

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
HIPAA AUDITS	<p>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.</p> <p>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:</p> <p>PHASE II / IN-OFFICE HIPAA AUDITS will begin in 2016. For more information, please check this link, listed to the right.</p>	<p>HIPAA Privacy, Security, and Breach Notification Audit Program HHS.gov</p> <p>Resolution Agreement In the Matter of The United States Department of Health and Human Services, Office for Civil Rights, Transaction No. 20-396202 HHS.gov</p>
HIPAA REPORTS	<p>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)</p> <ol style="list-style-type: none"> 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) <p>**Do not print the sections; Complete and save to a single computer** Upgrade to RISK ASSESSMENT made EASY Template: We will co-create this required report with you in 1 hour! Call for details: 941-587-2864</p> <p>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</p>	<p>Find This Report Template on: HIPAA On-Line Portal</p> <p>SRA Video Tutorial Link: Security Risk Assessment Videos HealthIT.gov</p> <p>SRA Tool Link: Security Risk Assessment Tool HealthIT.gov</p>
		<p>Find This Form: HIPAA On-Line Portal or HIPAA Manual: at “by year” tabs</p>
TRAINING & EMPLOYEE FORMS	<p>ADMINISTRATIVE SAFEGUARD Signed Employee Forms should be stored in Manual in “by year” organizer & Scanned to a Management Accessible Folder</p>	
	<p>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**</p> <ol style="list-style-type: none"> 1. HIPAA CONFIDENTIALITY & NON-DISCLOSURE AGREEMENT + EMPLOYEE DOCUMENTATION OF HIPAA OMNIBUS RULE TRAINING Proof-of Training Certificate. (Group Sign-In Sheet) 2. HIPAA RISK ASSESSMENT & MANAGEMENT ANALYSIS+ HI TECH LAW/ HIPAA SECURITY RULE POLICY EMPLOYEE TRAINING ACKNOWLEDGEMENT (Group Sign-In Sheet) 	<p>Video & Forms: on HIPAA On-Line Portal Re-watch video at least annually</p> <p>Find This Form on: HIPAA On-Line Portal or HIPAA Manual: 2017-2019 HIPAA Manual: pg 170-172</p>
		<p>Find This Form on: HIPAA On-Line Portal or HIPAA Manual: 2017-2018 HIPAA Manual: pg 120 or 173</p>
OFFICE FORMS	<p>ADMINISTRATIVE & PHYSICAL SAFEGUARD</p>	
	<p>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</p>	<p>Find This Form: HIPAA On-Line Portal or HIPAA Manual: BAA: 2017-2019 HIPAA Manual: pg 154-159 NDA: 2017-2019 HIPAA Manual: pg 78-79</p>
	<p>BUSINESS ASSOCIATE AGREEMENT LOG This Log will make tracking your BAA project—easy!</p>	<p>Find This Form: HIPAA On-Line Portal or HIPAA Manual: 2017-2019 HIPAA Manual: pg 169 or 176</p>
	<p>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</p>	<p>Find This Form: HIPAA On-Line Portal or HIPAA Manual: 2017-2019 HIPAA Manual: pg 160 (Healthcare) pg 161 (Pharmacies)</p>

Check-off/Done	Task to complete	Where to find
	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: 2017-2019 HIPAA Manual: pg 162
	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: 2017-2019 HIPAA Manual: pg 146-153
HIPAA MANUAL UPDATE PAGES	Update Your HIPAA Manual on (3) pages Add today's date to these pages:	2012 - 2016 MANUALS: CALL HIPAA made EASY® TO REORDER HIPAA COMPLETE PKG These versions are obsolete! 941-587-2864 2017-2019 MANUALS: DATA BACK-UP & CONTINGENCY 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 throughout 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