mirë për të folur me ne për kujdesin shëndetësor shërbim që ne ofrojmë.

Hindi: हम वर्तमान HIPAA आव यकताओं केअनुसार, सामान्य भाषा बोलने वाले लोगों को मु भाषा सहायता सेवाएं प्रदान करने केलिए उचित कदम उठाएंगे, जो कि हमारे अभ्यास केभीतर सुनने की संभावना है और जो स्वा य सेवाओं केबारे में हमसे बात करने केलिए पर्याप्त अंग्रेजी नहीं बोलते हैं सेवा हम प्रदान करते हैं।

Tagalog:
Magsasagawa kami ng mga makatwirang hakbang, alinsunod sa kasalukuyang mga kinakailangan ng HIPAA, upang magbigay ng mga serbisyo ng tulong sa libreng wika sa mga taong nagsasalita ng mga karaniwang wika na malamang na marinig natin sa loob ng aming pagsasanay at hindi mahusay na nagsasalita ng Ingles upang makipag-usap sa amin tungkol sa pangangalagang pangkalusugan serbisyo na ibinigay namin.

Japenese: 私たちは、現在のHIPAAの要件に従って、私たちが慣れ親しんでいると思う一般的な言語を話し、ヘルスケアについて私たちに十分話すことができない英語を話す人々に無料の言語支援サービスを提供する私達が提供するサービス。

Arabic:

سوف نتخذ خطوات معقولة ، وفقًا لمتطلبات
الحالية ، لتوفير خدمات مساعدة لغوية مجانية
للأشخاص الذين يتحدثون اللغات الشائعة التي من
المرجح أن نسمعها داخل ممارستنا والذين لا يتحدثون
الإنجليزية بشكل جيد للتحدث إلينا حول الرعاية
الصحية الخدمة التي نقدمها.

Polish: Podejmiemy uzasadnione kroki, zgodnie z aktualnymi wymaganiami HIPAA, aby świadczyć bezpłatne usługi pomocy językowej osobom znającym wspólne języki, które prawdopodobnie usłyszymy w naszej praktyce i które nie mówią po angielsku wystarczająco dobrze, aby porozmawiać z nami na temat opieki zdrowotnej. świadczone przez nas usługi.

Vietnamese: Chúng tôi sẽ thực hiện các bước hợp lý, theo các yêu cầu hiện tại của HIPAA, để cung cấp dịch vụ hỗ trợ ngôn ngữ miễn phí cho những người nói ngôn ngữ phổ biến mà chúng tôi có thể nghe trong khi thực hành và những người không nói tiếng Anh đủ tốt để nói chuyện với chúng tôi về chăm sóc sức khỏe dịch vụ chúng tôi cung cấp.

Chinese: 我们将根据当前的HIPAA要求采取合理措施，为在我们的实践中可能会听到的普通语言的人提供免费的语言协助服务，并且他们不会说英语，以便与我们讨论医疗保健我们提供的服务。

Russian: Мы предпримем разумные шаги в соответствии с текущими требованиями HIPAA, чтобы предоставить бесплатные услуги языковой помощи людям, которые говорят на общих языках, которые мы, вероятно, услышим в нашей практике, и которые недостаточно хорошо говорят по-английски, чтобы говорить с нами о здравоохранении Сервис, который мы предоставляем.

BREACH NOTIFICATION POLICY & PROCEDURES
PRACTICE NAME: _____

1. PURPOSE

The purpose of this Breach Notification Policy is to provide guidance to our employees at our office, (referred to within this document at "the Practice") when there is a breach an acquisition, access, use, or disclosure of the Practice's patients' unsecured protected health information in a manner not permitted under the Health Insurance Portability and Accountability Act of 1996 and HIPAA Omnibus Rules of 2013, its implementing rules and regulations, which compromises the security or privacy of the Protected Health Information (PHI) &Electronic Protected Health Information ePHI. HIPAA requires that we notify individuals whose unsecured PHI has been compromised by such a breach. In certain circumstances, when breaches involve more than 500 patient files have been compromised, the Practice must also report such breaches to the Secretary of HHS and through the media. Our breach notification process will be carried out in compliance with the Health Information Technology for Economic and Clinical Health Act of the American Recovery and Reinvestment Act of 2009 & HIPAA Omnibus Rules of 2013 and its implementing rules and regulations, each as may be amended from time to time, including those regulatory amendments of the Department of Health and Human Services published at 78 Fed. Reg. 5566 (Jan. 25, 2013), collectively "HIPAA."

2. DEFINITIONS

2.1 Breach. Breach means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information. Breach excludes:

2.1.1 Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under HIPAA.

2.1.2 Any inadvertent disclosure by a person who is authorized to access protection health information at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

2.1.3 A disclosure of protected health information where a covered entity

or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.2 Protected Health Information (PHI) (ePHI). Protected health information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

2.3 Unsecured Protected Health Information (Unsecured PHI). Unsecured PHI means any PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

2.4 Workforce. Workforce means employees, volunteers, trainees, and other persons under the direct control of the Practice, whether or not they are paid by the Practice.

3. POLICY AND PROCEDURES

In summary, HIPAA requires that covered entities notify individuals whose unsecured protected health information has been impermissibly accessed, acquired, used, or disclosed, compromising the security or privacy of the protected health information. The notification requirements apply to breaches of unsecured PHI & ePHI. In other words, if PHI is encrypted or destroyed in accordance with the HIPAA guidance, there is a "safe harbor" and notification is not required.

3.1 Discovery of Breach. A breach shall be treated as discovered as of the first day on which such breach is known to the Practice or, by exercising reasonable diligence, would have been known to the Practice or any person, other than the person committing the breach, who is a workforce member or agent of the Practice.

Workforce members who believe that patient information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify [list all as appropriate: his/her supervisor, the Practice administrator, the privacy officer, other].

Following the discovery of a potential breach, the Practice shall begin an investigation, conduct a risk assessment on our (4) Factor Risk Assessment Form found in our HIPAA MAnual, and, based on the results of the Risk Assessment, begin the process of notifying each individual whose PHI has been, or is reasonably believed by the Practice to have been, accessed, acquired, used, or

disclosed as a result of the breach. The Practice shall also begin the process of determining what notifications are required or should be made, if any, to the Secretary of the Department of Health and Human Services (HHS), media outlets, [optional: or law enforcement officials].

3.2 Breach Investigation. The Practice shall name an individual to act as the investigator of the breach (e.g., privacy officer, security officer, risk manager, other). The investigator shall be responsible for the management of the breach investigation, completion of the risk assessment, and coordinating with others in the Practice as appropriate (e.g., administration, security incident response team, human resources, risk management, public relations, legal counsel.) The Practice's entire workforce is expected to assist management in this investigation as requested. The investigator shall be the key facilitator for all breach notification processes.

3.3 Risk Assessment. For breach response and notification purposes, a breach is presumed to have occurred unless the Practice can demonstrate that there is a low probability that the PHI has been compromised based on, at minimum, the following risk factors (also see (4) Factor Risk Assessment Form in HIPAA Manual):

3.3.1 The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. Consider:
- 3.3.1.1 Social security numbers, credit cards, financial data
- 3.3.1.2 Clinical detail, diagnosis, treatment, medications
- 3.3.1.3 Mental health, substance abuse, sexually transmitted diseases, pregnancy

3.3.2 The unauthorized person who used the PHI or to whom the disclosure was made.
- 3.3.2.1 Does the unauthorized person have obligations to protect the PHI's privacy and security?
- 3.3.2.2 Does the unauthorized person have the ability to re-identify the PHI?

3.3.3 Whether the PHI was actually acquired or viewed.
- 3.3.3.1 Does analysis of a stolen and recovered device show that PHI stored on the device was never accessed?

3.3.4 The extent to which the risk to the PHI has been mitigated.
- 3.3.4.1 Can the Practice obtain the unauthorized person's satisfactory assurances that the PHI will not be further used or disclosed or will be destroyed?

The evaluation should consider these factors, or more, in combination to determine the overall probability that PHI has been compromised. The risk assessment should be thorough and completed in good faith, and the conclusions should be reasonable.

Based on the outcome of the risk assessment, the Practice will determine the need to move forward with breach notification. The investigator must document the risk assessment and the outcome of the risk assessment process. All documentation related to the breach investigation, including the risk assessment, must be retained for a minimum of six years.

3.4 Notification: Individuals Affected. If it is determined that breach notification must be sent to affected individuals, the Practice's standard breach notification letter (as modified for the specific breach) will be sent out to all affected individuals. The Practice also has the discretion to provide notification following an impermissible use or disclosure of PHI without performing a risk assessment, if the Practice so chooses. Notice to affected individuals shall be written in plain language and must contain the following information, which elements are included in the Practice's standard breach notification letter:

3.4.1 A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
3.4.2 A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved).
3.4.3 Any steps the individuals should take to protect themselves from potential harm resulting from the breach.
3.4.4 A brief description of what the Practice is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
3.4.5 Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, email address, website, or postal address.

This letter will be sent by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If the Practice knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

If there is insufficient or out-of-date contact information that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. If there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, by telephone,

or by other means. If there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of the Practice's website, or a conspicuous notice in major print or broadcast media in the Practice's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

Notice to affected individuals shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. If the Practice determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above. It is the responsibility of the Practice to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of any delay.

[A copy of all patient correspondence shall be retained by the Practice in accordance with state law record retention requirements.]

3.5 Notification: HHS. In the event a breach of unsecured PHI /ePHI affects 500 or more of the Practice's patients, HHS will be notified at the same time notice is made to the affected individuals, in the matter specified on the HHS website. If fewer than 500 of the Practice's patients are affected, the Practice will maintain a log of the breaches to be submitted annually to the Secretary of HHS no later than 60 days after the end of each calendar year, in the manner specific on the HHS website. The submission shall include all breaches discovered during the preceding calendar year.

3.6 Notification: Media. In the event the breach affects more than 500 residents of a state, prominent media outlets serving the state and regional area will be notified without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach. The notice shall be provided in the form of a press release. Copy of press release will be retained on file and include all pertinent information originally sent to effected individuals.

3.7 Delay of Notification Authorized for Law Enforcement Purposes. If a law enforcement official states to the Practice or a business associate that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Practice shall:

3.7.1 If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or

3.7.2 If the statement is made orally, document the statement, including the identify of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

This applies to notices made to individuals, the media, HHS, and by business associates.

3.8 Maintenance of Breach Information. The Practice shall maintain a process to record or log all breaches of unsecured PHI, regardless of the number of patients affected. The following information should be collected for each breach:

3.8.1 A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
3.8.2 A description of the types of unsecured protected health information that were involved in the breach (such as full name, social security number, date of birth, home address, account number, other).
3.8.3 A description of the action taken with regard to notification of patients regarding the breach.
3.8.4 Steps taken to mitigate the breach and prevent future occurrences.

3.9 Business Associate Responsibilities. The Practice's business associates shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach of unsecured PHI, notify the Practice of such breach. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been, accessed, acquired, used, or disclosed during the breach. The business associate shall provide the Practice with any other available information that the Practice is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of discovery of a breach, the Practice will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals. We will also clarify who is responsible for notification, cost of such, etc.

3.10 Workforce Training. The Practice shall train all members of its workforce on the Practice's policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the Practice. We train all employees on HIPAA Protocols at least annually. Reception Personal are trained more frequently as well as our HIPAA Officer.

3.11 **Complaints**. The Practice provides a process for individuals to make complaints concerning the Practice's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals also have the right to complain about the Practice's breach notification processes. [See our NOPP for complaint process & contact information/ HIPAA Officer.]

3.12 **Sanctions**. Members of the Practice's workforce who fail to comply with this policy shall be subject to disciplinary action, up to and including termination.

3.13 **Retaliation/Waiver**. The Practice may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for exercising his or her privacy rights. Individuals shall not be required to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

3.14 **Burden of Proof**. The Practice has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach.

(4)-Factor Breach Assessment Sheet for HIPAA Omnibus Rule PHI Breach Determination

(This file is also available on your training HIPAA On-Line Portal in the **Omnibus Rule eForms** folder)

Date of Incident: _____

Name of Patient at Risk: _____

Type of PHI breached:

❑ paper / mail ❑ email ❑ fax ❑ phone ❑ conversation ❑ visual ❑ theft ❑ hacking

❑ other, describe: _____

Brief description of incident: _____

_____

_____

Check "**Yes**" or "**No**" for the breached situation you are evaluating:

RISK FACTORS				
#1 PHI INVOLVED—Is this PHI likely to be identified and linked easily to the patient?				
SENSITIVE / HIGH RISK PHI: Includes any of these…			**Yes**	**No**
Name Address Email Address Full Face Photo Name with Lab Results	Phone Number Credit Card Number Web Address Finger Print	Social Security Number License Number Vehicle ID Medical Device ID		
#2 RECIPIENT of the PHI—Is recipient authorized to receive PHI? Examples of ***Safe Recipients:*** Doctor or Health Facility, Insurance Carrier of Patient, Pharmacy, Authorized Legal Representative, Our Employee, Our Business Associate, Our Business Associates Subcontractor, Our Patient			**Yes**	**No**
UNSAFE RECIPIENTS/HIGH RISK: Includes any of these… Un Known Stolen Hacked-Into Known but not Business Associate Known but not Patient			**Yes**	**No**
#3 PHI ACQUIRED / VIEWED—Was the PHI acquired & viewed?			**Yes**	**No**
Unsafe recipient received PHI			**Yes**	**No**
Safe recipient received & viewed PHI			**Yes**	**No**
#4 PHI MITIGATION **UNSAFE PHI: Includes any of these…** Not Traceable Not Retrievable UNABLE to mitigate Lost Stolen Hacked-Into			**Yes**	**No**
If the PHI *can be located and suppressed* it will be considered *diffused*. Locate by a: phone call, email, letter, text to confirm correspondence; PHI needs to be destroyed!			**Yes**	**No**

Since there are no "quantifiable parameters", we advise you to Report most everything

1 Yes = **Report this Breach**
2 Yes = **Report this Breach**
3 Yes = **Report this Breach**
4 Yes = **Report this Breach**
5 Yes = **Report this Breach**

Breaches of PHI need to be reported to:

The ***Secretary of U. S. Department of Human Health Services*** using this electronic link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Major Breach Protocols also requires: *Report to Media:* Newspaper, Radio & TV; Notify media as a Press Release; This notice must be within 60 days of discovery of a Major HIPAA Breach & must include the same information required for the individual notice.

OFFICE POLICIES

Data Backup and Contingency Planning Procedure

- Federal Requirement to have this written policy
- Fill in Dates on 1st page; Review and Date Annually

Our Annual Data Back-Up, Contingency & Operations Assessment Report

Risk Assessment Vulnerabilities Test / ePHI in Transit or at Rest Report

- Find this document in the back of this HIPAA Manual.

  Be sure to fill this out annually with your IT Tech)

HIPAA Red Flag Rule Packet

- Not a Federal Law; Recommended that you have a Fraud Protection Policy in Place

HIPAA HITECH Law Packet

- Federal Requirement as of February 2010. Fill in the blanks to customize this to your Office Protocols

Good Faith Estimate Law

- FAQs and related sample pages to implement Good Faith Policies within your office.

HIPAA Omnibus Rule Workbook Required Forms
(Turn to WORKBOOK TABLE OF CONTENTS for PAGE NUMBERS)

If you need additional guidance and help with implementing Omnibus Rule, do not be overwhelmed! We make the forms available in electronic format with our Omnibus Rule Training, available via our ***HIPAA UPDATE ON-LINE PORTAL.*** Contact us via email ticket or phone for your HIPAA Portal Access credentials.

Data Backup and Contingency Planning Procedure

Please fill in date implemented and updates for your facility:

Goal:

This document will serve as our back-up storage and contingency plan for the protection of **ePHI** (electronic Protected Health Information)* and **EHR**** (Electronic Health Records) HIPAA information. Because Health Information is continually being shared over internet and digital devices and from remote locations, we will ensure our business practices are in accordance with HIPAA Federal Standards and update these on a regular bases to keep up with advancing technology in the work force.

*Protected health information, or "PHI", is defined at 45 CFR § 160.103, which can be found on the OCR website at http://hhs.gov/ocr/hipaa.

** **Electronic Transactions and Code Sets Rule** — All covered entities should have been in compliance with the electronic transactions and code sets standard formats as of October 16, 2003.

In accordance with:

Privacy Rule 45 CFR § 164.530(c) that currently require covered entities to adopt certain safeguards for PHI as contained within this document.

"Security Standards for the Protection of Electronic Protected Health Information", HIPAA law ***45 CFR Part 160 and Part 164, Subparts A–E***. Commonly referred to as the Security Rule, was adopted to implement provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

All HIPAA **Covered Entities** must comply with the Security Rule. In general, the standards, requirements, and implementation specifications of HIPAA apply to the following covered entities: **Covered Health Care Providers** — Any provider of medical or other healthcare services or supplies who transmits any health information in electronic form in connection with a transaction for which HHS has adopted a standard.

PRIMARY LOCATION: (this office location)	**SECONDARY LOCATIONS:** Each sub-location will have their own HIPAA Manual and Policy
EFFECTIVE DATE of POLICY:	**PRIOR POLICY OR CROSS REFERENCE (if any):**
Date of Policy Review & Update:	**HIPAA Committee Approval:** Approved
Date of Policy Review & Update:	**Date Approved:** Same date as Effective
Date of Policy Review & Update:	
Date of Policy Review & Update:	

Scope of Procedure

The Business Procedures necessary to protect our ePHI & EHR to recover from an emergency, vandalism, system failure, accidental or natural disaster, technology and/or Federal updates will include:

1. Our Risk Analysis
2. Our Security Analysis
3. Data Back- Up
4. Disaster Recovery Planning
5. Emergency Mode/ Our Operation Plan

1) Our Risk Analysis

Our HIPAA Advisory Committee will review annually what current circumstances may be leaving us open to unauthorized access or disclosure of PHI. Policies will include:

- Our Software Operating System is maintained, updated, upgraded and tested annually to comply with current HIPAA standards
- Our Technical Safeguards include protection from Malicious Software in the form of Routers and Firewalls.
- We will update Patient HIPAA Acknowledgement forms for proper Guardian Access, we will ask patients to update this information when they are updating their annual Medical Histories.
- We will be sure our routers and firewalls are functioning and to Federal Standards.
- We will be sure our credit card companies are conducting security tests of our data as well as securing our ePHI to Federal Standard as they process it.
- We will use Business Associate Agreements and Employee Confidentiality Agreements to safeguard PHI and ePHI.
- We will review new laws and requirements and implement them.

The initial assessment revealed that all critical (to patient care) applications are functioning to standard at this time. Additional or changes can be added in an update.

2) Our Security Analysis

Our existing Security to protect ePHI, PHI and EHR consists of:

- Technical, Physical and Administrative Controls to include:
- Shredder for paper PHI.
- Employee Training & Confidentiality Agreements / Business Associate Agreements signed and filed in this HIPAA Manual.
- Locked office with alarm system and / or locked drawers / cabinets.
- Router and Firewall to Federal Standard
- Use of HIPAA complying banks and credit card companies.
- Keeping up-to-date with evolving HIPAA requirements.
- Updating our Patient Acknowledgment Forms for Guardian Access and other evolving information that may be required.
- Sharing current HIPAA Notice of Privacy Acts with concerned entities.
- Others as needed

3) Data Backup Plan

The following general plan is provided to describe our facility's backup procedures for computers storing ePHI and managed by our staff.

- Type of data: Our computers with professional software store critical PHI & EHR data and we have (to standard) off-site back up for recovery
- Off-Site storage: We have a contracted service to store our back –up data. Our data is encrypted and stored
  ❑ Off-Site ❑ On-Site
  This service provider has a signed Business Associate Agreement on file within this HIPAA Manual.
- Maintenance of Software and Computers: Our Internet Technology Engineer maintains our computer systems and would be called to intervene should there be an emergency. If our IT Tech is not a member of our Workforce, our IT Tech has a signed Business Associate Agreement on file within this HIPAA Manual. We will update and use systems in accordance with HIPAA Federal / State requirements.
  - Our Current Software System is: _____ Our Current Email Platform is: _____
    For Added Protection we have a: ❑ SSL ❑ Pre-Encryption Service (i.e.: Revenue Well or Smile Reminder)
    ❑ other _____

3) Contingency Planning Procedure

Testing for recovery: Requests for recovery of files from our back up provider service will be "a real-time test" of backup recovery. The backup procedures will be reviewed at the HIPAA Advisory Committee's annual, periodic assessment of HIPAA procedures in this facility.

4) Disaster Recovery Plan

Our Disaster Recovery Process, for purposes of ePHI protection and restoration, is as follows:

Emergency Procedures

Our facilitiy'sSafety & Emergency Plan is part of our general OSHA Manual. It contains the following responses:

- Notification for calling EMT or other help
- Emergency responses by our team
- Emergency assembly areas and communication guidelines
- Emergency safety procedures / Natural Disaster & Homeland Security Plan
- Illness and injury management procedures
- Location of emergency supplies

Regular evaluation drills and emergency power tests are conducted.

Computer Disaster Recovery Procedures would be a secondary procedure after human safety is secured and would be carried out by our practice owner, management or our HIPAA Officer, whoever is available at the time to complete this task.

Computer Disaster Recovery Procedures

a) Response by anyone, after attending to safety and any injury to patients and our team.

- Notify the appropriate Data Services:

Our Software Provider's Help Desk, Phone Number: _____

Our software provider: _____

Our IT Tech's Support Phone Number: _____

- Document treatment & billing information on paper for later data entry if patients are being treated.

b) Recovery

Assess the Availability & Capability of Personnel

Assess operational status and damage to:

Computers (power, Main Data Towers, Equipment, etc.)
Network Infrastructure (firewalls, switches, links, plugs)
Network Services
Servers (evaluate operational status, event logs)
Applications (evaluate operational status)
Data (perform database integrity checks, evaluate logs)

Formulate & execute recovery plan based upon damage assessed

Plan Staged Recovery with Support Techs
Restore vital network links and infrastructure as needed
Reconfigure servers as needed
Restore Applications and Data from Backup
Restore Secondary Services as needed
Reevaluate working condition of our Business

5). Emergency Mode Operation Plan

Emergency mode operation of Radiation Equipment requires calibrated treatment machines to be operating in a safe and effective manner as well as access to the electronic copy (or hardcopy) of patient radiographs. Try to ensure power or fuse boxes are off. Doctor or Management will check this.

Treatment Equipment Operation should be checked for damage. Try to ensure power or fuse boxes are off. Doctor or Management will check this.

Clinical Software Application & Information System should be checked for damage. Try to ensure power or fuse boxes are off. Doctor or Management will check this. Access to hardcopy of patient medical records should be checked.

Emergency mode operation will be reviewed (as necessary) at the annual meeting of the HIPAA Advisory Committee and revisions made to this document.

Our Annual Data Back-Up, Contingency & Operations Assessment Report

This report is to be filled out annually by our Data Management and IT Support team:

1. *Review of our Operation Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

2. *Review of our Risk Analysis*

   Date of Review: _____
   Evaluation reveals the need for: _____

3. *Review of our Security Analysis*

   Date of Review: _____
   Date of Review: _____
   Evaluation reveals the need for: _____

4. *Review of our Data Back- Up*

   Date of Review: _____
   Evaluation reveals the need for: _____

5. *Review of our Disaster Recovery Planning*

   Date of Review: _____
   Evaluation reveals the need for: _____

6. *Review of our Emergency Mode of Operations Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

BE SURE TO ALSO KEEP A CURRENT **WRITTEN RISK ASSESSMENT REPORT** IN ADDITION TO THIS REPORT

Risk Assessment Vulnerabilities Test / ePHI in Transit or at Rest
SAMPLE

The following table is part of our Risk Assessment for our facility and reviews devices that transmit ePHI or keep it at rest. It also indicates threats and vulnerabilities that could be susceptible from the environment, people or natural disasters. An Impact & Risk Rating is also included in this Assessment. Management and IT Support works to rectify all risks to keep our ePHI secure and up to current HIPAA Standards.

ePHI	Threat	Vulnerability	Precautions Taken	Likelihood	Impact	Risk
Pt Electronic Records	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls / Malware Software Updates	LOW	unlikely	LOW 1-2
Billing Software	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls /Malware Software Updates	LOW	unlikely	LOW 1-2
Scheduling	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls / Malware Software Updates	LOW	unlikely	LOW 1-2
Email	Hackers	Hacking Phishing Untrained Employees	IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Fax	Wrong Recipient	Untrained Employees	iFax IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Cloud Storage		Ha Ph	IT Services Firewalls / Malv oftware Upd nployee Tra		unlikely	
Computer Hard wear	Natural Disaster	ut da not pr cting Natural D ster	ervices walls / M ware ware U ates oyee ining	LOW	unlikely	LOW 1-2
Mobile devices	Loss Hacke	Outdated No Encrypti	Do t te PHI Use t cryptio rvice	LOW	unlikely	LOW 1-2
Website	Hack	IT not protec	IT Se Firew Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Laptops & Tablets	Hackers	Hacking Phishing Untrained Employees Theft	Encrypted Password protected Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Office Computers	Hackers	Break in Electrical Surge Flooding	Password Protected Malware / Firewalls Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Server	Theft	Break In Inside Tampering	Stored Remotely Employee Training & Updates to Training IT Services Antivirus Protection	LOW	unlikely	LOW 1-2

Threads could include: (ex. malware and hackers, outdated software, unintentional error, hardware failure, theft and loss, flooding),

Risk Assessment Vulnerabilities Test / ePHI in Transit or at Rest
OFFICE NAME: _____

The following table is part of our Risk Assessment for our facility and reviews devices that transmit ePHI or keep it at rest. It also indicates threats and vulnerabilities that could be susceptible from the environment, people or natural disasters. An Impact & Risk Rating is also included in this Assessment. Management and IT Support works to rectify all risks to keep our ePHI secure and up to current HIPAA Standards.

ePHI	Threat	Vulnerability	Precautions Taken	Likelihood	Impact	Risk
Pt Electronic Records						
Billing Software						
Scheduling						
Email						
Fax						
Cloud Storage						
Computer Hard wear						
Mobile devices						
Website						
Laptops & Tablets						
Office Computers						
Server						

Threads could include: (ex. malware and hackers, outdated software, unintentional error, hardware failure, theft and loss, flooding),

RED FLAG LAW

Training, Implementation & Sign-off Sheets

The RED FLAG LAW is a federally mandated law that must be in place and operating in your office by May 1, 2009. It is a prevention from IDENTITY THEFT for your patients who may opt to "make payments" for their healthcare treatment. Healthcare practices must review billing and payment procedures and know the law and how to enforce it. **Red Flag** simply means suspicious actions surrounding a patient's payment/ identification practices. For instance, they do not provide an authentic looking ID when opening an account with your office, or their credit card does not match their ID. Read on to learn the full intent of the law and how to abide.

KEY TERMS TO KNOW:

Creditor: Healthcare providers may be subject to the Rule if they are ***Creditors.*** Although you may not think of your practice as a Creditor in the traditional sense of a bank or mortgage company, the law defines Creditor to include any entity that regularly defers payments for goods or services or arranges for the extension of credit. For example, you are a Creditor if you regularly bill patients after the completion of services, including for the remainder of medical fees not reimbursed by insurance. Similarly, healthcare providers who regularly allow patients to set up payment plans after services have been rendered are Creditors under the Rule. Healthcare providers are also considered creditors if they help patients get credit from other sources—for example, if they distribute and process applications for credit accounts tailored to the healthcare industry.

"On the other hand, healthcare providers who require payment before or at the time of service are not Creditors under the Red Flags Rule. In addition, if you accept only direct payment from Medicaid or similar programs where the patient has no responsibility for the fees, you are not a creditor. Simply accepting credit cards as a form of payment at the time of service does not make you a creditor under HIPAA Rule.

Covered Account: Is defined as a consumer account that allows multiple payments or transactions or any other account with a reasonably foreseeable risk of identity theft. The accounts you open and maintain for your patients are generally 'covered accounts' under the law. If your organization or practice is a Creditor with ***'Covered Accounts,'*** you must develop a written identity Theft Prevention Program to identify and address the red flags that could indicate identity theft in those accounts."

Understanding Identity Theft… ***Identity Theft*** is fraud committed or attempted using the identifying information of another person without authority.

Identifying Information Is any name or number that may be used, alone or in conjunction with any other information, top identify a specific person, including any—

Name	Social Security number
Date of Birth	Official Driver's License
Identification Number	Alien Registration Number
Passport Number	Employer or Taxpayer Identification Number

Also, any **unique biometric data, such as:**

Fingerprint	Voice print
Retina or Iris Image	Other unique physical representation

Any **unique electronic identification number, such as:**

Address	Routing code
Telecommunication ID	Access Device (as defined in 18 U.S.C. 1029(e)).”’

By now, you are familiar with the *HIPAA Administrative Simplification Privacy and Security Rules*, note that these identifiers also are pertinent to the definition of protected health information in oral, written, or electronic formats.

Attached is the official ***Fighting Fraud with the Red Flag Rule Business Guide*** for an outline of a Four Step Process for compliance with the Red Flag rule. These steps (outlined below) are in more detail in the business guide. Please fill in the Red *Flag Rule Made Easy Worksheets* at the end of the official guide to make your office fully compliant.

FOUR STEP PROCESS FOR RED FLAG COMPLIANCE:

1. **Identify Relevant Red Flag** Identify the red flags of identity theft you’re likely to come across in your business.
2. **Detect Red Flag** Set up procedures to detect those red flags in your day-to-day operations.
3. **Prevent and mitigate identity theft** If you spot the red flags you’ve identified, respond appropriately to prevent and mitigate the harm done.
4. **Update your Program** The risks of identity theft can change rapidly, so it’s important to keep your Program current and educate your staff.

As a healthcare Covered Entity, you will note that these steps once completed, will take you to compliance for this new Red Flag Law. It will also be necessary to periodically update other HIPAA Security Rules. For more information, keep in close contact with HealthcareEnhancements.com or use these resources:
www.HIPAA.com www.ftc.gov/infosecurity

National Institute of Standards and Technology (NIST)
Special Publication 800-66 Revision 1 (October 2008),
which is available for download on HIPAA.com under “Security”.

** Excerpts from: Health Insurance Portability and Accountability Act (HIPAA) Security Rule, Ed Jones, Author & Healthcare Authority

Fraud-Prevention Guidelines in accordance with HIPAA and Red Flag Law

Office: _____ Date Implemented: _____

Listed below is our official procedure for Fraud-Prevention at this facility. These guidelines were developed in accordance and comply with HIPAA's Red Flag Law. All employees have been trained and agree to uphold the following courses of actions:

1. Relevant Red Flags in our Business:

- Fake ID (Driver's License, Passport, Credit cards, Insurance Cards)
- ID appears to be altered or forged
- No ID
- No address or proof-thereof
- Signature does not match IDs
- Social Security or Employee IDs do not match or exist
- Will not take a patient photo ID for our files
- Patient completes forms with mismatched info
- Patient cannot answer personal info without looking at IDs
- Patient leaves pertinent parts of application blank
- Soon after patient gives us info they want to CHANGE info associated with the account
- Credit card info that keeps changing—at repeated visits
- We receive *unauthorized* notices from credit card company or banking institution

2. Detect Red Flags:

- Reception Personal as well as Healthcare Providers will read and re-read info for inconsistencies and report any to each other.
- All new patients must provide a current ID that we can copy, inspect and keep in their record.
- All credit card and personal check paying patients will be asked to supply their matching ID.
- All Personal Checks will have to match ID on file.
- Suspicious candidates will be asked to have a seat in a private area and we will call credit card company or banking institution to verify authenticity.
- Such patients will be asked to pay in advance in cash at future appointments, unless matching IDs can be provided.
- Do a Google Search on said individual, check with police department or Department of Motor Vehicles.

3. Prevent & Mitigate:

- Close the account (depending on circumstance, open a new one).
- Report the account as improper to banking institution, credit card company and or police.
- Monitor the account for evidence of future foul play.

4. Update our Program: as needed

Fraud-Prevention Policy
ADMINISTRATOR'S APPROVAL

For the Office of: _____

Practice Name: _____

Doctor Name(s): _____

Address: _____

Phone: _____

Management Administrator: _____

As Management Administrator for this facility I, do hereby acknowledge, that all current employees have been thoroughly trained, have the proper knowledge to carry out the said Fraud Prevention Policies as stated above. This has been designed and will be carried out in accordance with HIPAA's Fraud-Prevention requirements and Red Flag Laws. [15 U.S.C. 1961a(e).], [16 C.F.R 603.2(a)], [817.5681(1)(a)], [41.90(d)(1)].

Date: _____

Print Name: _____

Signature: _____

RED FLAG Fraud-Prevention Policy
EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document, I declare that I have been fully trained understand the materials and steps necessary to carry out and enforce the Fraud-Prevention Policies and Practices for this facility. I will fully abide by these practices in accordance with our Administrator and Federal Law. This is a one time Employee Training,

DATE	PRINT NAME	SIGNATURE

HITECH LAW

Comprehensive Training & Risk Management Employee Certification +

Training, Implementation & Sign-off Sheets

THE HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT

HIPAA Required Security Risk Management Assessment Protocols Required as of 2010

EMPLOYEE TRAINING & HITECH OFFICE POLICIES

The healthcare industry is in the midst of sweeping changes. Internet information sharing has made Protected Health Information (PHI) vulnerable to many indiscretions. From disgruntled employees stealing patient info and maliciously posting it on the internet, to hackers stealing insurance ID information and misusing social security and credit card numbers, the breaches are serious and astounding. The federal government has recognized an immediate need for the way health records are managed. *The Health Information Technology for Economic and Clinical Health Act* (HITECH or "The Act"), of 2009 (ARRA), allowed a number of incentives to *encourage* the adoption of health information technology use. Electronic Health Record (EHR) systems among health care providers *has increased* but, this *diminishes privacy* and security regulations under (HIPAA). Now this electronic health information sharing will be subject to much *stricter* guidelines. It defines what incidents constitute a privacy breach and requires business associates and employees to comply with the Security Rule's *administrative, physical*, and *technical safeguard requirements.* The Act also requires accounting of disclosures to patients upon their request. Penalties under the new **Federal HIPAA Omnibus Rules, (enacted on September 23, 2013)** have HIPAA violations ranging from $10,000 to $1.5M per incident for businesses in non-compliance. Under the new Federal Laws, Employees become directly responsible for misconduct when using PHI to include jail time and up to $750,000 in personal fines. Penalties for malicious conduct with posting PHI on the internet (for example: on Facebook ™ or My Space™) will also result in jail time if traced back to the employee. Employers are no longer responsible for the misconduct of employees with regard to foul play on the net. As a result of this legislation, offices ***must have a Privacy Officer appointed to conduct Risk Management Analysis*** so that it may comply with the new "Breach of PHI Disclosure Notification Regulations" starting February 17, 2010.

As a result of this legislation, Healthcare Offices ***must have a Privacy Officer appointed to conduct Risk Management Analysis (at least annually)*** so that they may comply with the new "breach of PHI disclosure notification regulations" in accordance with both HITECH Standards, as well as, Federal HIPAA Omnibus Rules.

UNDERSTANDING PATIENT HEALTH INFORMATION RISK / DEFINITIONS

The duties of our Privacy Officer is first to understand definitions and concepts associated with private Protected Health Information (PHI), Risk Management, Confidentiality, Breaches in Information Confidentiality, Practices of the Employees to Ensure Privacy, Protocol for Notification if a breach occurs and keeping abreast of New Challenges with PHI. These are important definitions under the new guidelines:

A breach [USE THE DEFINITION OF BREACH CONTAINED IN SECTION II(o) on page 36]

We understand that Administrative, Technical and Physical Safeguards must be in place to protect PHI in our office. Follow this link to discover more about **Policy on Administrative, Technical and Physical Safeguards:** https://www.dhs.state.or.us/policy/admin/privacy/100_005.pdf

- **Administrative Safeguards** encompass how our PHI is to be handled and maintained in terms of bookkeeping and accounting. Protocols must be in place for ensuring privacy and taking seriously the ramifications of negligence, misuse or inappropriate use of PHI by our employees.
- **Technical Safegiards** will include encryption /web-keys, firewalls and password protection when using communication devices and the internet. There will be in place a way of authenticating communication with other entities. Encryption is abided by for sharing x-rays and other electronically shared PHI. A double-keying password system can ensure this and we will only work with software providers that allow us a way of authenticating digital signatures. Working with our I.T. Professional for these key security pathways is how we will accomplish and update these HIPAA security procedures. Our daily data backup will be stored off-site and encrypted and include protection against occurrences like catastrophes and disasters. Data will be accessible from an outside source so as to protect our business function and not expose our PHI. Wireless routers and Firewalls will be used to isolate PHI from the primary network. Again our I.T. Professional will update and advise us on best practices and safeguards as they evolve and need updating.
- **Physical Safeguards** involve the handling of our patient charts/ records, forms, x-rays and all applicable PHI. Private workstations will be kept secure and inaccessible to non-employees. There are lockdown procedures in place for logging in and out of practice management software when away from our stations and at the end of our work day.

REQUIRED WRITTEN PROCEDURES

We have this written set of HIPAA Security Procedures in accordance with HITECH as well as HIPAA Omnibus Rules, in place that address the following areas:

Breach Occurrences

This section lists possible breaches, how they will be handled and the risk of the breach occurring. This plan also states who has access to PHI, what kind of PHI can be accessible by an employee and for what purpose.

Balancing Test

Our Privacy Officer will develop and test that our office PHI procedures are secure and do not expose PHI to outside sources easily. We understand that, left untested, our office would be vulnerable to major business risks, whether from fraud, theft or simple errors that can compromise our patients' ePHI and PHI. Protected Health Information, whether electronic or paper, can be vulnerable to a breach in any of the following conditions: ***data in motion*** (data moving through a network); ***data at rest*** (data that resides in databases, file systems, and other structured storage methods); ***data in use*** (data in the process of being created, retrieved, updated, or deleted); or ***data disposed*** (discarded paper records or recycled electronic media). Our Information Security Risk Assessments can help us identify and keep controls in place to secure Protected Health Information (PHI) based on its data state. An Informational Security Risk Assessment will identify any gaps or inadequacies in our policies and procedures, and will

provide recommendations to protect sensitive patient and business information. Here's our step-by-step guide on how we perform a security assessment and what it includes: (We update this at least annually)

- Identify what is at risk
- Assess the risk
- Analyze risk control measures
- Making control decisions
- Implement risk controls
- Supervise and review
- Updating Policies and Procedures

Our Privacy Officer will provide training to all employees for both HB 300 and Federal HIPAA Rules. Such training will include:

- Definitions of PHI, ePHI & EHR
- Accountability for Confidentiality & Risks & Fines
- Legal Ramifications for Confidentiality Breaches
- What is considered a Breach
- Incident Response Program
- How to Prevent a Breach
- How Quickly We Must Deliver EHR upon Written Request from Patients

CONCLUSION

As the health care industry keeps evolving it is imperative to realize the importance of maintaining the integrity of our patient PHI, ePHI and EHR. We realize this and have designed ***this HIPAA HITECH Law Packet (HIPAA Secu-rity Rule)*** to seriously address and create safeguards for issues that can have severe implications with regards to handling our patient PHI whether paper or electronic. We understand that our Employer as well as individual Employees of our Practice can be held responsible for misconduct with ePHI and PHI. And ignorance of the law is not a defense. We will protect our office by filling-in the following written plan. All of our employees will be made aware of these procedures, their importance and implications for following the HIPAA HITECH Standards, as well as, Federal HIPAA Omnibus Rules.

BIBLIOGRAPHY

[1]] Jorge Rey, Information Security Manager at Kaufman, Rossin & Co, jrey@kaufmanrossin.com.
http://kaufmanrossin.mediaroom.com/index.php?s=43&item=121

[2] Ed Jones, Author & Healthcare Authority
http://www.hipaa.com/2009/05/the-definition-of-breach/

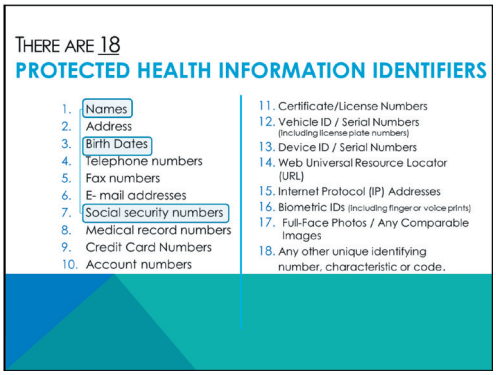
Risk Management Analysis
Our Written HITECH — HIPAA SECURITY RULE Guidelines
in accordance with HIPAA Omnibus Rules

Privacy Officer: _____ Date Implemented: _____

Facility Name: _____

Listed below is our official definitions and procedure for Risk Management Analysis at this facility. These guidelines were developed in accordance and comply with HIPAA's Health Information Technology for Economic and Clinical Health Act (HITECH) updated and revised to comply with HIPAA HITECH Standards & HIPAA Omnibus Rules. All employees have been trained and agree to uphold the following courses of actions:

1. DEFINITIONS ASSOCIATED WITH PHI:



PHI: Protected Health Information of our patients. There are 18 common Protected Health Identifiers which we may use day-to-day in our business activities.

EHR: Electronic Health Records are any patient PHI that we send or store on computers, phones, or electronic tablets or that can be transmitted via email or the internet.

ePHI: any Protected Health Information of the patient that is stored or sent electronically.

Employee Confidentiality: an understanding that encounters when Patients' Healthcare Information (PHI) can pose serious harm if handled improperly. Every employee can be subject to civil prosecution should their behavior with PHI be reckless or casual. All PHI must be handled with strict confidentiality, digression and care according to the guidelines set forth by this offices' Privacy Officer.

HIPAA Breach [Use the definition in Section II(o) on page 36] All breaches will be reported to the Privacy Officer who will report them to the HHS breach reporting link promptly. This link is made available from our computer desktop. Please reference the flow chart and risk analysis on page 39-40

Administrative, Technical and Physical Safeguards are in place

Administrative Safeguards would encompass how PHI is to be handled and maintained in terms of book-keeping and accounting. Protocols are to be in place for ensuring privacy and taking seriously the ramifications of negligence, misuse or inappropriate use of PHI.

Technical Safeguards would include encryption /wep-keys, firewalls, password protection and updated software to current HIPAA standards when using communication devices and the internet. We also authenticate communication with other entities. Software Encryption is in place for sharing x-rays, PHI and ePHI. A system of double-keying passwords is our test and we employ a method for authenticating digital signatures when needed. Speaking to an I.T. Professional for these key security pathways is updated at least annually. There is also a secure path for data backup which includes protection against occurrences like catastrophes and natural disasters; data is encrypted and accessible from an outside source. Our wireless router is isolated from our primary network. Again our I.T. Professional advises us on best practices and safeguards to comply with current HIPAA Standards and with regards to HIPAA Omnibus Rule Federal Laws.

Physical Safeguards involve the handling of patient charts, forms, x-rays and all applicable PHI. Private workstations keep PHI secure and inaccessible to non-employees. There are lockdown procedures in place for logging in and out of our practice management software when away from each station or at the end of the day.

Business Associate Agreement is a HIPAA contract between a given office and outside contracted individuals that create, access, use, disclose and/or store PHI in order to perform a function, service, or activity by or on behalf of this Office. Examples of Business Associate relationships include, but are not limited to, claims processing or administrative services; accreditation; data analysis; billing; legal services; consulting; software maintenance or support that includes access to PHI; and record storage or disposal services. Temporary workers or subcontractors working on premises will also sign a BAA. BAAs stay on-file within our HIPAA Manual.

2. ACCOUNTABILITY FOR CONFIDENTIALITY

All employees of this office have a full understanding of proper professional and legal behavior when encountering Patients' Protected Health Information (PHI). Detailed training has been provided to differentiate improper handling and when misuse may pose a threat, and that we need to deliver EHR to our patients, upon written request within 15 days. All employees, understand and agree to comply with policies set forth by management, HHS, to ensure proper handling and security of Patient Protected Health Information (PHI). Employees also understand that the mishandling of such information can lead to civil prosecution should they behave recklessly with such information. In signing a training affidavit, they pledge understanding and accountability to protect the confidential nature of all of this office's PHI.

3. LEGAL RAMIFICATIONS FOR CONFIDENTIALITY BREACHES

Employees understand that civil monetary penalties for HIPAA confidentiality violations are enforceable and that both the federal Office of Civil Rights and the State Attorney General enforces these rules through prosecution. Penalties for HIPAA violations can include jail time and civil monetary penalties.

4. OUR BREACH PROFILE / WHAT IS CONSIDERED A BREACH

This applies to information being transmitted to non-interested parties. An interested party might include a lab, specialist, other healthcare professional, approved legal entity or healthcare facility. Having patients sign documentation or a release form further ensure transmissions are permissible. Citing the general name of where transmissions go, can suffice for repeat transmission of such information. For instance, if a patient signs off that an office can file their claims to their insurance, that would grant permission. Transmission of PHI should not go to outside sources, onto internet sites or other entities that do not have proper clearance from your Privacy Officer. Electronic Claims submission should be with proper encryption and routing in place.

5. INCIDENT RESPONSE PROGRAM

Our office will not procrastinate with due diligence as it could relate to a possible breach. We will make every effort to ensure that PHI data is fully encrypted. We are aware that PHI data that isn't encrypted can increase the risk of unauthorized disclosure. This would apply to large amounts of information left open to exposure, not properly transmitted to a large insurance company for example. We will be sure our computer systems and wireless routers are working properly and are not at risk for compromise by continually using and maintaining our protective measures.

We are aware that The HITECH Act has a specific provision that discusses this issue. The breach notification provision states who must be notified if our records are compromised. In some cases, just the patients need to be notified; in others, it extends to various federal agencies and even the media. After the discovery of a breach, patients and

the Department of Health and Human Services will be notified via the governmental web-links.

We will be quick to respond to initial incidents and handle them before they escalate and coordinate response with I.T Professionals.

6. PREVENTING BREACHES

Our employees will all have proper training and be required to sign off on this training before having access to transmittable PHI. We will monitor the changes in law technology and physical characteristics in relation to the HITECH laws. Yearly our Privacy Officer will investigate, update and initiate any changes to keep our Risk Management Assessment program strong and secure. Employees involved in compromising practices with regard to PHI will be terminated and the incident reported to the proper authorities.

7. BREACH OCCURRENCES

This section must list possible breaches, how they will be handled and the risk of the breach occurring. This plan will also state who has access to PHI, what kind of PHI can be accessible by an employee and for what purpose. (We will add more as they apply to our office)

Risk Management Security Management Process—Security Rule: 164.308(a)(1)(ii)(B)

POSSIBLE BREACH	HOW TO HANDLE (always report breach via HHS link)	RISK of OCCURANCE	TEAM ACCESS (list)	PURPOSE
E Claims	Have manager call Insurance Co. and authorities	Slim	**INSURANCE CLAIMS COORDINATORS**	Filing Insurance
PHI Internet Listing	Terminate Employee	Rare	**ALL TEAM**	Malicious Intent
PHI Paperwork in wrong hands	Situational	Rare	**ALL TEAM**	Varies
Pt. Chart accessed	Re-claim immediately	Moderate	**ALL TEAM**	To view info
Workstation Access	Enforce password use at all times	Moderate	**ALL TEAM**	To view info
Credit Card Terminal	Investigate Improper Use	Rare	**RECEPTION TEAM**	Malicious Intent or Mistakes
Stolen/ Missing Device Server, Laptop, Drives	Call Police	Moderate	**ALL TEAM**	Malicious Intent Situational
Wrong Email, Text or Fax sent	Situational	Moderate	**ALL TEAM**	In Error

8. OUR BALANCING TEST

Risk Analysis/ Security Management Process—Security Rule: 164.308(a)(1)(ii)(A)

Identification of What is at Risk: Check the appropriate answers below:

1. File Cabinets containing Charts will be protected by ☐ LOCKED OFFICE ☐ LOCKED CABINETS ☐ NOT APPLICABLE
2. Discarded PHI Papers and forms will be protected by SHREDDER
3. Faxed copies of information will be protected by SHREDDER
4. Previously scanned documents will be protected by SHREDDER
5. Inactive Patient Charts will be protected by ☐ STORAGE ☐ COMPUTER BACK UP
6. Obsolete Patient Schedules will be protected by SHREDDER
7. Obsolete Patient Routing Slips will be protected by SHREDDER
8. Employee Workstations will be protected by PASSWORD
9. Employee Access to Internet NON-PROFESSIONAL ACTIVITY PROHIBITED
10. Employee Social Network Posting NON-PROFESSIONAL ACTIVITY PROHIBITED
11. Electronic Claim Submission will be protected by ☐ ROUTER & FIREWALL ☐ NOT APPLICABLE
12. Credit card Terminal Stations will be Protected by ☐ ROUTER & FIREWALL ☐ NOT APPLICABLE
13. Our Internal Database will be protected by DAILY BACK UP
14. Our Internet Server will be protected by ROUTER & FIREWALL
15. Daily Data Back-up will be protected by ☐ AUTOMATIC ☐ BACK-UP DRIVE OTHER: _____
16. Cell Phone Use / Texting Info will be protected by ☐ ENCRYPTION ☐ PHI NOT TRANSMITTED
17. Our Telephone Answering System will be protected by ☐ VOICE MAIL ☐ ANSWERING SERVICE ☐ MACHINE
18. Our eTronic Confirmation Service will be protected by ☐ SERVICE PROVIDER ☐ NOT APPLICABLE
19. Emailing Patient Information will be protected by ENCRYPTION
20. Receiving Emailed Patient Information will be protected by ENCRYPTION
21. Digital x-ray transmission will be protected by ☐ ENCRYPTION
22. Faxed Information to Patient, Doctor or Facility ☐ FAX to EMAIL ENCRYPTION ☐ NOT APPLICABLE
    ☐ WRITTEN MONITORED FAX PROTECTION PROGRAM

Other: _____

Other: _____

We have conducted an inventory of all the confidential electronic health records on file and are aware of what we have. We will do this annually.

Date: _____ Date: _____ Date: _____

Date: _____ Date: _____ Date: _____

9. ASSESSING OUR RISK

The following table illustrates what sort of risk tolerance our organization may be susceptible to, who may be involved and will allow us to plan our security strategy and protocols:

PHI SYSTEM	RISK FACTOR	All Team Access ✓ (check)	Limited Access ✓ (check)	Who has Access (list)
Copier	Team copying PHI for outside use	✓		
E Claims	Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	✓	✓	Insurance Coordinator
Internet	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	✓		
Work Station	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	✓		
E mail	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	✓		
Voicemail	Passwords used Passwords not used	✓		
Smart Phone Devises	Passwords used Passwords not used Encryption used Encryption not used	✓		
Website Access	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	✓		
Credit Card Terminals	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used		✓	Reception Team Others per Designation
Text	Encryption used No PHI Shared		✓	
Fax	Encryption used Encryption not used Passwords Fax-to-Email Conversion	✓		

10. ANALYSIS OF RISK CONTROL MEASURES

Making Controlled Decisions for Our Practice

After identifying and assessing the risks from above, we are now able to create specific solutions or risk controls that will eliminate or reduce PHI risk to acceptable levels within our office. Discussion between our Practice Owner, Privacy Officer and/or an I.T. Security Specialist will influence our final structured protocol. We will also take into consideration our employees that have access to confidential data and ensure they are trustworthy individuals. Finally, with this information, we will be authorizing levels of security clearance, for access to our more sensitive information and making sure all employees create new, ***private*** passwords for their access. We will enforce that they are responsible for their work stations and protecting PHI.

Identify and evaluate current controls that will prevent unauthorized disclosure, misuse, alteration, or destruction of information or information systems. Also, look into methods of further increasing your security. Compare the various technologies that may be worth investing in for added control measures.

Implementation of Risk Controls:

Controls are inadequate or don't exist, for: _____NONE AT THIS TIME

Action plan to improve and implement controls:_____NONE AT THIS TIME

(i.e.: wireless router for internet, firewall for all computers)

We will Set Security Levels on our computer software in the following manner:

Circle the appropriate answers below:

High Level Access: DOCTOR / MANAGEMENT

Moderate Level: MANAGEMENT

Standard Level: ALL TEAM

Supervise and Review:

At least once a year, we review the risk assessment to validate that controls are addressing risks effectively and consider any changes to the business environment.

2023 Date: _____ Evaluation and research reveals we should implement _____

2024 Date: _____ Evaluation and research reveals we should implement _____

2025 Date: _____ Evaluation and research reveals we should implement _____

2026 Date: _____ Evaluation and research reveals we should implement _____

2027 Date: _____ Evaluation and research reveals we should implement _____

2028 Date: _____ Evaluation and research reveals we should implement _____

— HITECH LAW & HIPAA SECURITY RULE Policy —
Risk Management Analysis
EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document I declare that I have been fully trained and understand the materials and steps necessary to carry out and enforce the Risk Management Analysis HITECH LAW Policies and Practices for this facility. I will fully abide by these practices in accordance with our Administrator and Federal law.

Date	Print Name	Signature

Office for Civil Rights ("OCR") of the
U.S. Department of Health and Human Services ("HHS")
final HIPAA Omnibus Rule (the "Final Rule")
Enacted January 17, 2013 by HHS
Effective September 23, 2013

HIPAA OMNIBUS RULE WORKBOOK

AN INTRODUCTION & OVERVIEW

Employee Video Training & Electronic Versions of Forms in this workbook are available with access via our HIPAA On-Line Portal

HIPAA ON-LINE ACCESS LINK:
https://www.healthfirst.com/ontraq/
Once you are on this link, please follow the **SIGN-ON PROMPTS** to enter this **HIPAA PORTAL**

HIPAA Annual Update Program

ACCESS IS FOR ONE LOCATION ONLY AND IS DIGITALLY TRACE PROTECTED.
PASSWORDS WILL CHANGE ANNUALLY. CALL US FOR RE-NEWAL PASSWORD.

Reference this workbook during your HIPAA training

OFFICE PROTOCOLS
in accordance with the
HIPAA Omnibus Rules

*Welcome to your **HIPAA Omnibus Rule** training packet and thank you for choosing* **HealthFirst** *for guidance as you integrate this important information into your day-to-day healthcare practice. This packet was designed to serve as an introduction and informative guide for implementing and maintaining the **HIPAA Privacy Practices of "HIPAA Omnibus Rule" / Effective September 23, 2013**. It is recommended that you study the information in this packet to understand the new mandates under the new **HIPAA Omnibus Rule.** Then, utilize the required forms, included at both the back of this packet and (in electronic format) accessible via our HIPAA On-Line Portal, to execute **HIPAA Omnibus Rules.** The electronic forms on our HIPAA On-Line Portal can be customized to your liking. They are in (.doc) format and will open in Microsoft WORD™. This packet is an introductory training guide and additional protocols, legal counsel and study is recommended to reflect the particular business practices of your healthcare facility. Please seek legal advice for more specifics on the **HIPAA Omnibus Rule.***

HIPAA FORMS TABLE OF CONTENTS

I. HIPAA OMNIBUS RULE CHECKLIST of REQUIREMENTS

Your HIPAA Protocols will need to be updated—at least annually.

To ensure that you have access to our HIPAA Portal
with the most current HIPAA updates, call: 941-587-2864

READ & IMPLEMENT THE HIPAA PROTOCOLS BELOW:

Check-off/ Done	Task to complete…	Where to find this…
HIPAA AUDITS	**IMPORTANT: Office of Civil Rights / The Department of Health & Human Services** will begin to send out emailed-survey to healthcare office that request detailed information about your HIPAA Practices. **PHASE I / HIPAA QUESTIONNAIRE AUDITS via EMAIL will begin in 2016.** Please check your email and complete pre-audit questionnaire within 10 days of receipt. If you do not respond, OCR will use public info to create its audit subject pool. For examples of OCR audit questions, click this link: **PHASE II / IN-OFFICE HIPAA AUDITS will begin in 2016.** For more information, please check this link, listed to the right…	http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/questionnaire/ http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html
HIPAA REPORTS	**RISK ASSESSMENT WRITTEN PLAN—Gov-Issued Template:** This report will take up to 20 hours to complete each year: (For a time-saving alternative see Upgrade Section in ***RED*** below) 1. Watch Security Risk Assessment Tool Video Tutorials first! 2. Click this link to: Security Risk Assessment Tool (SRA Tool) Complete these **4-Sections**: Users, About Your Practice, Business Associates & Asset Inventory (office equipment) ****Do not print the sections; Complete and save to a single computer**** ***Up grade to RISK ASSESSMENT made EASY Template:*** *We will co-create this required report with you in 1 hour!* ***Call for details: 941-587-2864***	**Find This Report Template on:** HIPAA On-Line Portal **SRA Video Tutorial Link:** https://www.healthit.gov/providers-professionals/security-risk-assessment-videos **SRA Tool Link:** https://www.healthit.gov/providers-professionals/security-risk-assessment-tool
	ANNUAL DATA BACK-UP & CONTINGENCY REPORT Print from HIPAA Portal or find blank copy in the 5-year organizer of your HIPAA Manual Fill out each year with your IT Tech	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:**
TRAINING & EMPLOYEE FORMS	***ADMINISTRATIVE SAFEGUARD*** ***Signed Employee Forms** should be stored **& Scanned to a Management Accessible Folder***	
	All employees must complete ***HIPAA Omnibus Rule Training*** by watching ***HIPAA Omnibus Rule Video.*** **Then sign (3) Forms:** ** All new hires must watch ***HIPAA Omnibus Rule Video & sign Employee Forms*** prior to handling patient PHI** 1. ***HIPAA CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT + EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAINING Proof-of Training Certificate.*** (Group Sign-In Sheet)	**Video & Forms:** on **HIPAA On-Line Portal** ***Re-watch video at least annually*** **Find These Forms on:** **HIPAA On-Line Portal** **or HIPAA Manual**
	2. HIPAA RISK ASSESSMENT & MANAGEMENT ANALYSIS+ **HITECH LAW/ HIPAA SECURITY RULE POLICY** **EMPLOYEE TRAINING ACKNOWLEDGEMENT** (Group Sign-In Sheet)	**Find These Forms on:** **HIPAA On-Line Portal** **or HIPAA Manual**
OFFICE FORMS	***ADMINISTRATIVE & PHYSICAL SAFEGUARD***	
	Have all applicable Business Vendors sign & retain on-file. ***HIPAA OMNIBUS RULE BUSINESS ASSOCIATE AGREEMENT (BAA)*** *(Vendor Confidentiality Agreement)* *Print Email or mail these to vendors; Retain Signature Page on file;* *Store in HIPAA Manual & Scan to a Folder for safe keeping* ***HIPAA NON-DISCLOSURE AGREEMENT*** ***Print these & have signed by Temporary Employees, Volunteers***	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:** **BAA: HIPAA Manual: pg 154-159** **NDA: HIPAA Manual: pg 78-79**
	BUSINESS ASSOCIATE AGREEMENT LOG *This Log will make tracking your BAA project—easy!*	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:** HIPAA Manual: pg 176
	HIPAA OMNIBUS RULE ***PATIENT ACKNOWLEDGEMENT FORM*** **Must be signed by all patients—new and existing patients must sign.** *Print 1000-2000 for use or use PDF version if paperless*	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:** HIPAA Manual: pg 60 (Healthcare) pg 61 (Pharmacies)

	THIRD PARTY MEDICAL RELEASE FORM *Must be signed by patient when a third-party needs to pick up records or radiographs* *Print 50+ copies: Use when needed*	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:** HIPAA Manual: pg 62
	NOTICE OF PRIVACY PRACTICES *Must be displayed in your office & posted on your website* ***To Display:*** *Print 1-4 copies from HIPAA Portal* *Place on clipboard; Laminate or place in a plastic page protector.* ***For Website:*** *Use PDF version from HIPAA Portal*	**Find This Form:** **HIPAA On-Line Portal or HIPAA Manual:** HIPAA Manual: pg 51-59
HIPAA MANUAL UPDATE PAGES	***Update Your HIPAA Manual on (3) pages*** Add today's date to these pages:	**HIPAA MANUAL:** Data Back-Up & Contingincy Plan pg 99 Our Balancing Test Pg 117 Analysis Risk Control Measures Pg 119
PHONE, INTERNET & COMPUTER UPDATES	***TECHNICAL & PHYSICAL SAFEGUARD***	
	TEXT PATIENT INFORMATION IN A SECURE MANNER: If you use your cell phone for texting patient PHI, do not use the patient's full name or other full identifiers. Always use abbreviated patient identifiers to be HIPAA compliant or HIPAA Compliant Phone Text APPs…	**HIPAA Compliant APPs:** www.Rhinogram.com www.Awrel.com www.Perfectserve.com www.Pmd.com www.zipwhip.com
	PROTECT YOUR OUTGOING EMAILS— ***ADD AN OUT-GOING-EMAIL ENCRYPTION SOFTWARE BRIDGE*** Out-going Email Encryption Subscriptions cost: $8-15 / month. Written Validation Programs are permissible but not Best Practices.	**Best Practices Choice:** iMedicore = https://signup.imedicor.com/deh/ (Multi User per Doctor) Enter Promo Code: IMED2250 www.weave.works www.potectedtrust.com **Google Search:** HIPAA Compliant Email Encryption Service (1) User = www.sendinc.com Most Comprehensive = www.N-krypt.com **877-265-7978**
	CONVERT FACIMILE TO A FAX-TO-EMAIL SERVICE Best Practices will have you converting Faxes to a HIPAA Compliant, Fax-to-Email Service. Traditional faxing will require you write a detailed **Fax Safeguard Plan:** move your fax machine to a "management guarded area", keep detailed sign-in sheets when fax is used & clear data back-ups daily.	**Google search a Fax-to-Email Service** Check out: www.LuxSci.com www.Faxage.com www.scrypt.com
	PROTECT YOUR SERVER FROM IDENTITY THIEVES Move your server to a vented / locked room or purchase a "server cage" to bolt your server to the floor or a piece of furniture. This will create a barrier and be a deterrent from your server being stolen by Identity Thieves.	**Google search & Order:** Server Cage / Server Locker (cost: $300-$400)
	DO AWAY WITH TAKE-ALONG BACK-UP DRIVES; GO FULLY-AUTOMATIC Take-along drives pose a risk of theft or loss: Theft of a device risks a $150K HIPAA fine + 18-month audit! Automatic, encrypted, cloud back-up is Best Practices. Research & choose a reputable cloud hosting service. Be sure to sign a Business Associates Agreement with your Cloud Service Provider.	**Check out:** Snap-Shot Back Up www.Carbonite.com Automatic Cloud Back Up www.ddsrescue.com Automatic Cloud Back Up Business Continuity System icoreCONNECT.com https://signup.imedicor.com/deh/
	UPDATE WINDOWS BASED SYSTEMS: Windows based systems should be updated to Windows 10 (or better) ASAP! Windows 8 is currently not HIPAA compliant. Windows 7 will be HIPAA Compliant thought the end of 2020.	**Update to:** Windows 10 (or better)
FACILITY PROTOCOLS	***ADMINISTRATIVE & PHYSICAL SAFEGUARD***	
	MAKE SURE YOUR PATIENT CHECK-IN/OUT AREAS ARE PRIVATE. Do not have patients stand in back of one another during patient check in /check out. Be sure overflow of patients have a seat in reception area to wait. Use the verbal skill and/ or make a sign saying: **"Please have a seat in our reception area while this patient finishes up their check-out as we like to insure each patient's privacy"**	Have a meeting with your team to review this important HIPAA protocols.
	HAVE A "HIPAA DRILL" MEETING: Just like you would have a "fire drill" plan to have a "HIPAA Drill" meeting to ensure your team understands proper Protocols & Procedures for preventing HIPAA Breaches and responding to them.	**HIPAA Drill Activities:** Use this Checklist for review Create HIPAA Breach Scenarios Review HIPAA Forms

For *more detailed information* about your *HIPAA Checklist of Requirements*... Read the following:

II. ADMINISTRATIVE/PHYSICAL ASPECTS

❑ **Create space within your office that promotes privacy.** Build by design, reconfigure or create protocols to stop and isolate patients when they are checking in, in treatment or checking out of your office. Internet reports for HIPAA Privacy & Security breaches are reported directly by the patent, 33% of the time.

❑ **Train your Employees** on Omnibus Rule Protocols, Terms & Requirements. Watch the 1-hour HIPAA Employee Training Video. Read this packet for more information and definitions.

❑ **Have each employee sign a new Omnibus Employee Proof-of-Training Certificate & Confidentiality Agreement.** Keep it in your HIPAA Manual. We suggest filing these by year for easy access. Pages 46-47 of this packet provide an ***Individual Employee Confidentiality Agreement.*** Pages 48-50 provide a ***Group Employee Confidentiality Agreement plus Proof-of-HIPAA Omnibus Rule Training.***

❑ **Make sure your IT Tech / IT Provider** will supply you with (2) reports—at least annually:

1. Data Back-Up & Contingency Plan Report
2. Risk Assessment Plan Report

We supply templates for you. Data Back-Up & Contingency Plan will be located blank--in your 5-Year Organizer. The Risk Assessment Plan Report is provided in template format via your HIPAA On-Line Portal.

❑ ***Have your vendors sign* a new *HIPAA Omnibus Rule Business Associates Agreement* (BAA).** Keep them on file within your HIPAA Manual. Please scan& save these signed BAAs in a management accessible folder for safe keeping / easy access. HIPAA Auditors will ask to see these!

Print 10–20 of these BAAs to sign with your appropriate vendors

BAA signature-on-file due dates were: **sign by Sept 23, 2013**

New Associates = sign BAA prior to doing business
Existing Associates = use updated BAA to HIPAA Omnibus Rule standard

"WHO" IS A BUSINESS ASSOCIATE?

BAA is Required for: (Data Collection Agencies)	BAA is Recommended: (to be safe)
• Confirmation Service • Consultants, IT Tech, Etc. • Data Storage Company	• Temp Employees / Volunteers / Students • After Hours Services

BAA *Not Necessary* for:

- Doctor-to-Doctor
- Doctor Referrals
- Pharmacy
- Insurance Company
- Delivery Conduits: UPS, FED EX, USPS
- Dental Labs

The above list is "considered the course-of-doing-business".

In these situations, sharing PHI is necessary for patient treatment.
PHI sharing should be at a "minimum necessary" level.

- **Educate your Business Associates** that they need to have their own Business Associate Agreements, signed and on file with their Subcontractors. Do not permit your Business Associates to use this Business Associate Agreement (Master Copy) with their subcontractors. Their agreements will need different wording and you do not want to become liable for their actions under this document. Advise your Business Associates to purchase their Business Associates / Subcontractors Agreements at: Amazon.com HIPAAOmnibusRule.com HealthFirst.com
- ***Scan & Copy all Employee Signature Forms & Business Associate Agreements* to a *management accessible folder for safe keeping*. Add new employee signature forms and new vendors as they join your office.**

  4-Factor Risk Assessment Sheets: We have started you off with a copy at the back of this packet. Use these when you have breach situations to track the event. Store these in a section of your HIPAA Manual labeled ***"Breach Assessment Sheets".*** This sheet will provide easy access & initial documentation, when breach occurrences need documenting. It is required that you submit all HIPAA Breach Occurrences to this URL; Create a link from your desktop or "favorite places" in your web browser:
  http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

  (If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

- ***Begin to use our* HIPAA Patient Acknowledgement Form** from our HIPAA On-Line Portal. You can print this from our **Microsoft WORD** or **PDF** file folder.

All patients need to sign this updated HIPAA form.

You can change this form to suit your office protocols, but keep in mind:

- **Keep the Third-Party Sales Statement on the bottom of this form, *if you sell products* or *if you receive commissions or rebates*,** participate in multi-level marketing product or service sales to patients within your practice. We encourage you to review the master copy of Patient Acknowledgement Form in your HIPAA Omnibus Rule Workbook (page 39) and via our HIPAA On-Line Portal. You can customize this form to suit your protocols.
- **Add a Statement to your HIPAA Patient Acknowledgement Form if you intend to use PHI for Fund Raising or Research.** Patients must be offered an "opt-out" option for texting and emails. One has been added to the **Patient Acknowledgement Form** included in your workbook and also our HIPAA On-Line Portal. We encourage you to review and use it should you participate in Fund Raising or Research that exposes patient PHI. It is also a respectful option to offer the opt-out to all patients.
- **REMEMBER: Deliver Patient Electronic Forms within 30 days** and in a format requested by the patient, if "readily available and producible". ***Texas HIPAA HB 300 Law*** requires delivery in 15 days. Electronic copies are required if you have them: Email, Microsoft™ WORD Document, PDF, fax.
- **Begin to use the Third-Party Release Form, as a consent to release medical records/radiographs to Third Party Representatives, wishing to pick-up patient information.** Use this for patients who may request that their records or radiography be picked-up or sent to a Third Party (Guardian, Spouse, Child). A copy is provided in back of your HIPAA Omnibus Rule Workbook and also our HIPAA On-Line Portal. All forms are also included in the OFFICE FORMS section in our HealthFirst HIPAA Manual.
- **Update your copies of Omnibus Rule Notice of Privacy Practices (NOPP).** A new copy of a NOPP, to

Omnibus Rule standard, is provided in back of your HIPAA Omnibus Rule Workbook, and on our HIPAA On-Line Portal. Replace these copies within your front office or other departments where you display the NOPP. Displaying a copy of the NOPP within your healthcare office is required. Make a copy of the NOPP for your reception room or keep a laminated/ plastic covered copy on the clipboard that the patient uses to update their patient forms. When they fill-out their forms, they can read the NOPP. You can also obtain a book-bound copy from any of our websites: Amazon.com HIPAAOmnibusRule.com HealthFirst.com

If a patient requests a copy of the NOPP you are required to give them a hard copy.

- **Post NOPP on your website:** If you, the Covered Entity, provide healthcare services on site, a copy of the ***NOPP*** is required to be posted on your website, if you have one. A **PDF** electronic copy of the new ***Omnibus Rule NOPP*** is also available our HIPAA On-Line Portal.
  - **Know & Include these (9) new elements in your *Omnibus Rule NOPP.*** Also available in book-bound version as mentioned above. These are the (9) elements to:

1. Sale of PHI is prohibited.
2. Use of PHI in marketing or fundraising is prohibited except with prior authorization (as noted within the new HIPAA Patient Acknowledgement Form).
3. Restrict disclosures of PHI to Insurance Plans for services paid for "out of pocket".
4. In-Office of display of HIPAA *Omnibus Rule* NOPP is required.
5. Web-Posting of HIPAA *Omnibus Rule* NOPP is required.
6. Written permission from patient to send PHI to non-authorized 3rd Parties is required.
7. Health Plans that underwrite cannot include genetic info.
8. Health Plans must web-post **Omnibus Rule NOPP** & send written notice of Omnibus Rule changes to all members.
9. Psychotherapy Notes: Use & Disclosure requires patient authorization.

Now Excluded from NOPP: You do not have to have patient authorization to send: Appointment Reminders, Treatment Information, Insurance Benefit Notifications. Now it's considered the course-of-doing-business.

❑ **Remember to fill-out: Annual Data Back Up & Contingency Plan / Located in your HIPAA Manual in the 5-Year Organizer.**

Additional Office Protocols to Revise

Omnibus Rule includes additional changes that, although are of lesser importance than the ones listed within this document, they are not without consequence. Please note and include these in your internal ***Employee Training*** and ***Office Protocols.*** They include:

- **Out-of-Pocket Payment Privacy Provision** to restrict PHI disclosures to health insurer when it pertains to items or services for which an individual has paid. Since this is a business office procedure, your billing department or receptionist needs to set in place protocols for complying with such requests;
- **Access to PHI in Electronic Format** upon request from patient. If you store PHI on a computer, you must supply designated record sets electronically to the patient;

- **Transmission of copies of PHI to Third Persons** when patient requests are made in writing; Request must include: who sent to, where sent to, & date.
- **Disclose PHI to family members of a Deceased Patient** who were involved with the patient's care or payment for their care, as long as there is no written restriction on file and as long as there is no state law requiring confidentiality.
- **Establishment a 50-year limit on the obligation to protect the PHI** of deceased individuals as long as there is no state law that is more restrictive;
- **Disclose Immunization Records Provision** to schools if required by law;
- **Genetic Information Provision** in accordance with the Nondiscrimination Act of 2008 (GINA) by prohibiting the use of genetic information for underwriting purposes, such as eligibility determinations and the computation of premiums.

III. TECHNICAL ASPECTS

- ❑ **Use Updated HIPAA Software.** In 2014, Microsoft stopped updating their software to HIPAA compliant standards for free. This means if you are still using Microsoft XP, it is not HIPAA compliant. Worse yet if you use Microsoft XP paired with an internet connection, all of your patient Protected Health Information (PHI) is open to the public and internet identity thieves. Make sure you get your Microsoft software updated to Windows 10 or higher. This will ensure that you are working to the current standard for these HIPAA Omnibus Rules.
- ❑ **Protect your Server.** Where is your server located in your office? It's important to make it "secured". If it is out in the open, it can be prone to vulnerable to being stolen. In 2015, 48% of all Healthcare Facility HIPAA Breaches were associated with the theft of a devise. Servers, laptops and take-along data back-up drives are most vulnerable. Be sure to secure your server in a ventilated closet or purchase a "server cage" that can bolt your server into the floor or to a piece of furniture. Server cages are available from www.eaton.com.
- ❑ **Retire Take-Along Back Up Drives.** Take along back-up drives are not ideal for today's vulnerable Privacy & Security threats. While many healthcare facilities have traditionally used them for data back-up, in today's vulnerable, high-priced HIPAA world, they come with too high a fine if they get lost or stolen. Recent fines for stolen back-up drives can bring a healthcare facility $150K in HIPAA fines! Please make smarter choices to upgrade to automatic secure cloud back up. This is Best Practices for your healthcare facility. Do away with the take along back-up drives.
- ❑ **Protect your Out-Going Email.** If you send emails to patients, labs and/ or doctors, you will want to make sure any patient Protected Health Information (PHI) is secure. There are (20 ways you can accomplish this: Create a ***Written Email Verification System*** or get ***Out-Going Email Encryption Service***. We think the latter is best. While creating an "Email Verification System" within your office is valid, it is time consuming and you will need to pre-verify (in writing every email prior to using it…uggh!). Purchasing an Out-Going Email Encryption Service costs about $8-12 per month. Try www.n-krypt.com, Weave, Protected Trust, iMedicore.
- ❑ **Text Properly.** Do not use a patient's full name. Best practices will have all employees using a HIPAA Compliant APP like Weave.

IV. GLOSSARY of TERMS:

HIPAA: *Health Insurance Portability & Accountability Act* was federally enacted in1996 and has been enforced strictly since 2003. HIPAA regulations are more significant now because of the massive and continual use of the internet and the importance of keeping identifiable Patient Health Information (PHI) private!

PHI: *Protected Health Information:* any identifiable information which relates to an individual's past, present or future physical or mental health or condition for which there is a reasonable cause to believe it can be used to identify that individual*. This would include:

1. Names
2. Zip Codes
3. Birth Dates
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle Identifiers & Serial Numbers (including license plate numbers)
13. Device Identifiers & Serial Numbers
14. Web Universal Resource Locator (URL)
15. Internet Protocol (IP) Address Number
16. Biometric identifiers (including finger or voice prints)
17. Full-Face Photographic Images (and any Identity Bearing Images)
18. Any other unique identifying number, characteristic or code*

There are 18 Protected Health Identifiers common to for business or professional use. ***(45 CFR Sec. 164.514 — Code of Federal Regulations)***

EHR Electronic Health Records: patient records that can be transmitted or copied and shared by electronic means: digital, fax, text, phone transmission or via internet.

ePHI: Electronically sending PHI. This would include fax, phone, text or emails. ePHI is similar to EHR but more specifically PHI. (See the 18 Protected Health identifiers listed above).

COVERED ENTITY: under the HIPAA Privacy Rule a Covered Entity refers to three specific groups, including: Health Plans, Healthcare Clearinghouses, and Health- care Providers that transmit health information electronically. See this link for more details: https://ocrnotifications.hhs.gov/ or www.hhs.gov/hipaa/

BUSINESS ASSOCIATE: An entity, (non-employee) that in the course of their work will directly / indirectly create, receive, maintain or transmit PHI on behalf of the Covered Entity. The following are considered Business Associates under the Omnibus Rule:

- Health Information Organization**
- e-Prescribing Gateway
- Data Transmission Services—requires access on a routine basis to (PHI).

**The Office of Civil Rights declined to specifically define a "Health Information Organization" because this scope of business is still evolving; an entity that does not require access to PHI is not included. These are considered conduits.

SUB CONTRACTOR: an entity that creates, receives, maintains or transmits PHI on behalf of a Business Associate. A signed Business Associate Agreement must be in place *between the Business Associate and its Subcontractor* to safeguard confidentiality from the subcontractor regarding all PHI handled, processed or viewed. The Business Associate keeps these documents on file for easiest access within their HIPAA Manual.

EXAMPLE: Doctor hires a Medical / Dental Software Company;

That Software Company sub-contracts with a text & e-mail confirmation service. The *text and email confirmation service is a "subcontractor" of the Business Associate Software Company. The Software Company must have a Business Associate Agreement with its subcontractor.*

CONDUIT: An entity who temporarily stores PHI either in paper or electronic format. Conduits are not required to sign Business Associate Agreements or Subcontractors agreements directly.

EXAMPLE: Mail Courier, Postman

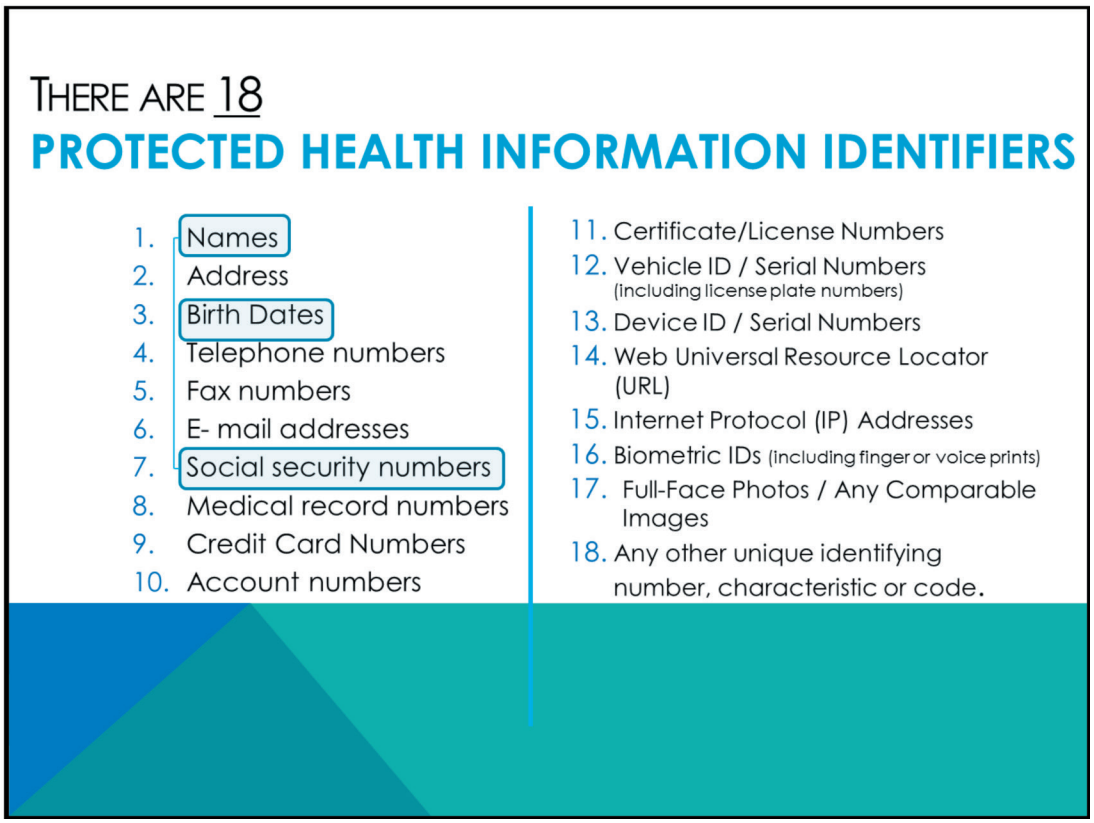
OCR: The Office for Civil Rights

HHS: The U.S. Department of Health and Human Services

Protect your Server with a "Server Cage / Server Locker"
Retire Take-Along Back-Up Drives /
Update to Encrypted Cloud Off-Site Data Storage

ALL CONVERSATIONS, INTERNET, DIGITAL & PAPER CORRESPONDANCE OF PHI SHOULD BE CONSIDERED CONFIDENTIAL AND PROHIBITED TO OFFICE USE ONLY this applies to all: EMPLOYEES, BUSINESS AFFILIATES AND NOW THEIR SUB-CONTRACTORS.

Patient privacy starts with you and cannot be shared except for professional use in the patients' health interest. Patient privacy is to be honored as never before!



V. OVERVIEW of OMNIBUS RULE

OMNIBUS by definition means:

noun: A volume containing several novels or previously published parts.
adjective: comprising several items.

As of January 17, 2013, HIPAA regulations have had a massive update and overhaul to protect patients. The new laws more extensively hold second and Third-Party businesses responsible to keep patient health information (PHI) private! *Protected Health Information* is defined as any identifiable information which relates to an individual's past, present or future physical health or condition for which there is a reasonable cause to believe it can be used to identify that individual. There are 18 Protected Health Identifiers common to business or professional use. ***(45 CFR Sec. 164.514 — Code of Federal Regulations)***

The Office for Civil Rights (**"OCR"**) of the U.S. Department of Health and Human Services (**"HHS"**) adopted this update to the USA's existing volumes of HIPAA Law and HITECH Law. The Final Rule or final HIPAA omnibus rule **(78 Fed. Reg. 5566)** has some important modifications to HIPAA as we know it. They are required to begin functioning within your workplace, begin-ning March 26, 2013. Though you are allowed time to attain signatures from Business Associates for compliance. Below we have listed requirements of the new Omnibus Rule law and what is required of you:

1. New Business Associate Agreements must be signed; Old ones become obsolete: **A new version of the Business Associates Agreement (BAA) is required to be Signed & On-File in your HIPAA Manual. New BAA must be signed to the Omnibus Rule Standard.**
2. New Compliance Obligations & Liability: Business Associates to their Subcontractors. **Business Associate must have Subcontractor Confidentiality signatures on-file in their HIPAA Manual.**
3. Breach Notification for Unsecured Protected Health Information (PHI) **Breach Assessment Protocols are required. Forms are included in this packet and on our HIPAA On-Line Portal for easy-access as you may need them.**

4. New Marketing & Fund-Raising Protocols
5. **Explained within this packet; included in your updated Notice of Privacy Practices (NOPP) within this packet and on your CD-ROM.**
6. New Additions to Notice of Privacy Practices (NOPP) for Patients' Right-to-Know
7. **Updated Revision included within this document; Keep as your new office copy of (NOPP / Omnibus Rule).**

VI. UNDERSTANDING YOUR BUSINESS ASSOCIATES OBLIGATIONS

Under Omnibus Rule, HIPAA Business Associates will now be subject to the same stringent HIPAA Security Rule requirements, use and disclosure limitations as you, the Covered Entity and will be subject to audit and fines by HHS. ***Business Associates will need Business Associate Agreements from their subcontractors*** who may receive, create, or transmit PHI on their behalf. Your Business Associates will need to:

1. ***Implement & maintain Information Security Policies*** that comply with the HIPAA Security Rule [1]
2. ***Enter into Business Associate Agreements with Subcontractors*** that exchange your PHI
3. These have to be **written, signed & on-file** in the **Business Associates workplace**

Respond to Breaches of PHI in accordance with new Omnibus Rule HHS regulation. Breaches of PHI need to be reported by the Business Associate to: The Secretary of U. S. Department of Human Health Services using this electronic link: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Business Associates under the ***new*** Omnibus Rule include:
- Health Information Organizations
- E-prescribing Gateways
- Data Transmission Services (personal health record vendors)

Business Associates under HIPAA law include, data collection agencies:
- Confirmation Services
- Collection Agencies
- Software Companies
- IT Techs
- Consultants
- Email & Fax Encryption Services
- Dental Suppliers & Dental Repair Services
- Data Back Up Providers
- Landlords
- Other Vendors

Business Associate Agreements are ***"highly recommended"*** to have for:
- Volunteers, students & temporary help
- After Hours Services that may be in your office unsupervised
- Sales Reps that enter business and treatment areas

Non-Business Associates or entities *not required to have a signed Business Associates agreement on file.* These are chosen by the patient or affiliated with by choice. Such will be:
- Doctor-to-Doctor business
- Healthcare Providers
- Insurance Company business
- Pharmacies
- Dental Labs

Under HIPAA doctrine, contact with these entities are considered the course-of-doing-business, if the sharing is necessary for patient treatment, and the PHI sharing is to be of "minimum necessary" rule.

What does Omnibus Rule mean to you the Healthcare Provider?
You must make sure you understand that the new Omnibus HIPAA regulations are far reaching. They will now penetrate all of your Business Associates and their Subcontractors to protect your patients' (PHI) Protected Health Information. Basically no one is to mishandle PHI or share it with marketers, advertisers or others for professional gain. The new Omnibus Rule helps prevent the "ripple effect" with regards to PHI. Now all entities that come into contact with PHI, directly or indirectly will need to respect PHI to the fullest degree of the law. This new protection is a massive effort on the part of the US government to decrease and mitigate identity fraud and malicious conduct.

What must be in place? The Covered Entity (which is your office in this case) will need to have a ***new format*** of the ***Business Associate Agreement,*** signed and on-file within your HIPAA Manual for all existing and new Business Associates with whom you do business. **We have provided a master copy of this new Business Associates Agreement (BAA) at the back of this packet and in electronic format with access via our HIPAA ON-LINE PORTAL. Please print/copy it and have all of your Business Associates sign and return it to you. Then keep it on file.** Keep in mind, if you have had BAAs signed prior to September 2013, they must be updated to this new ***Omnibus Rule Business Associate Agreements*** format.

US Department of Health & Human Services **(HHS)** has released a new Omnibus Rule BAA form that includes all of the revisions and requirements of the Omnibus Rule. The model form is available at:
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Remember, we have included a master copy of this new ***Omnibus Rule Business Associates Agreement*** at the back of this document. Please print, copy and have it signed by all of your Business Associates. When returned, keep them on file in your HIPAA Manual.

If your present HIPAA Manual predates the Omnibus Rule, then you will need to purchase and keep an updated, Omnibus version on file. You can purchase one on any of our websites:

Amazon.com HIPAAOmnibusRule.com HealthFirst.com

VII. BREACH OCCURANCES: BREACH RESPONSE PLAN

The HIPAA Breach Notification Process has changed. Previously you were to report a HIPAA breach if there was **"Significant Risk"** that the breach of (PHI) protected health information was "compromised" and could cause either financial or representational harm to an individual. Currently, the Omnibus Rule authors, nor any HIPAA Officials, provide a clear or quantifying definition for the meaning of "compromised".

Under new Omnibus Rule, breach reporting goes from **Significant Risk** to "Presume Risk unless you can prove **Low Probability**". Because there is no way to "quantify a compromise", or ***"measure"*** low to high risk probability, (i.e.: if there is a 1% probability or a 20% probability that PHI will be truly compromised), **you should be reporting most breaches and you will need to document each situation.** This process will be easy as the government provides this easy-access automated link to report all Breach Occurrences:
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

We have also provided our **(4)-Factor Breach Assessment Sheet** for your HIPAA PHI breach determinations at the back of this packet (also in electronic format on tour HIPAA On-Line Portal. Get access via this link: http://dental-enhancements.com/hipaa-annual-update-program/. You will find several blank **(4)-Factor Breach Assessment Sheets** in the very back of this packet. We encourage you to place these inside your existing HIPAA Manual. Use

the divider tab that we have provided, which is labeled "**Breach Assessment Sheets**". This will provide you easy access to these sheets should you care to use them and document your Breach Occurrences. You may use these to document your breaches, or you can print a copy of the automated HIPAA Breach Reporting website screen upon entering your breach details. Keep in mind, if you choose ***not*** to report a breach, you may be called upon in the future to justify your decision. Remember, there is no established "quantifying system" with which you can qualify a breach. In this early stage of breach assessment, the **HHS** will most likely be trying gather breach assessment information to quantify and qualify situations for future law revisions.

Do not be confused or disappointed that at this time, the US Government is not clearer in providing definite reporting guidelines for your breach occurrences. We will get to that point. For now, all Healthcare Facilities will contribute to this risk assessment process. With time, PHI risk assessment and reporting should evolve to become more uniform as the US Government evaluates all reported data. The main goal now is protection of the patient and reduction of identity theft.

To understand more about Breach Assessment under Omnibus Rule, we will now provide a bit more insight. The original ***Breach Notification Risk of Harm Trigger*** has been changed: From: **Providing notice when there is a "Significant Risk" of harm**… as set forth in the Breach Notification Interim Final Rule issued by HHS on August 24, 2009 (the "Interim Final Breach Notification Rule"). Under that rule, entities were required to provide notice of breaches *resulting in unauthorized access to PHI* where the breach posed a *significant risk of financial, reputational or other harm to the affected individual.*

Now it is changed to: **Providing notice in all situations except in "Low Probability" situations.** Omnibus Rule legislators expressed concerns that the "risk of harm" standard was too subjective, noticing "no standard-ization of reporting" was established, which could increase PHI leaks. Under the Omnibus Rule there still is no established standardization to the reporting. The legislators must first want to collect more data on breach situations in general. They did however, ***include*** in the new Omnibus Rule breach reporting protocol that ***non-permitted*** acquisition, access, use and disclosure of PHI is deemed to be a breach. Unless the Covered Entity or Business Associate ***can demonstrate***, using a **4-Factor Assessment Formula**, that there is a ***low probability*** that PHI has been compromised. If you are confused by this definition, we will now simplify it for you: If your PHI has found its way into non-authorized hands, you should fill out our **(4)-Factor Breach Assessment Sheet** and ***in most cases, report the breach*** to this web-link: http://www.hhs.gov/hipaa/for-pro-fessionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

We want you to be cautious and prudent in all breach occurrence situations. New HIPAA fines are extremely costly, ranging from $100 to $1.5 K. So, we are teaching you to over-report rather than under-report in all breach situations.

Be aware, that other than listing (4) Risk Assessment Factors, the Omnibus Rule legislators do not provide an actual Risk Assessment Form. We have created and provided one for you in this packet. Additionally, **HHS** does not define the term "compromise" or explain what it means for PHI to be compromised. United States Depart-ment of Health and Human Services **(HHS)** does support, that it will offer additional guidance "to aid Covered

Entities and Business Associates in performing Risk Assessments with respect to frequently occurring scenarios." ***Best practices*** will be to report all Breach Occurrences to the HHS automated web link provided. You can us our **(4)-Factor Breach Assessment Sheets** to document all incidents and retain a copy of your incidents within your patient files so you are not remiss in following the law. Better to over-report, than under-report, since fines are excessive for negligence. Remember, there is no way to quantify "low probability" so be conscientious with your breach reporting.

4-Risk Factor Assessment Sheets

At the back of this packet, a **4-Risk Factor Breach Assessment Sheet** awaits you. You know by now that these are "reference sheets" and should only be used as a helpful guide. You should actually report all Breach Occurrences directly using the HHS Website Link:
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)
Major Breach Protocols also requires: *Report to Media:* Newspaper, Radio & TV; Notify media as a Press Release; This notice must be within 60 days of discovery of a Major HIPAA Breach & must include the same information required for the individual notice.

Our 4-Risk Factor Breach Assessment Sheets will serve as an objective, user-friendly breach occurrence reference sheet. They will help you determine whether PHI has been "compromised" for each situation you evaluate. Finally, they will demonstrate accordance with HIPAA Omnibus Rule standards for assessing various breaches. Here are some examples of possible breaches:

- Theft of an office computer
- You determine your computer data has been "hacked into"
- You dial the wrong phone number and leave a message using PHI
- You stuff an envelope with an incorrect patient invoice
- You notice a patient has walked off with your patient sign-in sheet
- You forgot to shred all documents and your cleaning crew has discarded them
- You accidently fax or email the wrong doctor's office PHI

While some of these occurrences may seem harmless, we caution you, as there is no "quantifying protocol" for this low probability measuring factor that Omnibus Rule imposes. And Omnibus Rule does not define the term "compromise" or explain what it means for PHI to be compromised. Please be mindful to *document and report your breach occurrences* to avoid costly HIPAA fines. You should also consult an attorney who specializes in this area of law should you encounter a situation that proves to be serious or highly questionable in scope. Theft or hacking of PHI would require an attorney's attention.

For now, let's look at how to use the **4-Risk Factor Assessment** provided in this packet:

How To Use the (4)-Factor Breach Assessment Sheet for PHI Breach Determination:

1. Determine/Discover that a breach situation has occurred within your workplace.

2. Locate the **(4)-Factor Breach Assessment Sheets** provided in the back of this packet. Please keep them in your HIPAA Manual and use the "tab divider" provided, labeled **"Breach Assessment Sheets"** for quick and easy access when needed.

3. It is optional to fill-out the **(4)-Factor Breach Assessment Sheet**. You may want to keep a copy of the report in your HIPAA Manual and place a copy in the appropriate patient charts.
   If you determine that you must report your breach, we urge you to do so most all of the time, do so by reporting the breach incident directly to: The ***Secretary of U. S. Department of Human Health Services*** using this electronic link:
   http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
   (If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)
   Major Breach Protocols also requires: *Report to Media:* Newspaper, Radio & TV; Notify media as a Press Release; This notice must be within 60 days of discovery of a Major HIPAA Breach & must include the same information required for the individual notice.

4. If your breach incident involves a group of patients you may need to notify **(OCR)** Office of Civil Rights, media, or other parties. Check immediately with the U.S. Dept. of Health & Human Services **(HHS)** or a legal professional specializing in this area of law for guidance in these matters. **HealthFirst** provides use-ful introductions and overviews to the law but will not consult or advise in matters of breach occurrences.

(4)-Factor Breach Assessment Sheet for HIPAA Omnibus Rule PHI Breach Determination

(This file is also available on your training HIPAA On-Line Portal in the **Omnibus Rule eForms** folder)

Date of Incident: _____

Name of Patient at Risk: _____

Type of PHI breached:

❑ paper / mail ❑ email ❑ fax ❑ phone ❑ conversation ❑ visual ❑ theft ❑ hacking

❑ other, describe: _____

Brief description of incident: _____

_____

_____

Check "**Yes**" or "**No**" for the breached situation you are evaluating:

RISK FACTORS		
#1 PHI INVOLVED—Is this PHI likely to be identified and linked easily to the patient?		
SENSITIVE / HIGH RISK PHI: Includes any of these… Name, Address, Email Address, Full Face Photo, Name with Lab Results Phone Number, Credit Card Number, Web Address, Finger Print Social Security Number, License Number, Vehicle ID, Medical Device ID	**Yes** ❑	**No** ❑
#2 RECIPIENT of the PHI—Is recipient authorized to receive PHI? Examples of **Safe Recipients:** Doctor or Health Facility, Insurance Carrier, Patient, Pharmacy, Authorized Legal Representative, Your Employee, Your Business Associate, Our Business Associates Subcontractor, Your Patient	**Yes** ❑	**No** ❑
UNSAFE RECIPIENT / HIGH RISK: Includes any of these… Un Known Stolen Hacked-Into Known but not Business Associate Known but not Patient	**Yes** ❑	**No** ❑
#3 PHI ACQUIRED / VIEWED—Was the PHI acquired & viewed?	**Yes** ❑	**No** ❑
Unsafe recipient received PHI	**Yes** ❑	**No** ❑
Safe recipient received & viewed PHI	**Yes** ❑	**No** ❑
#4 PHI MITIGATION **UNSAFE PHI: Includes any of these…** Not Traceable Not Retrievable UNABLE to mitigate Lost Stolen Hacked-Into	**Yes** ❑	**No** ❑
If the PHI *can be located and suppressed* it will be considered *diffused*. Locate by a: phone call, email, letter, text to confirm correspondence; PHI needs to be destroyed!	**Yes** ❑	**No** ❑

Since there are no "quantifiable parameters", we advise you to Report most everything

1 Yes = **Report this Breach**
2 Yes = **Report this Breach**
3 Yes = **Report this Breach**
4 Yes = **Report this Breach**
5 Yes = **Report this Breach**

Breaches of PHI need to be reported to:

The ***Secretary of U. S. Department of Human Health Services*** using this electronic link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Major Breach Protocols also requires: *Report to Media:* Newspaper, Radio & TV; Notify media as a Press Release; This notice must be within 60 days of discovery of a Major HIPAA Breach & must include the same information required for the individual notice.

HIPAA HHS
Affordable Care Act: Section 1557
Healthcare Reimbursement Requirements

If your Healthcare facility gets government reimbursement for **Medicaid, Medicare Part C / Medicare Advantage** or **State Funded Healthy Kids Programs,** www.hhs.gov requires that you **post & use (2) Notices** within your practice:

- ✔ **A Non-Discrimination Notice**
- ✔ **Taglines: That reference Free Language Translation Assistance**

The US Department of Health & Human Services provides a free resource for you and translation in 15 languages. They list a **free phone number for each language** that may need translation.

You can search for this link by using the key words: **HHS—Language Assistance Services** or by following this link: http://www.hhs.gov/civil-rights/for-individuals/language-assistance/index.html

These NON-DISCRIMINIATION & TRANSLATION TAGLINES must Appear:

- ✔ **In your Office**
- ✔ **On your Website**
- ✔ **On Office Postcards & Brochures as a shorter version** (referencing your State's Top (2) Languages)

Sample materials are also available on HHS website: http://www.hhs.gov/civil-rights/for-individuals/section-1557/trainingmaterials/index.html

For more information, visit the OCR's website and search Section 1557

Please see pages 96A – 96C for:
15 Language Translation Statement for Section 1557 Medicaid Medicare

VIII. NEW PATIENT ACCESS to ELECTRONIC RECORDS RULE

Requesting PHI for Self

Under Omnibus Rule, patients have new rights to access their electronic records. Under the ***previous HIPAA rule,*** a patient could access their records upon written request. If "readily producible" you would give the patient an electronic copy. If not "readily producible", you would give the patient a paper copy.

Under the ***new HIPAA Omnibus Rule,*** upon written request the patient should get their records in this manner: If "readily producible", you should give the patient their files ***"in the format they desire"*** (i.e.: PDF, word document, fax copy, etc.)

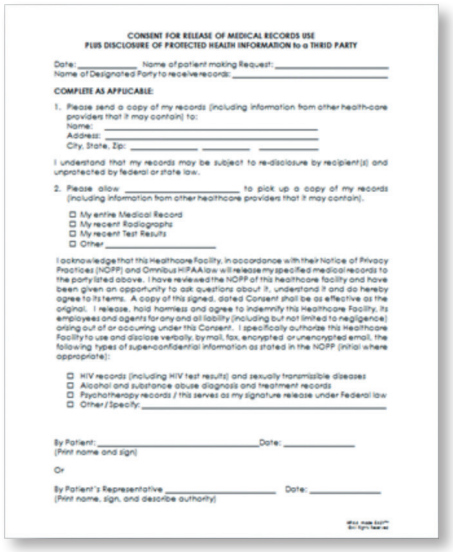
THIS IS THE ONLY CHANGE…IN THE FORMAT THEY DESIRE IF AVAILABLE.

If their records are not "readily producible in a format they desire", you should provide a comparable electronic file. For instance, if the patient is requesting their electronic files in word format (.doc), but you can only provide them in PDF, then that is what is required. Always offer a paper copy as well.

Requesting PHI for a Third Party

Omnibus Rule allows for patients to ***request their medical records be given or sent to a Third Party,*** as long as their request includes the following:

- The request must be written
- The Third Party must be designated by name
- It must be clear where the records are to be sent or picked up



CONSENT FOR RELEASE OF MEDICAL RECORDS USE
PLUS DISCLOSURE OF PROTECTED HEALTH INFORMATION to a THIRD PARTY

Date: _____ Name of patient making Request: _____
Name of Designated Party to receive records: _____

COMPLETE AS APPLICABLE:

1. Please send a copy of my records (including information from other health-care providers that it may contain) to:
Name: _____
Address: _____
City, State, Zip: _____ _____ _____

I understand that my records may be subject to re-disclosure by recipient(s) and unprotected by federal or state law.

2. Please allow _____ to pick up a copy of my records (including information from other healthcare providers that it may contain).

☐ My entire Medical Record
☐ My recent Radiographs
☐ My recent Test Results
☐ Other _____

I acknowledge that this Healthcare Facility, in accordance with their Notice of Privacy Practices (NOPP) and Omnibus HIPAA law will release my specified medical records to the party listed above. I have reviewed the NOPP of this healthcare facility and have been given an opportunity to ask questions about it, understand it and do hereby agree to its terms. A copy of this signed, dated Consent shall be as effective as the original. I release, hold harmless and agree to indemnify this Healthcare Facility, its employees and agents for any and all liability (including but not limited to negligence) arising out of or occurring under this Consent. I specifically authorize this Healthcare Facility to use and disclose verbally, by mail, fax, encrypted or unencrypted email, the following types of supercconfidential information as stated in the NOPP (initial where appropriate):

☐ HIV records (including HIV test results) and sexually transmissible diseases
☐ Alcohol and substance abuse diagnosis and treatment records
☐ Psychotherapy records / this serves as my signature release under Federal law
☐ Other / Specify: _____

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative _____ Date: _____
(Print name, sign, and describe authority)

At the back of this packet you will find an Omnibus Rule compliant, ***PATIENT CONSENT FOR RELEASE FORM*** (also in electronic format on our HIPAA On-Line Portal), you can access and revise, customize or copy-and-paste this form into an email for ease-of-use. Keep in mind that all of these new Omnibus Rule documents should also be represented in your HIPAA Manual. Make sure you have a HIPAA Manual to new Omnibus Rule standard. Get one at:

Amazon.com HIPAAomnibusrule.com HealthFirst.com

Keep in mind that the following entities have ***allowable access*** to patient PHI (with patients' approval): Attending or Referral Doctors Healthcare Facilities, Pharmacies, Health Insurance Carriers. This is considered the course- of- doing- business.

IX. NEW MARKETING & FUND-RAISING PROTOCOLS

New Limitations on the Sale of PHI

Selling PHI without authorization is strictly prohibited. There are some exceptions where remuneration for PHI is allowed under Omnibus Rule, they are:

- Public health purpose disclosure
- Treatment and payment for healthcare (limited situations)
- For the sale, transfer, merger, or consolidation of all or part of a covered entity/ healthcare facility
- To a business associate in connection with the business associate's job performance for the covered entity

- To a patient / beneficiary upon request
- Or as the law may require

Be cautious with selling PHI even under the above circumstances. **HealthFirst** suggests that you con-sult with an attorney before doing so, to ensure you are keeping with the Omnibus Rule prescribed standards. We have listed the above as stated in the Omnibus Rules but will not attempt to advise you on this topic.

Disclosure of PHI for research purposes will not be considered a "sale" if there is only a reasonable PHI transmission fee as payment received. If you, the covered entity, is to sell PHI, an authorization must state remuneration will result.

Prior to Omnibus Rule, it was permissible to sell and disclose limited data sets (a form of PHI with a number of identifiers removed in accordance with specific HIPAA requirements). This agreement is permissible until September 22, 2014, so long as the agreement is not modified within one year before that date. **HealthFirst** always suggests checking with an attorney specializing in this area of law before attempting to sell or agree to receive payment for PHI of any type.

New Limitations for Marketing with PHI

Marketing is defined as "a communication about a product or service that encourages the recipient to purchase / use the product or service". In day-to-day practice, healthcare practitioners may currently use patient PHI to "market" a variety of alternative therapies or products, without obtaining authorization from the patient or beneficiary. Under Omnibus Rule this interaction is now limited. Now, within the confines of Omnibus Rule, recommending products or services (from a third party), for which you, (the covered entity), receives remuneration, you must first obtain authorization to use PHI (from the patient) to make any treatment and healthcare recommendations. For instance, you may register your patients to obtain supplements from a company that also pays you a commission. If employees receive commissions on dispensed products, the patient now needs to know commissions are received.

The easiest way to accomplish this is to add a statement explaining that you participate in such business activity, onto your ***HIPAA Patient Acknowledgement*** form. The following is an example of such a statement:

"In signing this ***HIPAA Patient Acknowledgement Form,*** you acknowledge and authorize, that this office may recommend products or services to promote your improved health. This office may or may not receive third party remuneration from these affiliated companies. We, under current HIPAA Omnibus Rule, provide you this information with your knowledge and consent."

You will find this paragraph contained on the ***HIPAA Patient Acknowledgement*** form in the back of this packet and within the eForms section on our HIPAA On-Line Portal. We encourage you to leave this paragraph in place should your facility participate in third party remuneration programs or promotions. You can customize the verbiage but must inform patients if you participate in such programs that provide you remuneration. Similarly, Business Associates who receive remuneration need to get patient authorization, even if the covered entity gets no direct remuneration.

There are (4) other important limitations now under Omnibus Rule that may affect you, they are:

1. **Refill Reminders** are excluded. The remuneration for this reminder service must be "reasonably related to the covered entity's cost". Costs are limited to labor, supplies, and postage. Other things considered "Refill Reminders" are:
   - Communications about Generic Equivalents
   - Adherence to Take Medication as Directed
   - Self-Administered Drugs / Biologics, Delivery Systems (i.e.: insulin pump)
2. **Face-to-Face Marketing** these communications are not subject to the authorization requirement (i.e. handing a patient a pamphlet or brochure)

3. **Promotional Gifts of Nominal Value** are not subject to the authorization requirement.
4. **In-Kind Payments** or payments to implement a disease management program are permissible.

New Fund-Raising Rules regarding PHI

Fundraising Rules under Omnibus can be used without the patient having to authorize and know these factors about the fund raising efforts:

- Department of service information (the particular department of your Facility that's participating)
- Identity of the particular physician
- Health Insurance status

Healthcare providers / Covered Entities should still note Fund-Raising protocols in their new ***Notice of Privacy Practices.*** Patients must be given the opportunity to "opt-out" of receiving future fundraising communications in the ***NOPP.*** You must not be influenced to treat or not treat a patient based on their decision to participate or be included in your fundraising efforts. We have provided this "opt-out" function in both your new ***Omnibus Rule NOPP*** and ***HIPAA Patient Acknowledgement*** forms.

New Regulations on the Use of PHI in Research

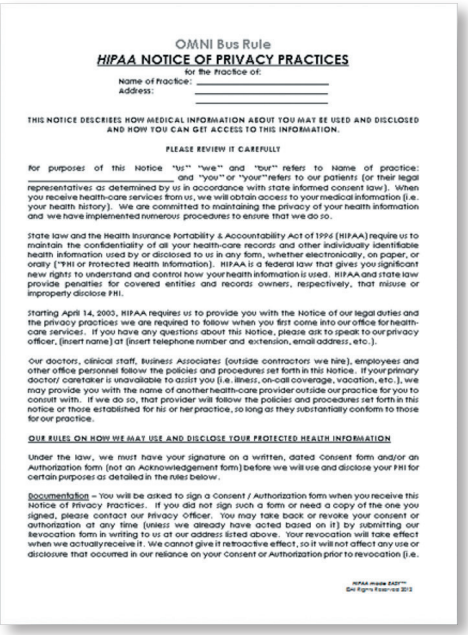
Omnibus Rule changes (2) components with regards to "authorizations for the use or disclosure of PHI for research":

1. **HHS** before did not want to authorize use of PHI for ***future*** research, without another authorization being issued, at that later time. Now HHS will consider these valid, if they adequately describe the future uses.
2. Compound authorizations for research have been changed. When used, compound authorizations, must differentiate between conditioned and unconditioned components.

HealthFirst suggests you consult an attorney specializing in this area of law if you are going to participate in research with your PHI. Be sure you obtain legal guidance in this very specialized area. **HealthFirst** will in no way make recommendation or comment in the areas of the Use of PHI in Research.

X. NEW ADDITIONS TO NOTICE OF PRIVACY PRACTICES (NOPP)

There are some specific changes in the new Omnibus Rule regarding what is required to include / exclude in your offices' **Notices of Privacy Practices (NOPPs)** and how to communicate these to your patients. All Patients have the "Right-to-Know" your HIPAA Privacy Practices.
A newly revised copy of the **Notices of Privacy Practices (NOPPs)** is included at the end of this packet (also available in electronic format on our HIPAA On-Line Portal. Get access via this link: https://www.healthfirst.com/ontraq/. Please read and review the NOPP thoroughly so that your entire staff can discuss and explain the current changes and additions to this document. It is required that you display this new **NOPP** in your facility to make it available for your patients to view and read. Provide a hard copy to patients should they ask for one. We offer a book-bound version of the **NOPP** (available on all of our websites), should you want a more sturdy copy for your reception room. (Find the ***book-bound NOPP*** at: HealthFirst.com HIPAAomnibusrule.com



OMNI Bus Rule

HIPAA NOTICE OF PRIVACY PRACTICES

for the Practice of:

Name of Practice: _____

Address: _____

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE REVIEW IT CAREFULLY

For purposes of this Notice "Us" "we" and "Our" refers to Name of practice: _____ and "you" or "your" refers to our patients (or their legal representatives as determined by us in accordance with state informed consent law). When you receive health-care services from us, we will obtain access to your medical information (i.e. your health history). We are committed to maintaining the privacy of your health information and we have implemented numerous procedures to ensure that we do so.

State law and the Health Insurance Portability & Accountability Act of 1996 (HIPAA) require us to maintain the confidentiality of all your health-care records and other individually identifiable health information used by or disclosed to us in any form, whether electronically, on paper, or orally ("PHI or Protected Health Information). HIPAA is a federal law that gives you significant new rights to understand and control how your health information is used. HIPAA and state law provide penalties for covered entities and records owners, respectively, that misuse or improperly disclose PHI.

Starting April 14, 2003, HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow when you first come into our office for health-care services. If you have any questions about this Notice, please ask to speak to our privacy officer, (insert name) at (insert telephone number and extension, email address, etc.).

Our doctors, clinical staff, Business Associates (outside contractors we hire), employees and other office personnel follow the policies and procedures set forth in this Notice. If your primary doctor/ caretaker is unavailable to assist you (i.e. illness, on-call coverage, vacation, etc.), we may provide you with the name of another health-care provider outside our practice for you to consult with. If we do so, that provider will follow the policies and procedures set forth in this notice or those established for his or her practice, so long as they substantially conform to those for our practice.

OUR RULES ON HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

Under the law, we must have your signature on a written, dated Consent form and/or an Authorization form (not an Acknowledgement form) before we will use and disclose your PHI for certain purposes as detailed in the rules below.

Documentation – You will be asked to sign a Consent / Authorization form when you receive this Notice of Privacy Practices. If you did not sign such a form or need a copy of the one you signed, please contact our Privacy Officer. You may take back or revoke your consent or authorization at any time (unless we already have acted based on it) by submitting our Revocation form in writing to us at our address listed above. Your revocation will take effect when we actually receive it. We cannot give it retroactive effect, so it will not affect any use or disclosure that occurred in our reliance on your Consent or Authorization prior to revocation (i.e.

Also, it is required that you post this new NOPP on your website if you have one.

Notices of Privacy Practices (NOPPs) for all Covered Entities, going forward, must include the following:

1. Acknowledgement that the sale of PHI is prohibited
2. Acknowledgement that the use of PHI in marketing or fundraising is prohibited except with prior authorization or consent from the patient. If you plan to utilize PHI for fundraising, your patients have a right to "opt out" of receiving fundraising communications.
3. A statement if you plan to use PHI in marketing or fundraising.
4. An acknowledgement that patients can restrict disclosures to their insurance health plan for services of which they will pay "out of pocket" and in full.

Below are the additional revisions:

XI. SECURITY & PRIVACY for INTERNET & COMPUTERS

❑ **Use Updated HIPAA Software.** In 2014, Microsoft stopped updating their software to HIPAA compliant standards for free. This means if you are still using Microsoft XP, it is not HIPAA compliant. Worse yet if you use Microsoft XP paired with an internet connection, all of your patient Protected Health Information (PHI) is open to the public and internet identity thieves. Make sure you get your Microsoft software updated to Windows 7 or higher. This will ensure that you are working to the current standard for these HIPAA Omnibus Rules.

❑ **Protect your Server.** Where is your server located in your office? It's important to make it "secured". If it is out in the open, it can be prone to vulnerable to being stolen. In 2015, 48% of all Healthcare Facility HIPAA Breaches were associated with the theft of a devise. Servers, laptops and take-along data back-up drives are most vulnerable. Be sure to secure your server in a ventilated closet or purchase a "server cage" that can bolt your server into the floor or to a piece of furniture. Server cages are available from www.eaton.com.

❑ **Retire Take-Along Back Up Drives.** Take along back-up drives are not ideal for today's vulnerable Privacy & Security threats. While many healthcare facilities have traditionally used them for data back-up, in today's vulnerable, high-priced HIPAA world, they come with too high a fine if they get lost or stolen. Recent fines for stolen back-up drives can bring a healthcare facility $150K in HIPAA fines! Please make smarter choices to upgrade to automatic secure cloud back up. This is Best Practices for your healthcare facility. Do away with the take along back-up drives.

❑ **Protect your Out-Going Email.** If you send emails to patients, labs and/ or doctors, you will want to make sure any patient Protected Health Information (PHI) is secure. There are (2) ways you can accomplish this: Create a ***Written Email Verification System*** or get ***Out-Going Email Encryption Service***. We think the latter is best. While creating an "Email Verification System" within your office is valid, it is time consuming and you will need to pre-verify (in writing every email prior to using it…uggh!). Purchasing an ***Out-Going Email Encryption Service*** costs about $8-12 per month. Try www.sendinc.com, Weave, Protected Trust, iMedicore.

OTHER AREAS IMPORTANCE...

Covered Entities / must post the new NOPP on your website if you maintain one. Also display the new revised **Omnibus Rule NOPP** in a clear and prominent location within your facility (if you provide physical services on site). Make the revised notice available to patients upon request after the effective date of Omnibus Rule.

Health Insurance plans that underwrite must state in their NOPP that the plan cannot use or disclose genetic information for underwriting purposes (this excludes certain long-term care plans). Health plans that post their NOPPs on their Web sites must post Omnibus Rule changes on their sites by the effective date of Omnibus Rule, as well as by US mail. Plans that do not post their NOPPs on their web sites must provide information about Omnibus Rule changes within 60 days of the revision to their clients.

Psychotherapy Notes maintained by a Covered Entity, must state in their NOPPs that "use and disclosure" of such notes require the patient's authorization.

New exclusion / Appointment Reminders, Treatment Info or Health Benefits, notice is ***no longer required.*** Omnibus Rule considers this "the course of doing business".

REFERENCES

For HIPAA CHECKLIST MASTER & HIPAA eFORMS that you have studied within this section, please assess our HIPAA On-Line Portal. Get access via this link: https://www.healthfirst.com/ontraq/

Omnibus Rule, Final edition, January 23, 2013,

https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the

WHAT IS A COVERED ENTITY, January 2012, http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/entityhipaa.html

OXFORD DICTIONARY, 2013, Oxford University Press, oxforddictionaries.com/definition/english/omnibus

HHS Issues HIPAA/HITECH Omnibus Final Rule Ushering In Significant Changes To Existing Regulations, 04 February 2013, Proskauer's Healthcare Practice Group, http://www.mondaq.com/unitedstates/x/219454/Healthcare/HHS+Issues+HIPAAHITECH+Omnibus+Final+Rule+Ushering+in+Significant+Changes+to+Existing+Regulations

HSS Final HIPAA Omnibus Rule, February 2013, http://www.mondaq.com/unitedstates/x/219978/Healthcare/HHS+Issues+LongAwaited+Final+HIPAA+Omnibus+Rule

The New HIPAA Omnibus Rule & Your Liability, 18 February 2013, http://www.mondaq.com/unitedstates/article.asp?article_id=222172&signup=true

All Aboard the HIPAA Omnibus: Navigating the New Privacy and Security Regulations, O'Connor, Welsh, Von Briesen & Roper, S.C., February 1, 2013, http://www.natlawreview.com/article/all-aboard-hipaa-omnibus-navigating-new-privacy-and-security-regulations

Analysis of Final HIPAA Omnibus Rule: Business Associates and Business Associate Agreements, February 4, 2013, Bricker & Eckler Healthcare Practice Group, Bricker & Eckler and INCompliance, http://www.bricker.com/documents/publications/Business%20Associates%20and%20Business%20Associate%20Agreements.pdf

HIPAA Breach Notification Information: https://ocrnotifications.hhs.gov/

[1] Within HITECH Law and amended by Omnibus Rule 45 C.F.R. § 164.104 make clear that HIPAA rules pertain directly to business associates. Other applicable rules to business associates: 45 C.F.R. § 164.306 / security standards, 45 C.F.R. § 164.308 / administrative safeguards, 45 C.F.R. § 164.310 / physical safeguards, 45 C.F.R. § 164.312 / technical safeguards, 45 C.F.R. § 164.316 / policies and procedures, 45 C.F.R. § 164.502 / disclosures of PHI, and 45 C.F.R. § 164.504 / organizational requirements.

XII. HIPAA OMNIBUS RULE REQUIRED FORMS

The following are hard copies for you to view only. Please use our HIPAA On-Line Portal to gain access to PDF copies.

OMNIBUS Rule
HIPAA NOTICE OF PRIVACY PRACTICES
for the Facility of:

Name of Facility: _____

Address: _____

_____

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION under the HIPAA Omnibus Rule of 2013.

PLEASE REVIEW IT CAREFULLY

For purposes of this Notice "us" "we" and "our" refers to the Name of this Healthcare Facility: _____ _____ and "you" or "your" refers to our patients (or their legal representatives as determined by us in accordance with state informed consent law). When you receive healthcare services from us, we will obtain access to your medical information (i.e. your health history). We are committed to maintaining the privacy of your health information and we have implemented numerous procedures to ensure that we do so.

The Federal Health Insurance Portability & Accountability Act of 1996, HIPAA Omnibus Rule, (formally HIPAA 1996 & HITECH of 2004) requires us to maintain the confidentiality of your healthcare records and other identifiable patient health information (PHI) used by or disclosed to us in any form, whether electronic, on paper, or spoken. HIPAA is a Federal Law that gives you significant new rights to understand and control how your health information is used. Federal HIPAA Omnibus Rule and state laws provide penalties for covered entities, business associates, and their subcontractors and records owners respectively that misuse or improperly disclose PHI.

Starting April 14, 2003, HIPAA requires us to provide you with the Notice of our legal duties and the privacy practices we are required to follow when you first come into our office for health-care services. If you have any questions about this Notice, please ask to speak to our HIPAA Privacy Officer.

Our doctors, clinical staff, employees, Business Associates (outside contractors we hire), their subcontractors and other involved parties follow the policies and procedures set forth in this Notice. If at this facility, your primary caretaker / doctor is unavailable to assist you (i.e. illness, on-call coverage, vacation, etc.), we may provide you with the name of another healthcare provider outside our practice for you to consult with. If we do so, that provider will follow the policies and procedures set forth in this Notice or those established for his or her practice, so long as they substantially conform to those for our practice.

OUR RULES ON HOW WE MAY USE AND DISCLOSE YOUR PROTECTED HEALTH INFORMATION

Under the law, we must have your signature on a written, dated Consent Form and/or an Authorization Form of Acknowledgement of this Notice, before we will use or disclose your PHI for certain purposes as detailed in the rules below.

Documentation—You will be asked to sign an Authorization / Acknowledgement form when you receive this Notice of Privacy Practices. If you did not sign such a form or need a copy of the one you signed, please contact our Privacy Officer. You may take back or revoke your consent or authorization at any time (unless we already have acted based on it) by submitting our Revocation Form in writing to us at our address listed above. Your revocation

will take effect when we actually receive it. We cannot give it retroactive effect, so it will not affect any use or disclosure that occurred in our reliance on your Consent or Authorization prior to revocation (i.e. if after we provide services to you, you revoke your authorization / acknowledgement in order to prevent us billing or collecting for those services, your revocation will have no effect because we relied on your authorization/ acknowledgement to provide services before you revoked it).

General Rule—If you do not sign our authorization/ acknowledgement form or if you revoke it, as a general rule (subject to exceptions described below under "Healthcare Treatment, Payment and Operations Rule" and "Special Rules"), we cannot in any manner use or disclose to anyone (excluding you, but including payers and Business Associates) your PHI or any other information in your medical record. By law, we are unable to submit claims to payers under assignment of benefits without your signature on our authorization/ acknowledgement form. You will however be able to restrict disclosures to your insurance carrier for services for which you wish to pay "out of pocket" under the new Omnibus Rule. We will not condition treatment on you signing an authorization / acknowledgement, but we may be forced to decline you as a new patient or discontinue you as an active patient if you choose not to sign the authorization/ acknowledgement or revoke it.

Healthcare Treatment, Payment and Operations Rule
With your signed consent, we may use or disclose your PHI in order:

- To provide you with or coordinate healthcare treatment and services. For example, we may review your health history form to form a diagnosis and treatment plan, consult with other doctors about your care, delegate tasks to ancillary staff, call in prescriptions to your pharmacy, disclose needed information to your family or others so they may assist you with home care, arrange appointments with other healthcare providers, schedule lab work for you, etc.
- To bill or collect payment from you, an insurance company, a managed-care organization, a health benefits plan or another third party; for example, we may need to verify your insurance coverage, submit your PHI on claim forms in order to get reimbursed for our services, obtain pre-treatment estimates or prior authorizations from your health plan or provide your x-rays because your health plan requires them for payment; Remember, you will be able to restrict disclosures to your insurance carrier for services for which you wish to pay "out of pocket" under this new Omnibus Rule.
- To run our office, assess the quality of care our patients receive and provide you with customer service. For example, to improve efficiency and reduce costs associated with missed appointments, we may contact you by telephone, mail or otherwise remind you of scheduled appointments, we may leave messages with whomever answers your telephone or email to contact us (but we will not give out detailed PHI), we may call you by name from the waiting room, we may ask you to put your name on a sign-in sheet, (we will cover your name just after checking you in), we may tell you about or recommend health-related products and complementary or alternative treatments that may interest you, we may review your PHI to evaluate our staff's performance, or our Privacy Officer may review your records to assist you with complaints. If you prefer that we not contact you with appointment reminders or information about treatment alternatives or health-related products and services, please notify us in writing at our address listed above and we will not use or disclose your PHI for these purposes.
- New HIPAA Omnibus Rule does not require that we provide the above notice regarding Appointment Reminders, Treatment Information or Health Benefits, but we are including these as a courtesy so you understand our business practices with regards to your (PHI) protected health information.

Additionally, you should be made aware of these protection laws on your behalf, under the new HIPAA Omnibus Rule:

- That **Health Insurance plans** that underwrite cannot use or disclose genetic information for underwriting purposes (this excludes certain long-term care plans). Health plans that post their NOPPs on their web sites must post these Omnibus Rule changes on their sites by the effective date of the Omnibus Rule, as well as notify you by US Mail by the Omnibus Rules effective date. Plans that do not post their NOPPs on their Web sites must provide you information about Omnibus Rule changes within 60 days of these federal revisions.
- **Psychotherapy Notes** maintained by a healthcare provider, must state in their NOPPs that they can allow "use and disclosure" of such notes only with your written authorization.

Special Rules

Notwithstanding anything else contained in this Notice, only in accordance with applicable HIPAA Omnibus Rule, and under strictly limited circumstances, we may use or disclose your PHI without your permission, consent or authorization for the following purposes:

- When required under federal, state or local law
- When necessary in emergencies to prevent a serious threat to your health and safety or the health and safety of other persons
- When necessary for public health reasons (i.e. prevention or control of disease, injury or disability, reporting information such as adverse reactions to anesthesia, ineffective or dangerous medications or products, suspected abuse, neglect or exploitation of children, disabled adults or the elderly, or domestic violence)
- For federal or state government health care oversight activities (i.e. civil rights laws, fraud and abuse investigations, audits, investigations, inspections, licensure or permitting, government programs, etc.)
- In judicial and administrative proceedings and law enforcement purposes (i.e. in response to a warrant, subpoena or court order, by providing PHI to coroners, medical examiners and funeral directors to locate missing persons, identify deceased persons or determine cause of death)
- For Worker's Compensation purposes (i.e. we may disclose your PHI if you have claimed health benefits for a work-related injury or illness)
- For intelligence, counterintelligence or other national security purposes (i.e. Veterans Affairs, U.S. military command, other government authorities or foreign military authorities may require us to release PHI about you)
- For organ and tissue donation (i.e. if you are an organ donor, we may release your PHI to organizations that handle organ, eye or tissue procurement, donation and transplantation)
- For research projects approved by an Institutional Review Board or a privacy board to ensure confidentiality (i.e. if the researcher will have access to your PHI because involved in your clinical care, we will ask you to sign an authorization)
- To create a collection of information that is "de-identified" (i.e. it does not personally identify you by name, distinguishing marks or otherwise and no longer can be connected to you)
- To family members, friends and others, but only if you are present and verbally give permission. We give you an opportunity to object and if you do not, we reasonably assume, based on our professional judgment and the surrounding circumstances, that you do not object (i.e. you bring someone with you into the operatory or exam room during treatment or into the conference area when we are discussing your PHI);

we reasonably infer that it is in your best interest (i.e. to allow someone to pick up your records because they knew you were our patient and you asked them in writing with your signature to do so); or it is an emergency situation involving you or another person (i.e. your minor child or ward) and, respectively, you cannot consent to your care because you are incapable of doing so or you cannot consent to the other person's care because, after a reasonable attempt, we have been unable to locate you. In these emergency situations we may, based on our professional judgment and the surrounding circumstances, determine that disclosure is in the best interests of you or the other person, in which case we will disclose PHI, but only as it pertains to the care being provided and we will notify you of the disclosure as soon as possible after the care is completed. **As per HIPAA law 164.512(j) (i)… (A) Is necessary to prevent or lessen a serious or imminent threat to the health and safety of a person or the public and (B) Is to person or persons reasonably able to prevent or lessen that threat.**

Minimum Necessary Rule

Our staff will not use or access your PHI unless it is necessary to do their jobs (i.e. doctors uninvolved in your care will not access your PHI; ancillary clinical staff caring for you will not access your billing information; billing staff will not access your PHI except as needed to complete the claim form for the latest visit; janitorial staff will not access your PHI). All of our team members are trained in HIPAA Privacy rules and sign strict Confidentiality Contracts with regards to protecting and keeping private your PHI. So do our Business Associates (and their Subcontractors). Know that your PHI is protected by several layers of people with regards to our business relations. Also, we disclose to others outside our staff, only as much of your PHI as is necessary to accomplish the recipient's lawful purposes. Still in certain cases, we may use and disclose the entire contents of your medical record

- To you and your legal representatives (as stated above) and anyone else you list on a Consent or Authorization to receive a copy of your records
- Healthcare providers for treatment purposes (i.e. making diagnosis and deciding/agreeing with prior recommendations in the medical record)
- To the U.S. Department of Health and Human Services (i.e. in connection with a HIPAA complaint)
- To others as required under federal or state law
- To our privacy officer and others as necessary to resolve your complaint or accomplish your request under HIPAA (i.e. clerks who copy records need access to your entire medical record)

In accordance with HIPAA law, we presume that requests for disclosure of PHI from another Covered Entity (as defined in HIPAA) are for the minimum necessary amount of PHI to accomplish the requestor's purpose. Our Privacy Officer will individually review unusual or non-recurring requests for PHI to determine the minimum necessary amount of PHI and disclose only that. For non-routine requests or disclosures, our Privacy Officer will make a minimum necessary determination based on, but not limited to, the following factors:

- The amount of information being disclosed
- The number of individuals or entities to whom the information is being disclosed
- The importance of the use or disclosure
- The likelihood of further disclosure
- Whether the same result could be achieved with de-identified information
- The technology available to protect confidentiality of the information

- The cost to implement administrative, technical and security procedures to protect confidentiality

If we believe that a request from others for disclosure of your entire medical record is unnecessary, we will ask the requestor to document why this is needed, retain that documentation and make it available to you upon request.

Incidental Disclosure Rule
We will take reasonable administrative, technical and security safeguards to ensure the privacy of your PHI when we use or disclose it (i.e. we shred all paper containing PHI, require employees to speak with privacy precautions when discussing PHI with you, we use computer passwords and change them periodically (i.e. when an employee leaves us), we use firewall and router protection to the federal standard, we back up our PHI data off-site and encrypted to federal standard, we do not allow unauthorized access to areas where PHI is stored or filed and/or we have any unsupervised business associates sign Business Associate Confidentiality Agreements).

However, in the event that there is a breach in protecting your PHI, we will follow Federal Guide Lines to HIPAA Omnibus Rule Standard to first evaluate the breach situation using the Omnibus Rule, 4-Factor Formula for Breach Assessment. Then we will document the situation, retain copies of the situation on file, and report all breaches (other than low probability as prescribed by the Omnibus Rule) to the US Department of Health and Human Services at: http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html ***(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)***

We will [illegible]ke proper[illegible]ification to [illegible] and any o[illegible] parti[illegible]ificance[illegible]s required by [illegible].

Busin[illegible]s Associate Ru[illegible]
Business [illegible]ciates are [illegible]efined[illegible]s: an e[illegible]ty, [illegible]on-e[illegible]ploy[illegible]e) that[illegible] the co[illegible]se of t[illegible]eir work will c[illegible]y[illegible] directly use, transmit, [illegible]w, tr[illegible]spo[illegible]t, [illegible]r, inte[illegible]ret, p[illegible]oce[illegible]s or o[illegible]er PH[illegible] this Facility.

Busin[illegible]ciates[illegible]nd other thi[illegible]pa[illegible]es (if ar[illegible]that re[illegible]ve yo[illegible] PHI from us w[illegible]ite[illegible]sclosing it unless required to do so by law or you give prior express written consent to the re-disclosure. Nothing in our Business Associate agreement will allow our Business Associate to violate this re-disclosure prohibition. Under Omnibus Rule, Business Associates will sign a strict confidentiality agreement binding them to keep your PHI protected and report any compromise of such information to us, you and the United States Department of Health and Human Services, as well as other required entities. Our Business Associates will also follow Omnibus Rule and have any of their Subcontractors that may directly or indirectly have contact with your PHI, sign Confidentiality Agreements to Federal Omnibus Standard.

Super-confidential Information Rule
If we have PHI about you regarding communicable diseases, disease testing, alcohol or substance abuse diagnosis and treatment, or psychotherapy and mental health records (super-confidential information under the law), we will not disclose it under the General or Healthcare Treatment, Payment and Operations Rules (see above) without your first signing and properly completing our Consent form (i.e. you specifically must initial the type of super-confidential information we are allowed to disclose). If you do not specifically authorize disclosure by initialing the super-confidential information, we will not disclose it unless authorized under the Special Rules (see above) (i.e. we are required by law to disclose it). If we disclose super-confidential information (either because you have initialed the consent form or the Special Rules authorizing us to do so), we will comply with state and federal law that requires us to warn the recipient in writing that re-disclosure is prohibited.

Changes to Privacy Policies Rule
We reserve the right to change our privacy practices (by changing the terms of this Notice) at any time as authorized

by law. The changes will be effective immediately upon us making them. They will apply to all PHI we create or receive in the future, as well as to all PHI created or received by us in the past (i.e. to PHI about you that we had before the changes took effect). If we make changes, we will post the changed Notice, along with its effective date, in our office and on our website. Also, upon request, you will be given a copy of our current Notice.

Authorization Rule
We will not use or disclose your PHI for any purpose or to any person other than as stated in the rules above without your signature on our specifically worded, written Authorization / Acknowledgement Form (not a Consent or an Acknowledgement). If we need your Authorization, we must obtain it via a specific Authorization Form, which may be separate from any Authorization / Acknowledgement we may have obtained from you. We will not condition your treatment here on whether you sign the Authorization (or not).

Marketing and Fund-Raising Rules

Limitations on the disclosure of PHI regarding Remuneration
The disclosure or sale of your PHI without authorization is prohibited. Under the new HIPAA Omnibus Rule, this would exclude disclosures for public health purposes, for treatment / payment for healthcare, for the sale, transfer, merger, or consolidation of all or part of this facility and for related due diligence, to any of our Business Associates, in connection with the business associate's performance of activities for this facility, to a patient or beneficiary upon request, and as required by law. In addition, the disclosure of your PHI for research purposes or for any other purposes permitted by HIPAA will not be considered a prohibited disclosure if the only reimbursement received is "a reasonable, cost-based fee" to cover the cost to prepare and transmit your PHI which would be expressly permitted by law. Notably, under the Omnibus Rule, an authorization to disclose PHI must state that the disclosure will result in remuneration to the Covered Entity.

Limitation on the use of PHI for Paid Marketing
We will, in accordance with Federal and State Laws, obtain your written authorization to use or disclose your PHI for marketing purposes, (i.e.: to use your photo in ads) but not for activities that constitute treatment or healthcare operations. To clarify, ***Marketing*** is defined by HIPAA's Omnibus Rule, as "a communication about a product or service that encourages recipients . . . to purchase or use the product or service." A communication is not considered "marketing" if it is in writing and if we do not receive direct or indirect remuneration from a third party for making the communication.

Under Omnibus Rule we will obtain your written authorization prior to using your PHI for making any treatment or healthcare recommendations, should financial remuneration for making the communication be involved from a third party whose product or service we might promote (i.e.: businesses offering this facility incentives to promote their products or services to you). This will also apply to our Business Associate who may receive such remuneration for making a treatment or healthcare recommendations to you.

We must clarify to you that financial remuneration does not include "in-kind payments" and payments for a purpose to implement a disease management program. Any promotional gifts of nominal value are not subject to the authorization requirement.

The Privacy Rule expressly excludes from the definition of "marketing" refill reminders or other communications about a drug or biologic that is currently being prescribed for you, provided that the financial remuneration received by us in exchange for making the communication, if any, is reasonably related to our cost of making the communication. Face-to-face marketing communications, such as sharing with you, a written product brochure or pamphlet, is permissible under current HIPAA Law.

Flexibility on the Use of PHI for Fund-Raising

Under the HIPAA Omnibus Rule, covered entities were provided more flexibility concerning the use of PHI for fund raising efforts. However, we will offer the opportunity for you to "opt out" of receiving future fund-raising communications. Simply let us know that you want to "opt out" of such situations. There will be a statement on your ***HIPAA Patient Acknowledgement Form*** where you can choose to "opt out". Our commitment to care and treat you will in no way effect your decision to participate or not participate in our fund raising efforts.

Improvements to Requirements for Authorizations Related to Research

Under HIPAA Omnibus Rule, we may seek authorizations from you for the use of your PHI for future research. However, we would have to make clear what those uses are in detail.

YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

If you received this Notice via email or website, you have the right to get, at any time, a paper copy by asking our Privacy Officer. Also, you have the following additional rights regarding PHI we maintain about you:

To Inspect and Copy

You have the right to see and get a copy of your PHI including, but not limited to, medical and billing records by submitting a written request to our Privacy Officer. Original records will not leave the premises, will be available for inspection only during our regular business hours, and only if our Privacy Officer is present at all times. You may ask us to give you the copies in a format other than photocopies (and we will do so unless we determine that it is impractical) or ask us to prepare a summary in lieu of the copies. We may charge you a fee not to exceed state law to recover our costs (including postage, supplies, and staff time for application, but excluding staff time for search and retrieval) to duplicate or summarize your PHI. We will not condition release of the copies on payment of your outstanding balance for professional services (if you owe). We will comply with Federal Law to provide your PHI in an electronic form with the 30 days, to Federal specification, when you provide us with proper written request. Paper copy will also be made available. We will respond to requests in a timely manner, without delay for legal review, or, if less than thirty days if submitted in writing, and in ten business days or less if malpractice litigation or pre-suit production is involved. We may deny your request in certain limited circumstances (i.e. we do not have the PHI, it came from a confidential source, etc.). If we deny your request, you may ask for a review of that decision. If required by law, we will select a licensed health-care professional (other than the person who denied your request initially) to review the denial and we will follow his or her decision.

To Request Amendment / Correction

If you think PHI we have about you is incorrect, or that something important is missing from your records, you may ask us to amend or correct it (so long as we have it) by submitting a **"Request for Amendment / Correction"** form to our Privacy Officer. We will act on your request within 30 days from receipt but we may extend our response time (within the 30-day period) no more than once and by no more than 30 days, or as per Federal Law allowances, in which case we will notify you in writing why and when we will be able to respond. If we grant your request, we will let you know within five business days, make the changes by noting (not deleting) what is incorrect or incomplete and adding to it the changed language, and send the changes within 5 business days to persons you ask us to and persons we know may rely on incorrect or incomplete PHI to your detriment. We may deny your request under certain circumstances (i.e. it is not in writing, it does not give a reason why you want the change, we did not create the PHI you want changed (and the entity that did can be contacted), it was compiled for use in litigation, or we determine it is accurate and complete). If we deny your request, we will (in writing within 5 business days) tell you why and how to file a complaint with us if you disagree, that you may submit a written disagreement with our denial (and we may submit a written rebuttal and give you a copy of it), that you may ask us to disclose your initial request and our denial when we make future disclosure of PHI pertaining to your request, and that you may complain to us and the U.S. Department of Health and Human Services.

To an Accounting of Disclosures

You may ask us for a list of those who got your PHI from us by submitting a **"Request for Accounting of Disclosures"** form to us. The list will not cover certain disclosures (i.e. PHI given to you, given to your legal representative, given to others for treatment, payment or health-care-operations purposes). Your request must state in what form you want the list (i.e. paper or electronically) and the time period you want us to cover, which may be up to but not more than the last six years. If we maintain your PHI in an electronic health record, then we must provide you with routine disclosures of PHI, including disclosures of treatment, payment or healthcare operations, for the 3-year period prior to the date of the request. If you ask us for this list more than once in a 12-month period, we may charge you a reasonable, cost-based fee to respond, in which case we will tell you the cost before we incur it and let you choose if you want to withdraw or modify your request to avoid the cost.

To Request Restrictions

You may ask us to limit how your PHI is used and disclosed (i.e. in addition to our rules as set forth in this Notice) by submitting a written **"Request for Restrictions on Use, Disclosure"** form to us (i.e. you may not want us to disclose your surgery to family members or friends involved in paying for our services or providing your home care). If we agree to these additional limitations, we will follow them except in an emergency where we will not have time to check for limitations. Also, in some circumstances we may be unable to grant your request (e.g. we are required by law to use or disclose your PHI in a manner that you want restricted).

To Request Alternative Communications

You ma[illegible]o commu[illegible]te with yo[illegible] different [illegible]or at a[illegible]lace b[illegible]ubmitting a [illegible]**quest for A[illegible]rnative Commu[illegible]ion"** Form[illegible]s. We wi[illegible]n[illegible] ask y[illegible] why ar[illegible]we w[illegible] accommod[illegible]e all reasonable reque[illegible](which may in[illegible]ude[illegible]o send a[illegible]po[illegible]tment [illegible]em[illegible]ders i[illegible]closed e[illegible]elop[illegible]s rather thar[illegible]y postcards, to send you[illegible]to a pos[illegible]ffice b[illegible]x instea[illegible]of y[illegible]ur ho[illegible]e a[illegible]ress, [illegible]comm[illegible]icate [illegible]th you at a te[illegible]umber other than yo[illegible]nom[illegible]. You m[illegible]t tell[illegible]s th[illegible]alte[illegible]ative [illegible]ans or locatio[illegible]ou want us t[illegible]use and explain to our satisfac[illegible]n h[illegible]v payme[illegible]o us [illegible]ll be r[illegible] if we [illegible]mmu[illegible]cate with you [illegible]you request

To Complain or Get More Information

We will follow our rules as set forth in this Notice. If you want more information or if you believe your privacy rights have been violated (i.e. you disagree with a decision of ours about inspection / copying, amendment / correction, accounting of disclosures, restrictions or alternative communications), we want to make it right. We never will penalize you for filing a complaint. To do so, please file a formal, written complaint within 180 days with:

The U.S. Department of Health & Human Services Office of Civil Rights
200 Independence Ave., S.W., Washington, DC 20201
877.696.6775

Or, submit a written Complaint form to us at the following address:

Our Privacy Officer: _____ Office Name: _____

Office Address: _____

Office Phone: _____ Ext.:_____ Office Fax: _____

Email Address: _____

You may get your **"HIPAA Complaint"** form by calling our privacy officer.

These privacy practices are in accordance with the original HIPAA enforcement effective April 14, 2003, and undated to Omnibus Rule effective September 23, 2013 and will remain in effect until we replace them as specified by Federal and/or State Law.

HIPAA OMNIBUS RULE
BUSINESS ASSOCIATES AGREEMENT
under OMNIBUS RULE

"A Business Vendor Confidentiality Agreement"

This document is required to be signed by the Business Associate and maintained on file by Covered Entity to comply with Omnibus Rule of 2013, and Effective March 26, 2013. Signatures need to be made by:

September 23, 2013 for new Business Associates Agreements, or, if after this date, at inception of the business date.

September 22, 2014 for Business Associate Agreements currently on-file. This new version needs to be signed and kept on-file.

BUSINESS ASSOCIATES ARE URGED TO GET AND USE THEIR OWN SUB CONTRACTORS AGREEMENTS. WE URGE YOU TO NOT GET INVOLVED IN THAT PROCESS OR YOU MAY BECOME LIABLE FOR ANY NON-COMPLIANT ACTIVITIES.

Term

The Term of this Agreement shall be effective as of _____ **(Today's Date),** and shall terminate upon the date that Covered Entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

Definitions

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Healthcare Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific definitions:

(a) Business Associate. ***"Business Associate"*** shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____ _____ **(Name of Vendor / Business Associate).**

(b) Covered Entity. ***"Covered Entity"*** shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean _____ _____ **(Name of Your Healthcare Facility / Covered Entity).**

(c) HIPAA Rules. ***"HIPAA Rules"*** shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Obligations and Activities of Business Associate

_____ **(Business Vendor)** agrees to:

(a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;

(b) Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;

(c) Report to Covered Entity any use or disclosure of PHI protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; The Business Associate, *will report these immediately or not more than 5 business days after such a discovery.*

The Business Associate *will handle breach notifications to individuals, the HHS Office for Civil Rights (OCR), and potentially the media*, on behalf of the Covered Entity *as its own breach*. Reporting is made to: HHS at this link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;

(e) Make available PHI (protected health information) in a designated record set to the "Covered Entity" as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524;

The Business Associate will respond to a request for access that the Business Associate receives directly from an individual for responsive business purpose, this will be either ***via email, (read-receipt option) and /or via registered mail, within 5 business days of a request.***

(f) The Business Associate will make any amendment(s) to PHI protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526; and:

The Business Associate will respond to a ***request for amendment*** when received directly from the individual either ***via email, (read-receipt option) and /or via registered mail, within 5 days*** of a request and the Business Associate will forward the individual's request to the Covered Entity ***with any amendments*** to the information in the designated record set will be incorporated.

(g) Maintain and make available the information required to provide an ***accounting of disclosures*** to the Covered Entity and also to the Individual, as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528;

The Business Associate will respond to a request for accounting of disclosures when received directly from the individual either ***via email, (read-receipt option) and /or via registered mail, either, within 5 days*** of a request ***and*** the Business Associate will ***forward the individual's request to the Covered Entity*** with any ***Accounting of Disclosures*** to the information in the designated record set will be incorporated.

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and

(i) The Business Associate will make its internal practices, books, and records available to legal inspectors, The HHS and Covered Entity for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business Associate may only use or disclose PHI protected health information pertaining only to situations that deem it necessary to perform the services set forth in the Business Associates & Covered Entities governing Service Agreement/ Contract.

In addition to other permissible purposes, the Business Associate is authorized to use PHI protected health information to ***de-identify the information*** in accordance with 45 CFR 164.514(a)-(c). The Business Associate may de-identify the information, permitted uses and disclosures by means legal and necessary to formulate this identity.

(b) Business Associate may use or disclose PHI protected health information as required by law.

(c) Business Associate agrees to make uses and disclosures and requests for PHI protected health information in timely and legal fashion consistent with Covered Entity's minimum necessary policies and procedures, which are defined as: the *least* effort and information disclosure necessary to complete this task.

(d) Business Associate may not use or disclose PHI protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below:

(e) Business Associate may use PHI protected health information for the proper management and administration to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law and that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed. Notifications will be made to the Business Associate of any instances in which the confidentiality of the PHI information has been breached.

(f) Business Associate may provide data aggregation services relating to the healthcare operations of the Covered Entity.

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions

(a) Covered Entity may notify Business Associate of any limitation(s) in the Notice of Privacy Practices of Covered

Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI protected health information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her PHI protected health information, to the extent that such changes may affect Business Associate's use or disclosure of PHI protected health information.

(c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that covered entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI protected health information.

Permissible Requests by Covered Entity

Covered Entity ***shall not request*** Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity. The exception would be if the Business Associate will use or disclose PHI protected health information for, data aggregation or management and administration and legal responsibilities of the Business Associate.

Termination

(a) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement (and Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity).

(b) Obligations of Business Associate Upon Termination.
Business Associate shall retain no copies of the protected health information except to use or disclose PHI protected health information for its own management and administration or to carry out its legal responsibilities and the Business Associate needs to retain PHI protected health information for such purposes after termination of the agreement.

Upon termination of this Agreement for any reason, Business Associate, with respect to PHI protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that PHI protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
2. Return to covered entity or destroy the remaining PHI protected health information that the Business Associate still maintains in any form;
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI electronic protected health information to prevent use or disclosure of the PHI protected health information, other than as provided for in this Section, for as long as Business Associate retains the PHI protected health information;
4. Not use or disclose the PHI protected health information retained by Business Associate other than for the

purposes for which such PHI protected health information was retained and subject to the same conditions set in the Permitted Uses and Disclosures by Business Associate sections (e) and (f) of this document, applied prior to termination; and

5. Return to Covered Entity or destroy the PHI protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

The Business Associate may be asked by the Covered Entity to transmit the PHI protected health information to another Business Associate of the Covered Entity at termination. The Business Associate would comply, confirm the transfer and then ensure the destruction of PHI protected health information created, received, or maintained by subcontractors.

(c) Survival. The obligations of Business Associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) Amendment. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law or law changes.

(b) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules by the Business Associates legal counsel.

This document was replicated from The Omnibus Rule model form is available at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

BUSINESS ASSOCIATES ADDENDUM
SIGNATURE PAGE—(RETAIN ON FILE)

THIS SIGNATURE PAGE—ADDENDUM (hereafter "Addendum") is entered into this _____ day of _____, 20_____, by and between _____ (hereafter "Business Associate") and _____ (hereafter "Healthcare Facility"), for themselves and their respective successors and assigns.

WHEREAS, the parties hereto desire to modify the aforementioned Agreement to set forth the terms and conditions under which information created or received by Business Associate on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under the Health Insurance Portability and Accountability Act "Omnibus Rule" of 2013 and regulations enacted thereunder (hereafter "HIPAA");

THEREFORE, both parties, for valuable consideration from each party to the other, the receipt and sufficiency of which is hereby acknowledged, do hereby mutually agree that the Agreement shall continue in full force and effect with the following modifications and additions, to wit: (additions or modifications state below, must comply with HIPAA Omnibus Rules):

_____

_____

_____

_____

_____

_____

_____

1. Except as amended by this Addendum, all terms, conditions and covenants of the Agreement are valid, shall remain in full force and effect, and hereby are ratified and confirmed.
2. Any inconsistencies between this Addendum and the Agreement shall be governed by this Addendum.
3. A copy of this Addendum shall be as effective as the original.

IN WITNESS WHEREOF, the parties hereto have entered into this Agreement as of the date first written above.

Name of Practice (Covered Entity)

_____
Signature

_____
Print name and title

Name of Business Associate (Vendor)

_____
Signature

_____
Print name and title

For the Office of:

_____

PATIENT ACKNOWLEDGEMENT FORM FOR RECEIPT OF NOTICE OF PRIVACY PRACTICES CONSENT

You may refuse to sign this acknowledgement & authorization. In refusing we may not be allowed to process your insurance claims.

Date: _____ Patient Name: _____

HOW DO YOU WANT TO BE ADDRESSED WHEN SUMMONED FROM RECEPTION AREA:

❑ First Name Only ❑ Proper Surname ❑ Other _____

PLEASE LIST ANY OTHER PARTIES WHO ARE ACTIVELY INVOLVED IN YOUR HEALTH CARE AND WHO CAN HAVE ACCESS TO YOUR HEALTH INFORMATION: (This includes step parents, grandparents and any care takers who can have access to this patient's records):

Name: _____ Relationship: _____

Name: _____ Relationship: _____

I AUTHORIZE CONTACT FROM THIS OFFICE TO **CONFIRM MY APPOINTMENTS, TREATMENT & BILLING INFORMATION** VIA:

❑ Cell Phone Confirmation
❑ Text Message to my Cell Phone
❑ Home Phone Confirmation
❑ Email Confirmation
❑ Work Phone Confirmation
❑ **Any of the Above**

I AUTHO **ORMATIO OUT MY H TH** BE CONV D VIA:

❑ Cel hone Confirmati
❑ Text essage to my l Ph e
❑ Home F Confir ation
Emai onfirma n
Work hone Co irma on
Any the A ve

I APPROVE BEIN CON ACTED AB T **SP IAL S ES, E NTS, ND RAISING E ORTS or NEW EALTH INFO** on behal thc Facility via:

❑ Phone Message
❑ Text Message
❑ Email
❑ **Any of the Above**
❑ **None of the Above** (opt out)

In signing this HIPAA Patient Acknowledgement Form, you acknowledge and authorize, that this office may recommend products or services to promote your improved health. This office may or may not receive third party remuneration from these affiliated companies. We, under current HIPAA Omnibus Rule, provide you this information with your knowledge and consent.

The undersigned acknowledges receipt of a copy of the currently effective Notice of Privacy Practices for this healthcare facility. A copy of this signed, dated document shall be as effective as the original.

_____ _____

Please ***print*** name of Patient Please ***sign*** Patient / Guardian of Patient

_____ _____

Legal Representative / Guardian Relationship of Legal Representative / Guardian

OFFICE USE ONLY

As Privacy Officer, I attempted to obtain the patient's (or representatives) signature on this Acknowledgement but did not because:

❑ It was emergency treatment
❑ I could not communicate with the patient
❑ The patient refused to sign
❑ The patient was unable to sign because
❑ Other (please describe)_____

Signature of Privacy Officer _____

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION (PHI) & MEDICAL RECORDS to a THIRD PARTY

Date: _____ Name of patient making Request: _____

Name of Designated Party to receive records: _____

COMPLETE AS APPLICABLE:

1. Please send a copy of my records for the period from _____ [insert date] to _____ [insert date] (including information from other health-care providers that it may contain) to:

Name_____

Address _____

City _____ State _____Zip_____

The purpose of this Authorization is: _____

I understand that my records may be subject to re-disclosure by recipient(s) and will no longer be protected by the HIPAA Privacy Rules.

2. Please allow _____ to pick up a copy of my records (including information from other he[illegible]care p[illegible]oviders th[illegible]may contai[illegible]

- ❑ My entire Medica[illegible]Rec[illegible]d
- ❑ M[illegible]sent Radi[illegible]raphs
- ❑ My rec[illegible] Test[illegible]
- ❑ Other _____

I specifically authorize this Healthcare Facility to disclose verbally, by mail, fax, encrypted or unencrypted email, the following types of PHI, if it is included in the records described in paragraph 1, above (initial where appropriate):

- ❑ HIV records (including HIV test results) and sexually transmissible diseases
- ❑ Alcohol and substance abuse diagnosis and treatment records
- ❑ Psychotherapy records / this serves as my signature release under Federal law
- ❑ Other / Specify: _____

This Authorization permits our Facility to use or disclose your Protected Health Information for purposes other than your treatment, payment to our Facility or the health care operations of our Facility. You have the right to revoke this Authorization by providing our Facility with written notice of revocation. The revocation will be effective upon receipt, except with respect to uses or disclosures made prior to receipt and in reliance upon this Authorization.

Our Facility cannot require you to sign this Authorization as a condition to the provision of services.

This Authorization shall expire on _____, 20_____, or one year after its effective date, whichever is sooner or unless it is revoked prior to the expiration date.

By Patient:_____Date: _____
(Print name and sign)

Or

By Patient's Representative: _____Date: _____
(Print name, sign, and describe authority)

REQUEST FOR ALTERNATIVE COMMUNICATIONS

Return completed form to: Privacy Officer [insert address] _____

_____

Please note that we will not ask you why you are requesting alternative communications. Also, we may be unable to agree to accommodate your request (i.e. it is unreasonable, we do not have the technology, in an emergency). We may deliver your electronic request in the format you request, or if we do not have the software to accommodate that, in a similar electronic format. If we agree to your request, we will follow the instructions stated below until such time as you instruct us otherwise in writing. A signed, dated copy of this Request shall be as effective as the original.

COMPLETE AS APPLICABLE:

1. This request pertains to the records of _____
2. I am requesting the following alternative communications:
   - ❑ Appointment Reminder
   - ❑ Telephone Contact
   - ❑ Other _____
   - ❑ Address
   - ❑ Email ContactFax Contact

Send all written communications only to the following address:

_____

_____

_____

During business hours, contact me by telephone only at the following phone number(s):

Cell: _____

Home: _____

Other: _____

Please communicate with me only by: _____

Please communicate with me only at the following address:

_____

_____

_____

Change in Payment (explain): _____

Additional request(s): _____

Please accept this as a formal request for communication.

By Patient: _____ Date: _____
(Print name and sign)

Or

By Patient's Representative: _____ Date: _____
(Print name, sign, and describe authority)

OFFICE USE ONLY

Describe what alternative communications were denied this _____ day of _____, 20 _____

_____

Describe what alternative communications were accepted this _____ day of _____, 20 _____

_____

HIPAA HHS
Affordable Care Act: Section 1557
Healthcare Reimbursement Requirements

If your Healthcare facility gets government reimbursement for **Medicaid, Medicare Part C / Medicare Advantage** or **State Funded Healthy Kids Programs,** www.hhs.gov requires that you **post & use (2) Notices** within your practice:

- ✔ **A Non-Discrimination Notice**
- ✔ **Taglines: That reference Free Language Translation Assistance**

The US Department of Health & Human Services provides a free resource for you and translation in 15 languages. They list a **free phone number for each language** that may need translation.

You can search for this link by using the key words: **HHS—Language Assistance Services** or by following this link: http://www.hhs.gov/civil-rights/for-individuals/language-assistance/index.html

These NON-DISCRIMINIATION & TRANSLATION TAGLINES must Appear:

- ✔ **In your Office**
- ✔ **On your Website**
- ✔ **On Office Postcards & Brochures as a shorter version** (referencing your State's Top (15) Languages) (See pages 96a – 96c)

Sample materials are also available on HHS website: http://www.hhs.gov/civil-rights/for-individuals/section-1557/trainingmaterials/index.html
For more information, visit the OCR's website and search Section 1557
Please see pages 96A – 96C for:
15 Language Translation Statement for Section 1557 Medicaid Medicare

Web, Social Media & Photo Release Form

_____ has my permission to have his/her dental work and/
(Patient Name)

or photographs posted within our dental practice and/or on our website, social media accounts, videos or slide shows presentations, print ads and all other marketing or advertising efforts that promote our dental practice.

_____ _____
(Parent / Guardian Signature) (Patient Signature)
(Over 18 years / Patient Signature)

BREACH ASSESSMENT FORMS

For use to evaluate & document breach occurrences.

**PLEASE USE THE TAB DIVIDER PROVIDED
AND PLACE THE FOLLOWING PAGE
IN YOUR HIPAA MANUAL FOR FUTURE USE
(make more copies as needed)**

Report breaches to:

The Secretary of U. S. Department of Human Health Services using this electronic link:
http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html
(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Breaches involving a group of patients may involve notifying (OCR) Office of Civil Rights, media, or other parties. Check with the U.S. Dept. of HHS or legal representative specializing in this area of law for guidance in these matters.

YOU ARE NOT REQUIRED TO USE THE FOLLOWING FORMS FOR BREACH REPORTING. AUTOMATED REPORTING IS MADE EASY BY FOLLOWING THE LINK ABOVE.

(4)-Factor Breach Assessment Sheet for HIPAA Omnibus Rule PHI Breach Determination

(This file is also available on your training HIPAA On-Line Portal in the **Omnibus Rule eForms** folder)

Date of Incident: _____

Name of Patient at Risk: _____

Type of PHI breached:

❑ paper / mail ❑ email ❑ fax ❑ phone ❑ conversation ❑ visual ❑ theft ❑ hacking

❑ other, describe: _____

Brief description of incident: _____

_____

_____

Check "**Yes**" or "**No**" for the breached situation you are evaluating:

RISK FACTORS		
#1 PHI INVOLVED—Is this PHI likely to be identified and linked easily to the patient?		
SENSITIVE / HIGH RISK PHI: Includes any of these… Name, Address, Email Address, Full Face Photo, Name with Lab Results; Phone Number, Credit Card Number, Web Address, Finger Print; Social Security Number, License Number, Vehicle ID, Medical Device ID	**Yes** ☐	**No** ☐
#2 RECIPIENT of the PHI—Is recipient authorized to receive PHI? Examples of ***Safe Recipients***: Doctor or Health Facility, Insurance Carrier, Patient, Pharmacy, Authorized Legal Representative, Your Employee, Other Business Associate, Our Business Associates, Subcontractor, Our Patient	**Yes** ☐	**No** ☐
UNSAFE RECIPIENTS/HIGH RISK: Includes any of these… Un Known Stolen Hacked-Into Known but not Business Associate Known but not Patient	**Yes** ☐	**No** ☐
#3 PHI ACQUIRED / VIEWED—Was the PHI acquired & viewed?	**Yes** ☐	**No** ☐
Unsafe recipient received PHI	**Yes** ☐	**No** ☐
Safe recipient received & viewed PHI	**Yes** ☐	**No** ☐
#4 PHI MITIGATION **UNSAFE PHI: Includes any of these…** Not Traceable Not Retrievable UNABLE to mitigate Lost Stolen Hacked-Into	**Yes** ☐	**No** ☐
If the PHI *can be located and suppressed* it will be considered *diffused*. Locate by a: phone call, email, letter, text to confirm correspondence; PHI needs to be destroyed!	**Yes** ☐	**No** ☐

Since there are no "quantifiable parameters", we advise you to Report most everything

1 Yes = **Report this Breach**
2 Yes = **Report this Breach**
3 Yes = **Report this Breach**
4 Yes = **Report this Breach**
5 Yes = **Report this Breach**

Breaches of PHI need to be reported to:

The ***Secretary of U. S. Department of Human Health Services*** using ***this form*** or the ***automated form*** at this electronic link:

http://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html

(If this link is broken, for updated link, Google Search: HIPAA Breach Reporting HHS)

Our Annual Data Back-Up, Contingency & Operations Assessment Report

This report is to be filled out annually by our Data Management and IT Support team:
Your IT Support Team may supply you with ***their own version*** of this report.

1. *Review of our Operation Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

2. *Review of our Risk Analysis*

   Date of Review: _____
   Evaluation reveals the need for: _____

3. *Review of our Security Analysis*

   Date of Review: _____
   Date of Review: _____
   Evaluation reveals the need for: _____

4. *Review of our Data Back- Up*

   Date of Review: _____
   Evaluation reveals the need for: _____

5. *Review of our Disaster Recovery Planning*

   Date of Review: _____
   Evaluation reveals the need for: _____

6. *Review of our Emergency Mode of Operations Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

BE SURE TO ALSO KEEP A CURRENT **WRITTEN RISK ASSESSMENT REPORT** IN ADDITION TO THIS REPORT

HIPAA CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
TO HIPAA OMNIBUS RULE STANDARD

THIS AGREEMENT entered into this_____ day of _____ , 20_____ , by and between _____ (name of Healthcare Facility), hereafter this "Healthcare Facility" and _____ (name of Affiliate Person), hereafter "Affiliate Person", sets forth the terms and conditions under which information created or received by or on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under state law and the Health Insurance Portability and Accountability Act of 1996 and updated through HIPAA Omnibus Rule of 2013 and will also uphold regulations enacted there under (hereafter "HIPAA").

THEREFORE, in consideration of the premises and the covenants and agreements contained herein, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. All parties acknowledge that meaningful employment may or will necessitate disclosure of confidential information by this Healthcare Facility to the Affiliate Person and use of confidential information by the Affiliate Person. Confidential information includes, but is not limited to, PHI, any information about patients or other employees, any computer log-on codes or passwords, any patient records or billing information, any patient lists, any financial information about this Healthcare Facility or it's patients that is not public, any intellectual property rights of Practice, any proprietary information of Practice and any information that concerns this Healthcare Facility's contractual relationships, relates to this Healthcare Facility's competitive advantages or is otherwise designated as confidential by this Healthcare Facility.

2. Disclosure and use of confidential information include oral communications as well as display or distribution of tangible physical documentation, in whole or in part, from any source or in any form (e.g., paper, digital, electronic, internet, social networks like Facebook or social network posting, magnetic or optical media, film, etc.). The parties have entered into this Agreement to induce use and disclosure of confidential information and are relying on the covenants contained herein in making any such use or disclosure. This Healthcare Facility, not the Affiliate Person, is the owner of state law and the Employee has no right or ownership interest in any confidential information.

3. Confidential information will not be used or disclosed by the Affiliate Person in violation of applicable law, including but not limited to HIPAA Federal and State records owner statute; this Agreement; the Practice's Notice of Privacy Practices, as amended; or other limitations as put in place by Practice from time to time. The intent of this Agreement is to ensure that the Affiliate Person will use and access only the minimum amount of confidential information necessary to perform the Affiliate Person's duties and will not disclose confidential information outside this Healthcare Facility unless expressly authorized in writing to do so by this Healthcare Facility. All Confidential information received (or which may be received in the future) by Affiliate Person will be held and treated by him or her as confidential and will not be disclosed in any manner whatsoever, in whole or in part, except as authorized by this Healthcare Facility and will not be used other than in connection with the Affiliate relationship.

4. The Affiliate Person understands that he or she will be assigned a log-on code or password by Practice, which may be changed as this Healthcare Facility, in its sole discretion, sees fit. The Affiliate Person will not change the log-on code or password without this Healthcare Facility's permission. Nor will the Affiliate Person leave confidential information unattended (e.g., so that it remains visible on computer screens after the Affiliate Person's use). The Affiliate Person agrees that his or her log-on code or password is equivalent to a legally-binding signature and will not be disclosed to or used by anyone other than the Affiliate Person. Nor will the Affiliate Person use or even attempt to learn another person's log-on code or password. The Affiliate Person immediately will notify this Healthcare Facility's privacy officer upon suspecting that his or her log-on code or password no longer is confidential. The Affiliate Person agrees that all computer systems are the exclusive property of Practice and will not be used by the Affiliate Person for any purpose unrelated to his or her employment. The Affiliate Person acknowledges that he or she has no right of privacy when using this Healthcare Facility's computer systems and that his or her computer use periodically will be monitored by this Healthcare Facility to ensure compliance with this Agreement and applicable law.

5. Immediately upon request by this Healthcare Facility, the Affiliate Person will return all confidential information to this Healthcare Facility and will not retain any copies of any confidential information, except as otherwise expressly permitted in writing signed by this Healthcare Facility. All confidential information, including copies thereof, will remain and be the exclusive property of this Healthcare Facility, unless otherwise required by applicable law. The Affiliate Person specifically agrees that he or she will not, and will not allow anyone working on their behalf or affiliated with the Affiliate Person in any way, use any or all of the confidential information for any purpose other than as expressly allowed by this Agreement. The Affiliate Person understands that violating the terms of this Agreement may, in this Healthcare Facility's sole discretion, result in disciplinary action including termination of Affiliation and/or legal action to prevent or recover damages for breach. Breach reporting is imperative.

6. The parties agree that any breach of any of the covenants or agreements set forth herein by the Affiliate Person will result in irreparable injury to this Healthcare Facility for which money damages are inadequate; therefore, in the event of a breach or an anticipatory breach, Practice will be entitled (in addition to any other rights and remedies which it may have at law or in equity, including money damages) to have an injunction without bond issued enjoining and restraining the Affiliate Person and/or any other person involved from breaching this Agreement.

7. This Agreement shall be binding upon and ensure to the benefit of all parties hereto and to each of their successors, assigns, officers, agents, employees, shareholders and directors. This Agreement commences on the date set forth above and the terms of this Agreement shall survive any termination, cancellation, expiration or other conclusion of this Agreement unless the parties otherwise expressly agree in writing.

8. The parties agree that the interpretation, legal effect and enforcement of this Agreement shall be governed by the laws of the State and by execution hereof, each party agrees to the jurisdiction of the courts of the State. The parties agree that any suit arising out of or relation to this Agreement shall be brought in the county where this Healthcare Facility's principal place of business is located.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have executed this Agreement on the date first above written, when signing below and after training in HIPAA law with full understanding this agreement shall stand.

Date: _____

Print Witness Name: _____

_____

(Signature of Witness of Management / Healthcare Facility)

I, the undersigned do hereby certify that I have received, read, understood and agree to abide by this Healthcare Facilities HIPAA Policies and Operating Procedures.

Date: _____

Print Affiliate Person's Name: _____

_____

(Signature of Affiliate Person to Healthcare Facility)

HIPAA BUSINESS ASSOCIATE AGREEMENT LOG

BUSINESS NAME	KEY CONTACT	ADDRESS	EMAIL ADDRESS	PHONE NUMBER	Sent BAA	Follow Up on BAA	Received BAA

BAA is Required for: (pgs 154-159)

- Confirmation Service
- Consultants, IT Tech, etc.
- Data Storage Company
- Dental Software/X-Ray Storage
- Shredding
- Property Management
- Bio-Hazard Hauler, N2/O2 Delivery, Water Delivery, Laundry, Towel or Rug Services
- Dental Supplier Reps & Repair Service

BAA is Recommended: (to be safe)

- Temp Employees
- After Hours Services
- Volunteers / Students
- After Hours Services
- Repair Maintenance Services

* Single Entities will sign a Non-Disclosure Agreement (NDA). Find NDA on page 78-79 of this manual. Keep signed and on file in this section on file in this section.

BAA *Not Necessary* for:

- Doctor-to-Doctor
- Doctor Referrals
- Pharmacy
- Insurance Company
- Conduit: UPS Fed Ex USPS
- Credit Card Processing Companies
- Labs

Considered Course-of-Doing-Business:
Sharing PHI is necessary for patient treatment
PHI sharing is to a "minimum necessary"

HIPAA CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT
PLUS EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAINING

THIS AGREEMENT entered into this_____ day of _____ , 20_____ , by and between _____ (name of Healthcare Facility), hereafter this "Healthcare Facility" and _____ (name of Employee), hereafter"Employee",sets forth the terms and conditions under which information created or received by or on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under state law and the Health Insurance Portability and Accountability Act of 1996 and updated through HIPAA Omnibus Rule of 2013 and will also uphold regulations enacted there under (hereafter "HIPAA").

THEREFORE, in consideration of the premises and the covenants and agreements contained herein, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. All parties acknowledge that meaningful employment may or will necessitate disclosure of confidential information by this Healthcare Facility to the Employee and use of confidential information by the Employee. Confidential information includes, but is not limited to, PHI, any information about patients or other employees, any computer log-on codes or passwords, any patient records or billing information, any patient lists, any financial information about this Healthcare Facility or its patients that is not public, any intellectual property rights of Practice, any proprietary information of Practice and any information that concerns this Healthcare Facility's contractual relationships, relates to this Healthcare Facility's competitive advantages, or is otherwise designated as confidential by this Healthcare Facility.

2. Disclosure and use of confidential information includes oral communications as well as display or distribution of tangible physical documentation in whole or in part, from any source or in any format (e.g., paper, digital, electronic, internet, social networks like Facebook™ or social network posting, magnetic or optical media, film, etc.). The parties have entered into this Agreement to induce use and disclosure of confidential information and are relying on the covenants contained herein in making any such use or disclosure. This Healthcare Facility, not the Employee, is the records owner under state law and the Employee has no right or ownership interest in any confidential information.

3. Confidential information will not be used or disclosed by the Employee in violation of applicable law, including but not limited to HIPAA Federal and State records owner statute; this Agreement; the Practice's Notice of Privacy Practices, as amended; or other limitations as put in place by Practice from time to time. The intent of this Agreement is to ensure that the Employee will use and access only the minimum amount of confidential information necessary to perform the Employee's duties and will not disclose confidential information outside this Healthcare Facility unless expressly authorized in writing to do so by this Healthcare Facility. All Confidential information received (or which may be received in the future) by Employee will be held and treated by him or her as confidential and will not be disclosed in any manner whatsoever, in whole or in part, except as authorized by this Healthcare Facility and will not be used other than in connection with the employment relationship.

4. The Employee understands that he or she will be assigned a log-on code or password by Practice, which may be changed as this Healthcare Facility, in its sole discretion, sees fit. The Employee will not change the log-on code or password without this Healthcare Facility's permission. Nor will the Employee leave confidential information unattended (e.g., so that it remains visible on computer screens after the Employee's use). The Employee agrees that his or her log-on code or password is equivalent to a legally-binding signature and will not be disclosed to or used by anyone other than the Employee. Nor will the Employee use or even attempt to learn another

person's log-on code or password. The Employee immediately will notify this Healthcare Facility's privacy officer upon suspecting that his or her log-on code or password no longer is confidential. The Employee agrees that all computer systems are the exclusive property of Practice and will not be used by the Employee for any purpose unrelated to his or her employment. The Employee acknowledges that he or she has no right of privacy when using this Healthcare Facility's computer systems and that his or her computer use periodically will be monitored by this Healthcare Facility to ensure compliance with this Agreement and applicable law.

5. Immediately upon request by this Healthcare Facility, the Employee will return all confidential information to this Healthcare Facility and will not retain any copies of any confidential information, except as otherwise expressly permitted in writing signed by this Healthcare Facility. All confidential information, including copies thereof, will remain and be the exclusive property of this Healthcare Facility, unless otherwise required by applicable law. The Employee specifically agrees that he or she will not, and will not allow anyone working on their behalf or affiliated with the Employee in any way, use any or all of the confidential information for any purpose other than as expressly allowed by this Agreement. The Employee understands that violating the terms of this Agreement may, in this Healthcare Facility's sole discretion, result in disciplinary action including termination of employment and/or legal action to prevent or recover damages for breach. Breach reporting is imperative.

6. The parties agree that any breach of any of the covenants or agreements set forth herein by the Employee will result in irreparable injury to this Healthcare Facility for which money damages are inadequate; therefore, in the ev[illegible]each or an[illegible]ticipatory b[illegible]ch, Practice [illegible]be en[illegible]ddition[illegible] any other rig[illegible]medies w[illegible]ch it may have at law or in equit[illegible]i[illegible]luding m[illegible]y dam[illegible]es) to h[illegible]e an[illegible]junction wit[illegible]ut bond issued e[illegible]ining and restr[illegible]ning [illegible]he Empl[illegible]ee and/or a[illegible]y o[illegible]her pe[illegible]on involv[illegible]d fro[illegible] breaching t[illegible] Agreement.

7. This Agree[illegible]ent s[illegible]ll be bi[illegible]ing up[illegible]n an[illegible]en[illegible]re to [illegible]he ben[illegible]it of all parties [illegible]ereto and to [illegible]ch of their successors, as[illegible]gns, [illegible]fficers, age[illegible]s, em[illegible]ployee[illegible]s, [illegible]areho[illegible]lders an[illegible] directors. This [illegible]greement co[illegible]mences on the d[illegible]e [illegible]orth a[illegible]ove and the [illegible]ms [illegible]f this Ag[illegible]eement [illegible]all su[illegible]ive any termin[illegible], [illegible]ella[illegible], [illegible]on or other conclusion of this Agreement unless the parties otherwise expressly agree in writing.

8. The parties agree that the interpretation, legal effect and enforcement of this Agreement shall be governed by the laws of the State in which the Healthcare Facility is located and by execution hereof, each party agrees to the jurisdiction of the courts of such State. The parties agree that any suit arising out of or relation to this Agreement shall be brought in the county where this Healthcare Facility's principal place of business is located.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have executed this Agreement on the date first above written, when signing below and after training on HIPAA Law with full understanding this agreement shall stand.

EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE PRIVACY TRAINING

The Health Insurance Portability Act of 1996 (HIPAA) requires our privacy officer to train employees on our health information privacy policies and procedures to the HIPAA Omnibus Standards of 2013 which also includes HITECH and Protected Health Information (PHI), Electronic Protected Health Information (ePHI) and Electronic Health Records (EHR). All employees with treatment, payment or healthcare operations responsibilities, which allow access to protected health information, are trained with updates periodically as State and Federal mandates require. HIPAA also requires that we keep this documentation (that the training was completed) for six years after the training.

I, the undersigned do hereby certify that I have received, read, understood and agree to abide by this Healthcare Facilities HIPAA Policies and Operating Procedures.

PRINTED NAME	SIGNATURE	DATE

HIPAA Risk Assessment & Management Analysis
+ HITECH LAW / HIPAA Security Rule Policy
EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document, I declare that I have been fully trained understand the materials and steps necessary to carry out and enforce the Risk Management & Risk Analysis Policies & Privacy/Security Practices in accordance with the HIPAA Omnibus Rules (to include HITECH LAW of 2010) for this facility. I will fully abide by these practices in accordance with our Adminis-trator and Federal Law. I understand that HIPAA Laws & Technology changes; I will participate and uphold updates for this office as management deems necessary.

DATE	PRINT NAME	SIGNATURE

EMPLOYEE TECHNOLOGY USE AGREEMENT

EMPLOYEE TRAINING OPERATIONS, MAINTENANCE & PROTECTION for

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) & ELECTRONIC HEALTH RECORDS (EHR)

HIPAA ePHI is protected as follows at this location: (check ✓ the appropriate boxes below)

1. ***Electronically printed PHI*** (patient routing slips, daily schedules, credit card & payment receipts, insurance claims) will be protected by: ☐ **We Use a** SHREDDER ☐ NOT APPLICABLE ☐ We have a SHREDDING SERVICE
2. ***Electronic Insurance Claims*** will be protected by: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
3. ***Credit Card Transmitting of PHI***: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
4. E-mail ***Transmitting of digital radiographs & PHI***: ☐ We have Email Encryption Software in place: **Name of Software:** _____ ☐ Pre-Encryption Service in place ☐ NOT APPLICABLE
5. ***E-Tronic Confirmations*** to patients (text or email): ☐ We use an *eTronic Confirmation Service* that has ROUTER & FIREWALL with ENCRYPTION ☐ We call to confirm appointments and do not use the patients full name when confirming
6. ***Computer Terminals*** from which we enter PHI: ☐ Terminals have *Unique Passwords* (protected) ☐ We can initiate *HIPAA Privacy Mode in our Software* to obscure the Pt. "last name" when patients are present ☐ Microsoft Compliant updated to ***WINDOWS Version***:_____ on all computers ☐ We do not use Microsoft.
7. **Telephone Answering System** is managed by: ☐ We have a Live-Answering Service with a signed *HIPAA Business Associates Agreement* for confidentiality ☐ Employees Take Forwarded Calls After Hours; Our employees have HIPAA training & signed Confidentiality Agreement ☐ We have a Phone Company or Voice-Over IP Service (VoIP) ☐ We use an Answering Machine
8. Individuals ***cell phones*** for business conversations and/or texting: ☐ When texting we *do not use patients full name* ☐ We have an Encrypted Texting Software on all cell phones
9. ***Faxed Documents***: ☐ We use an *iFax-Encrypted Fax Service* with a signed HIPAA Business Associates Agreement for confidentiality ☐ We do not "Fax out" & our Fax machine is under Management Supervision

HIPAA MAINTENANCE & PROTECTION of ELECTRONIC PHI for specific JOB TITLE at this location:

Job Title: _____ Name: _____ Signature: _____ Date: _____

☐ I have been trained for my job-specific Texas HB 300 HIPAA PHI & ePHI requirements

IN THE COURSE OF MY JOB, I UNDERSTAND MY RESPONSIBLITIES FOR PROPERLY EXECUTING, MAINTAINING AND PROTECTING THE FOLLOWING:
(check ✓ the appropriate boxes below that pertain to your job):

MY JOB TITLE: ↓	I use Computer Terminal for Electronic Patient Chart / Treatment Entry	I use the Office Telephone re: Patient Info	I Use a Credit Card Payment Terminal	I use my Cell Phone for Texts, Emails & Calls Involving Pt. Info	I transmit Electronic Faxes w/ Patient info	I use Office Email Account w/: Patient info	I deploy Text Confirmations w/ Pt. Info	I discard Paper w/ Patient PHI via Shredder	I submit Electronic Insurance Claims via email or fax	I update Office Internet & Software
Doctor										
Dentist										
Pharmacist										
Chiropractor										
Dental Hygienist										
Dental Assistant										
Nurse										
Physical therapist										
Massage Therapist										
Physicians Assistant										
Office Manager										
Receptionist										

New Employees: Complete this employee document within **60 days** of hire. **Existing Employees**: should update document **once every (2) years**. Completion of this form fulfills our obligation for our Technology Use Agreement and how we handle our **ELECTRONIC HEALTH RECORDS (EHR)** & **PROTECTED HEALTH INFORMATION (PHI)** withinr this office, Please see our **HITECH PACKET** for more information **HIPAA OMNIBUS RULE CHANGES NEED TO BE TRAINED ON WITH Y O UR TEAM IN A SEPARATE MODULE** REFERENCES: h p://www.nixonpeabody.com/publications_detail3.asp?ID=3915 www.HIPAA.org

XII. HIPAA RESOURCES — BIBLIOGRAPHY

Omnibus Rule, updated edition, November 2016,
http://www.hhs.gov/about/news/2013/01/17/new-rule-protects-patient-privacy-secures-health-information.html

Omnibus Rule, updated edition, November 2016,
http://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/omnibus-hipaa-rulemaking/

Omnibus Rule, Final edition, January 23, 2013,
https://www.federalregister.gov/articles/2013/01/25/2013-01073/
modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the

WHAT IS A COVERED ENTITY, Jan 2013,
http://www.hrsa.gov/healthit/toolbox/HealthITAdoptiontoolbox/PrivacyandSecurity/entityhipaa.html

OXFORD DICTIONARY, 2013, Oxford University Press,
oxforddictionaries.com/definition/english/omnibus

HHS Issues HIPAA/HITECH Omnibus Final Rule Ushering In Significant Changes To Existing Regulations,
04 February 2013, Proskauer's Health Care Practice Group,
http://www.mondaq.com/unitedstates/x/219454/Healthcare/
HHS+Issues+HIPAAHITECH+Omnibus+Final+Rule+Ushering+in+Significant+Changes+to+Existing+Regulations

HSS Final HIPAA Omnibus Rule, February 2013,
http://www.mondaq.com/unitedstates/x/219978/Healthcare/HHS+Issues+LongAwaited+Final+HIPAA+Omnibus+Rule

The New HIPAA Omnibus Rule & Your Liability, 18 February 2013,
http://www.mondaq.com/unitedstates/article.asp?article_id=222172&signup=true

All Aboard the HIPAA Omnibus: Navigating the New Privacy and Security Regulations,
O'Connor, Welsh, Von Briesen & Roper, S.C., February 1, 2013,
http://www.natlawreview.com/article/all-aboard-hipaa-omnibus-navigating-new-privacy-and-security-regulations

Analysis of Final HIPAA Omnibus Rule: Business Associates and Business Associate Agreements,
February 4, 2013, Bricker & Eckler Health Care Practice Group, Bricker & Eckler and INCompliance,
http://www.bricker.com/documents/publications/Business%20Associates%20and%20Business%20Associate%20Agreements.pdf

HIPAA Breach Notification Information:

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

http://whatishipaa.org

http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

http://www.healthlaw.org/index.php?option=com_content&view=article&id=198%3A50-
state--periodicity-schedules&catid=38&Itemid=192

[1] Within HITECH Law and amended by Omnibus Rule 45 C.F.R. § 164.104 make clear that HIPAA rules pertain directly to business associates. Other applicable rules to business associates: 45 C.F.R. § 164.306 / security standards, 45 C.F.R. § 164.308 / administrative safeguards, 45 C.F.R. § 164.310 / physical safeguards, 45 C.F.R. § 164.312 / technical safeguards,

45 C.F.R. § 164.316 / policies and procedures, 45 C.F.R. § 164.502 / disclosures of PHI, and 45 C.F.R. § 164.504 / organizational requirements.

HIPAA BUSINESS ASSOCIATE AGREEMENT LOG

BUSINESS NAME	KEY CONTACT	ADDRESS	EMAIL ADDRESS	PHONE NUMBER	Sent BAA	Follow Up on BAA	Received BAA

BAA is Required for: (pgs 154-159)

- Confirmation Service
- Consultants, IT Tech, etc.
- Data Storage Company
- Dental Software/X-Ray Storage
- Shredding
- Property Management
- Bio-Hazard Hauler, N2/O2 Delivery, Water Delivery, Laundry, Towel or Rug Services
- Dental Supplier Reps & Repair Service

BAA is Recommended: (to be safe)

- Temp Employees
- After Hours Services
- Volunteers / Students
- After Hours Services
- Repair Maintenance Services

* Single Entities will sign a Non-Disclosure Agreement (NDA). Find NDA on page 78-79 of this manual. Keep signed and on file in this section on file in this section.

BAA *Not Necessary* for:

- Doctor-to-Doctor
- Doctor Referrals
- Pharmacy
- Insurance Company
- Conduit: UPS Fed Ex USPS
- Credit Card Processing Companies
- Labs

Considered Course-of-Doing-Business:
Sharing PHI is necessary for patient treatment
PHI sharing is to a "minimum necessary"

HIPAA CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT *PLUS* EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAINING

THIS AGREEMENT entered into this_____ day of _____ , 20_____ , by and between _____ (name of Healthcare Facility), hereafter this "Healthcare Facility" and _____ (name of Employee), hereafter"Employee",sets forth the terms and conditions under which information created or received by or on behalf of this Healthcare Facility (hereafter collectively referred to as protected health information or "PHI") may be used or disclosed under state law and the Health Insurance Portability and Accountability Act of 1996 and updated through HIPAA Omnibus Rule of 2013 and will also uphold regulations enacted there under (hereafter "HIPAA").

THEREFORE, in consideration of the premises and the covenants and agreements contained herein, the parties hereto, intending to be legally bound hereby, covenant and agree as follows:

1. All parties acknowledge that meaningful employment may or will necessitate disclosure of confidential information by this Healthcare Facility to the Employee and use of confidential information by the Employee. Confidential information includes, but is not limited to, PHI, any information about patients or other employees, any computer log-on codes or passwords, any patient records or billing information, any patient lists, any financial information about this Healthcare Facility or its patients that is not public, any intellectual property rights of Practice, any proprietary information of Practice and any information that concerns this Healthcare Facility's contractual relationships, relates to this Healthcare Facility's competitive advantages, or is otherwise designated as confidential by this Healthcare Facility.

2. Disclosure and use of confidential information includes oral communications as well as display or distribution of tangible physical documentation, in whole or in part, from any source or in any format (e.g., paper, digital, electronic, internet, social networks like Facebook™ or social network posting, magnetic or optical media, film, etc.). The parties have entered into this Agreement to induce use and disclosure of confidential information and are relying on the covenants contained herein in making any such use or disclosure. This Healthcare Facility, not the Employee, is the records owner under state law and the Employee has no right or ownership interest in any confidential information.

3. Confidential information will not be used or disclosed by the Employee in violation of applicable law, including but not limited to HIPAA Federal and State records owner statute; this Agreement; the Practice's Notice of Privacy Practices, as amended; or other limitations as put in place by Practice from time to time. The intent of this Agreement is to ensure that the Employee will use and access only the minimum amount of confidential information necessary to perform the Employee's duties and will not disclose confidential information outside this Healthcare Facility unless expressly authorized in writing to do so by this Healthcare Facility. All Confidential information received (or which may be received in the future) by Employee will be held and treated by him or her as confidential and will not be disclosed in any manner whatsoever, in whole or in part, except as authorized by this Healthcare Facility and will not be used other than in connection with the employment relationship.

4. The Employee understands that he or she will be assigned a log-on code or password by Practice, which may be changed as this Healthcare Facility, in its sole discretion, sees fit. The Employee will not change the log-on code or password without this Healthcare Facility's permission. Nor will the Employee leave confidential information unattended (e.g., so that it remains visible on computer screens after the Employee's use). The Employee agrees that his or her log-on code or password is equivalent to a legally-binding signature and will not be disclosed to or used by anyone other than the Employee. Nor will the Employee use or even attempt to learn another

person's log-on code or password. The Employee immediately will notify this Healthcare Facility's privacy officer upon suspecting that his or her log-on code or password no longer is confidential. The Employee agrees that all computer systems are the exclusive property of Practice and will not be used by the Employee for any purpose unrelated to his or her employment. The Employee acknowledges that he or she has no right of privacy when using this Healthcare Facility's computer systems and that his or her computer use periodically will be monitored by this Healthcare Facility to ensure compliance with this Agreement and applicable law.

5. Immediately upon request by this Healthcare Facility, the Employee will return all confidential information to this Healthcare Facility and will not retain any copies of any confidential information, except as otherwise expressly permitted in writing signed by this Healthcare Facility. All confidential information, including copies thereof, will remain and be the exclusive property of this Healthcare Facility, unless otherwise required by applicable law. The Employee specifically agrees that he or she will not, and will not allow anyone working on their behalf or affiliated with the Employee in any way, use any or all of the confidential information for any purpose other than as expressly allowed by this Agreement. The Employee understands that violating the terms of this Agreement may, in this Healthcare Facility's sole discretion, result in disciplinary action including termination of employment and/or legal action to prevent or recover damages for breach. Breach reporting is imperative.

6. The parties agree that any breach of any of the covenants or agreements set forth herein by the Employee will result in irreparable injury to this Healthcare Facility for which money damages are inadequate; therefore, in the event of a breach or an anticipatory breach, Practice will be entitled (in addition to any other rights and remedies which it may have at law or in equity, including money damages) to have an injunction without bond issued enjoining and restraining the Employee and/or any other person involved from breaching this Agreement.

7. This Agreement shall be binding upon and ensure to the benefit of all parties hereto and to each of their successors, assigns, officers, agents, employees, shareholders and directors. This Agreement commences on the date set forth above and the terms of this Agreement shall survive any termination, cancellation, expiration or other conclusion of this Agreement unless the parties otherwise expressly agree in writing.

8. The parties agree that the interpretation, legal effect and enforcement of this Agreement shall be governed by the laws of the State in which the Healthcare Facility is located and by execution hereof, each party agrees to the jurisdiction of the courts of such State. The parties agree that any suit arising out of or relation to this Agreement shall be brought in the county where this Healthcare Facility's principal place of business is located.

IN WITNESS WHEREOF, and intending to be legally bound, the parties hereto have executed this Agreement on the date first above written, when signing below and after training on HIPAA Law with full understanding this agreement shall stand.

The Health Insurance Portability Act of 1996 (HIPAA) requires our privacy officer to train employees on our health information privacy policies and procedures to the HIPAA Omnibus Standards of 2013 which also includes HITECH and Protected Health Information (PHI), Electronic Protected Health Information (ePHI) and Electronic Health Records (EHR). All employees with treatment, payment or healthcare operations responsibilities, which allow access to protected health information, are trained with updates periodically as State and Federal mandates require. HIPAA also requires that we keep this documentation (that the training was completed) for six years after the training.

I, the undersigned do hereby certify that I have received, read, understood and agree to abide by this Healthcare Facilities HIPAA Policies and Operating Procedures.

PRINTED NAME	SIGNATURE	DATE

— HITECH LAW & HIPAA SECURITY RULE Policy —
Risk Management Analysis
EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document, I declare that I have been fully trained and understand the materials and steps necessary to carry out and enforce the Risk Management Analysis HITECH LAW Policies and Practices for this facility. I will fully abide by these practices in accordance with our Administrator and Federal law.

Date	Print Name	Signature

EMPLOYEE TRAINING ACKNOWLEDGEMENT

In signing this document, I declare that I have been fully trained understand the materials and steps necessary to carry out and enforce the Risk Management & Risk Analysis Policies & Privacy/Security Practices in accordance with the HIPAA Omnibus Rules (to include HITECH LAW of 2010) for this facility. I will fully abide by these practices in accordance with our Adminis-trator and Federal Law. I understand that HIPAA Laws & Technology changes; I will participate and uphold updates for this office as management deems necessary.

DATE	PRINT NAME	SIGNATURE

EMPLOYEE TECHNOLOGY USE AGREEMENT

EMPLOYEE TRAINING OPERATIONS, MAINTENANCE & PROTECTION for

ELECTRONIC PROTECTED HEALTH INFORMATION (ePHI) & ELECTRONIC HEALTH RECORDS (EHR)

HIPAA ePHI is protected as follows at this location: (check ✓ the appropriate boxes below)

1. ***Electronically printed PHI*** (patient routing slips, daily schedules, credit card & payment receipts, insurance claims) will be protected by: ☐ **We Use a** SHREDDER ☐ NOT APPLICABLE ☐ We have a SHREDDING SERVICE
2. ***Electronic Insurance Claims*** will be protected by: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
3. ***Credit Card Transmitting of PHI***: ☐ ROUTER & FIREWALL with ENCRYPTION ☐ NOT APPLICABLE
4. E-mail ***Transmitting of digital radiographs & PHI***: ☐ We have Email Encryption Software in place: **Name of Software:** _____ ☐ Pre-Encryption Service in place ☐ NOT APPLICABLE
5. ***E-Tronic Confirmations*** to patients (text or email): ☐ We use an *eTronic Confirmation Service* that has ROUTER & FIREWALL with ENCRYPTION ☐ We call to confirm appointments and do not use the patients full name when confirming
6. ***Computer Terminals*** from which we enter PHI: ☐ Terminals have *Unique Passwords* (protected) ☐ We can initiate *HIPAA Privacy Mode in our Software* to obscure the Pt. "last name" when patients are present ☐ Microsoft Compliant updated to ***WINDOWS Version***:_____ on all computers ☐ We do not use Microsoft.
7. **Telephone Answering System** is managed by: ☐ We have a Live-Answering Service with a signed *HIPAA Business Associates Agreement* for confidentiality ☐ Employees Take Forwarded Calls After Hours; Our employees have HIPAA training & signed Confidentiality Agreement ☐ We have a Phone Company or Voice-Over IP Service (VoIP) ☐ We use an Answering Machine
8. Individuals ***cell phones*** for business conversations and/or texting: ☐ When texting we *do not use patients full name* ☐ We have an Encrypted Texting Software on all cell phones
9. ***Faxed Documents***: ☐ We use an *iFax-Encrypted Fax Service* with a signed HIPAA Business Associates Agreement for confidentiality ☐ We do not "Fax out" & our Fax machine is under Management Supervision

HIPAA MAINTENANCE & PROTECTION of ELECTRONIC PHI for specific JOB TITLE at this location:

Job Title: _____ Name: _____ Signature: _____ Date: _____

☐ I have been trained for my job-specific Texas HB 300 HIPAA PHI & ePHI requirements

IN THE COURSE OF MY JOB, I UNDERSTAND MY RESPONSIBLITIES FOR PROPERLY EXECUTING, MAINTAINING AND PROTECTING THE FOLLOWING:
(check ✓ the appropriate boxes below that pertain to your job):

MY JOB TITLE: ↓	I use Computer Terminal for Electronic Patient Chart / Treatment Entry	I use the Office Telephone re: Patient Info	I Use a Credit Card Payment Terminal	I use my Cell Phone for Texts, Emails & Calls Involving Pt. Info	I transmit Electronic Faxes w/ Patient info	I use Office Email Account w/: Patient info	I deploy Text Confirmations w/ Pt. Info	I discard Paper w/ Patient PHI via Shredder	I submit Electronic Insurance Claims via email or fax	I update Office Internet & Software
Doctor										
Dentist										
Pharmacist										
Chiropractor										
Dental Hygienist										
Dental Assistant										
Nurse										
Physical therapist										
Massage Therapist										
Physicians Assistant										
Office Manager										
Receptionist										

New Employees: Complete this employee document within **60 days** of hire. **Existing Employees**: should update document **once every (2) years**. Completion of this form fulfills our obligation for our Technology Use Agreement and how we handle our **ELECTRONIC HEALTH RECORDS (EHR)** & **PROTECTED HEALTH INFORMATION (PHI)** withinr this office, Please see our **HITECH PACKET** for more information **HIPAA OMNIBUS RULE CHANGES NEED TO BE TRAINED ON WITH Y O UR TEAM IN A SEPARATE MODULE** REFERENCES: h p://www.nixonpeabody.com/publications_detail3.asp?ID=3915 www.HIPAA.org

Our Annual Data Back-Up, Contingency & Operations Assessment Report

This report is to be filled out annually by our Data Management and IT Support team:
Your IT Support Team may supply you with ***their own version*** of this report.

1. *Review of our Operation Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

2. *Review of our Risk Analysis*

   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

3. *Review of our Security Analysis*

   Date of Review: _____
   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

4. *Review of our Data Back- Up*

   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

5. *Review of our Disaster Recovery Planning*

   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

6. *Review of our Emergency Mode of Operations Plan*

   Date of Review: _____
   Evaluation reveals the need for: _____

   _____

   _____

BE SURE TO ALSO KEEP A CURRENT **WRITTEN RISK ASSESSMENT REPORT** IN ADDITION TO THIS REPORT

Risk Assessment Vulnerabilities Test / ePHI in Transit or at Rest
SAMPLE

The following table is part of our Risk Assessment for our facility and reviews devices that transmit ePHI or keep it at rest. It also indicates threats and vulnerabilities that could be susceptible from the environment, people or natural disasters. An Impact & Risk Rating is also included in this Assessment. Management and IT Support works to rectify all risks to keep our ePHI secure and up to current HIPAA Standards.

ePHI	Threat	Vulnerability	Precautions Taken	Likelihood	Impact	Risk
Pt Electronic Records	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls / Malware Software Updates	LOW	unlikely	LOW 1-2
Billing Software	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls /Malware Software Updates	LOW	unlikely	LOW 1-2
Scheduling	Hackers	Hacking Untrained Employees Late Updates	IT Services Firewalls / Malware Software Updates	LOW	unlikely	LOW 1-2
Email	Hackers	Hacking Phishing Untrained Employees	IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Fax	Wrong Recipient	Untrained Employees	iFax IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Cloud Storage	Hackers	Hacking Phishing	IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Computer Hard wear	Natural Disaster Fires	Out dated IT not protecting Natural Disaster Fire / Flood	IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Mobile devices	Loss Hackers	Outdated No Encryption	Do not text PHI Use Text Encryption Service	LOW	unlikely	LOW 1-2
Website	Hackers	IT not protecting	IT Services Firewalls / Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Laptops & Tablets	Hackers	Hacking Phishing Untrained Employees Theft	Encrypted Password protected Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Office Computers	Hackers	Break in Electrical Surge Flooding	Password Protected Malware / Firewalls Malware Software Updates Employee Training	LOW	unlikely	LOW 1-2
Server	Theft	Break In Inside Tampering	Stored Remotely Employee Training & Updates to Training IT Services Antivirus Protection	LOW	unlikely	LOW 1-2

Threads could include: (ex. malware and hackers, outdated software, unintentional error, hardware failure, theft and loss, flooding),

Risk Assessment Vulnerabilities Test / ePHI in Transit or at Rest
OFFICE NAME: _____

The following table is part of our Risk Assessment for our facility and reviews devices that transmit ePHI or keep it at rest. It also indicates threats and vulnerabilities that could be susceptible from the environment, people or natural disasters. An Impact & Risk Rating is also included in this Assessment. Management and IT Support works to rectify all risks to keep our ePHI secure and up to current HIPAA Standards.

ePHI	Threat	Vulnerability	Precautions Taken	Likelihood	Impact	Risk
Pt Electronic Records						
Billing Software						
Scheduling						
Email						
Fax						
Cloud Storage						
Computer Hard wear						
Mobile devices						
Website						
Laptops & Tablets						
Office Computers						
Server						

Threads could include: (ex. malware and hackers, outdated software, unintentional error, hardware failure, theft and loss, flooding),