

# TEXAS HIPAA HB 300 2024-2025

## TEXAS HB 300 HI TECH & RISK MANAGEMENT LAW PACKET



# TEXAS HB 300: EMPLOYEE TRAINING & OUR OFFICE POLICIES

The healthcare industry is in the midst of sweeping changes. Internet information sharing has made Private 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 noncompliance. 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.

Texas Governor Rick Perry set forth a mandate to enforce Texas State HIPAA Compliance for all Healthcare Professionals & Legal Entities to better protect Patient Protected Health Information (PHI) and Electronic Health Records (EHR). This mandate was effective September 1, 2012 and all Texas Employers handling PHI must re-train their employees on updated Texas HB 300 materials every two years. Proof of training is required to be kept on file. Texas HB 300 protects patient privacy on a stronger level as compared to Federal HIPAA Omnibus Rules. Non-compliance with Texas HB300 laws will bring the offenders: Harsher penalties for violations that can accumulate daily! There are (3) requirements for those businesses effected: Employee Training & Paperwork Requirements and a (15) Patient Notification Requirement for any misuse of Breach of PHI handling.

As a result of this legislation, Offices **must have a Privacy Officer appointed to conduct Risk Management Analysis (in a report, at least annually)** so that they may comply with the new “breach of PHI disclosure notification regulations” in accordance with both Texas HB 300 law and 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 Patient 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** is an unauthorized disclosure of PHI which may result in financial, reputational or other harm to the individual. The Privacy Officer would need to make decisions if breaches were to occur as to whether the disclosure would result in significant enough harm to the individual to warrant notification to that individual or to other authorities.

**We understand that Safeguards must be in place** to protect administrative, technical and physical aspects of our office.

- **Administrative Protection** encompasses 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 Protection** 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 Protection** involves 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 HITECH Privacy Procedures in accordance with Texas HB 300 in place, within our office, 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 Texas 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 **Texas HB 300 HI TECH RISK ASSESSMENT Packet** 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 Texas HB 300 law as well as Federal HIPAA Omnibus Rules.

### **BIBLIOGRAPHY**

1. Jorge Rey, Information Security Manager at Kaufman, Rossin & Co, [jrey@kaufmanrossin.com](mailto: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 Guidelines in accordance with HIPAA Law for TEXAS HB 300

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 Texas HB 300. 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 with 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** is an unauthorized disclosure of PHI which may result in financial, reputational or other harm to the individual. The Privacy Officer would need to make decisions if breaches were to occur as to whether the disclosure would result in significant enough harm to the individual to warrant notification to that individual. All breaches will be reported to the HHS breach reporting link promptly. This link is made available from our computer desktop.

### THERE ARE 18 Protected Health Information Identifiers

<ol style="list-style-type: none"><li>1. <b>Names</b></li><li>2. <b>Address</b></li><li>3. <b>Birth Dates</b></li><li>4. <b>Telephone numbers</b></li><li>5. <b>Fax numbers</b></li><li>6. <b>E- mail addresses</b></li><li>7. <b>Social security numbers</b></li><li>8. <b>Medical record numbers</b></li><li>9. <b>Credit Card Numbers</b></li><li>10. <b>Account numbers</b></li></ol>	<ol style="list-style-type: none"><li>11. <b>Certificate/License Numbers</b></li><li>12. <b>Vehicle ID / Serial Numbers</b> <small>(including license plate numbers)</small></li><li>13. <b>Device ID / Serial Numbers</b></li><li>14. <b>Web Universal Resource Locator (URL)</b></li><li>15. <b>Internet Protocol (IP) Addresses</b></li><li>16. <b>Biometric IDs</b> <small>(including finger or voice prints)</small></li><li>17. <b>Full-Face Photos / Any Comparable Images</b></li><li>18. <b>Any other unique identifying number, characteristic or code.</b></li></ol>
---	---



**Safeguards are in place** to protect administrative, technical and physical aspects of this office and are updated at least annually with our IT Specialist or our Practice Software Provider.

**Administrative Protection** would encompass how PHI is to be handled and maintained in terms of bookkeeping and accounting. Protocols are to be in place for ensuring privacy and taking seriously the ramifications of negligence, misuse or inappropriate use of PHI. (See Texas HB 300 Worksheets)

**Technical Protection** 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 both with regards to Texas State law and HIPAA Federal Laws.

**Physical Protection** involves 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 or vendors 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 Healthcare 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, the State of Texas and Federal HIPAA Law Makers, 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 this office's PHI.

## 3. LEGAL RAMIFICATIONS FOR CONFIDENTIALITY BREACHES

Employees understand that civil monetary penalties for HIPAA confidentiality violations are enforceable and that 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

In general, this office deems the term 'breach' to mean the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. 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 carrier, 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.

Exceptions to the term 'breach' does not include— Any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if the acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate, any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility or any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person

## 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.





## 8. OUR BALANCING TEST

Identification of What is at Risk: Check the appropriate answers below:

- |  |   |
|--|---|
| 1. File Cabinets containing Charts will be protected by        | <input type="checkbox"/> LOCKED OFFICE <input type="checkbox"/> LOCKED CABINETS <input type="checkbox"/> NOT APPLICABLE |
| 2. Discarded PHI Papers and forms will be protected by         | <input type="checkbox"/> SHREDDER   |
| 3. Faxed copies of information will be protected by            | <input type="checkbox"/> SHREDDER   |
| 4. Previously scanned documents will be protected by           | <input type="checkbox"/> SHREDDER   |
| 5. Inactive Patient Charts will be protected by                | <input type="checkbox"/> STORAGE / COMPUTER BACK UP   |
| 6. Obsolete Patient Schedules will be protected by             | <input type="checkbox"/> SHREDDER   |
| 7. Obsolete Patient Routing Slips will be protected by         | <input type="checkbox"/> SHREDDER   |
| 8. Employee Workstations will be protected by                  | <input type="checkbox"/> PASSWORD   |
| 9. Employee Access to Internet                                 | <input type="checkbox"/> NON-PROFESSIONAL ACTIVITY PROHIBITED   |
| 10. Employee Social Network Posting                            | <input type="checkbox"/> NON-PROFESSIONAL ACTIVITY PROHIBITED   |
| 11. Electronic Claim Submission will be protected by           | <input type="checkbox"/> ROUTER & FIREWALL <input type="checkbox"/> NOT APPLICABLE                                      |
| 12. Credit card Terminal Stations will be Protected by         | <input type="checkbox"/> ROUTER & FIREWALL <input type="checkbox"/> NOT APPLICABLE                                      |
| 13. Our Internal Database will be protected by                 | <input type="checkbox"/> DAILY BACK UP  |
| 14. Our Internet Server will be protected by                   | <input type="checkbox"/> ROUTER & FIREWALL  |
| 15. Daily Data Back-up will be protected by                    | <input type="checkbox"/> AUTOMATIC <input type="checkbox"/> OFFICE MANAGER <input type="checkbox"/> RECEPTION TEAM      |
| 16. Doctor's Smart Phone Patient Info will be protected by     | <input type="checkbox"/> DOCTOR   |
| 17. Our Telephone Answering System will be protected by        | <input type="checkbox"/> INTERNAL PHONE SYSTEM <input type="checkbox"/> MACHINE <input type="checkbox"/> OTHER          |
| 18. Our eTronic Confirmation Service will be protected by      | <input type="checkbox"/> SERVICE PROVIDER <input type="checkbox"/> NOT APPLICABLE                                       |
| 19. Emailing Patient Information will be protected by          | <input type="checkbox"/> ENCRYPTION   |
| 20. Receiving Emailed Patient Information will be protected by | <input type="checkbox"/> ENCRYPTION   |
| 21. Digital x-ray transmission will be protected by            | <input type="checkbox"/> ENCRYPTION   |
| 22. Faxed Information to Patient, Doctor, or Facility          | <input type="checkbox"/> FAX-TO-EMAIL ENCRYPTION <input type="checkbox"/> NOT APPLICABLE                                |
|  | <input type="checkbox"/> 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: \_\_\_\_\_

## 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	<input type="checkbox"/>	<input type="checkbox"/>	
E Claims	Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	<input type="checkbox"/>	<input type="checkbox"/>	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	<input type="checkbox"/>	<input type="checkbox"/>	
Work Station	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	<input type="checkbox"/>	<input type="checkbox"/>	
E mail	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	<input type="checkbox"/>	<input type="checkbox"/>	
Voicemail	Passwords used Passwords not used	<input type="checkbox"/>	<input type="checkbox"/>	
Smart Phone Devices	Passwords used Passwords not used Encryption used Encryption not used	<input type="checkbox"/>	<input type="checkbox"/>	
Website Access	Wireless Router Used Wireless Router not used Encryption used Encryption not used Passwords used Passwords not used Firewall used Firewall not used	<input type="checkbox"/>	<input type="checkbox"/>	
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	<input type="checkbox"/>	<input type="checkbox"/>	Reception Team Others per Designation
		<input type="checkbox"/>	<input type="checkbox"/>	
		<input type="checkbox"/>	<input type="checkbox"/>	
		<input type="checkbox"/>	<input type="checkbox"/>	

## 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:

Check 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.

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 \_\_\_\_\_



