TMLT

Texas Medical Liability Trust

Guide to Getting Started

For Solo and Small Practices

Federal and Texas Privacy & Security Requirements
Minimizing Your Risk of Violations

Texas physicians continue to be overwhelmed by federal and state regulatory requirements. With ongoing changes to federal and Texas privacy and security rules and laws and increased numbers of reported breaches, investigations, audits and fines; physician practices must be proactive in their review of the rules to minimize their risk of violations.

TMLT is committed to helping Texas physicians comply with these regulatory requirements, which is why our Product Development and Consulting Services team created the enclosed *Privacy Toolkit*. This toolkit is designed to help minimize the impact of these privacy laws on physician practices.

Additionally, our team is available to assist you with other practice-based concerns, such as:

- EMR consultative services to improve EMR utilization and policies and procedures;
- practice reviews to augment medical documentation and to identify patient safety issues;
- CME programs in live, online/video, or home-study formats;
- risk management publications and resources, including phone consultations; and
- purchasing appropriate coverage for cyber liability, disciplinary proceedings, and employment practices liability insurance.

If we can be of further assistance to you, please call TMLT's Product Development and Consulting Services team at 1-800-580-5658 or email consultingwebmail@tmlt.org.

Sincerely,



John Devin

Vice President of Product Development and Consulting Services

Table of Contents

I. About This Guide 6

Objectives 7

Introduction 7

Overview of Federal and Texas Privacy & Security Laws 9

Covered Entity 13

HIPAA (federal) definition of a CE 13

Texas definition of a CE 13

Business Associates & Business Associate Agreements 14

II. Privacy 19

HIPAA 19

PHI 19

De-Identified Health Information. 21

Uses and Disclosures of PHI 22

Required disclosures 22

Permitted uses and disclosures 23

Authorized uses and disclosures 23

Psychotherapy Notes 28

Minimum Necessary 28

Notices and Individual Rights 30

Administrative Requirements of the HIPAA Privacy Rule 41

Organizational Options 48

Other Provisions: Personal Representatives and Minors 49

Relationship Between Federal and Texas Laws 51

III. Security 52

Security 101 53

Security Rule Implementation for Small Providers 54

Conducting a Risk Analysis 56

IV. Breach and Breach Notification 59

V. Encryption 62

VI. Mobile Devices, Texting and Remote Access 66

VII. HIPAA Privacy and Security Audits and Investigations 68

VIII. Texas Medical Records Privacy Act 70

IX. Texas Identity Theft Enforcement & Protection Act (ITEP) 72

Unauthorized Use or Possession of PII 72

Duty to Protect SPI 73

ITEP Breach Notification Requirements 74

X. Training Requirements 75

HIPAA 75

HITECH 75

Texas Medical Records Privacy Act 76

XI. Minimizing Your Risk 77

Footnotes 78

Appendices 82

TMA Survey of Texas Physicians Electronic Health Records 2012 Report 83

Sample Business Associate & Agreement List 85

Sample Business Associate Agreement 87

Sample Notice of Privacy Practices 97

Sample Notice of Privacy Practices Acknowledgment 103

The Texas Attorney General's "Authorization to Disclose PHI" 105

Security Matrix 108

Glossary 111

DISCLAIMER

The information contained in this document highlights the various laws and statutes set forth below. It does not, nor does it intend to, address all provisions of the specific laws and statutes cited herein. Further, the statutes and laws referenced in this tool are not an exhaustive list of federal and Texas privacy laws. This document is intended merely as an aid to assist physicians and their office staff in understanding their obligations under the changes to privacy provisions found in House Bill 300 (HB 300), Senate Bill 1609 (SB1609) and Senate Bill 1610 (SB 1610) as compared to the various federal privacy counterparts set forth in HIPAA/HITECH and HIPAA Omnibus Rule. TMLT makes no representation that compliance with the provisions set forth in this tool will constitute full compliance with the various federal and state privacy laws. The information presented should be used as a resource, selected and adapted with the advice of your attorney. It is distributed with the understanding that TMLT and its affiliates are not engaged in rendering legal services.

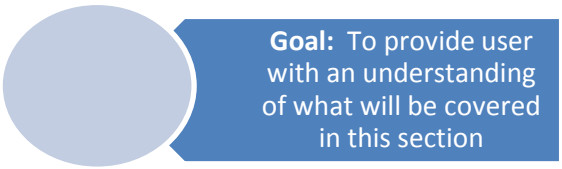
© Copyright 2013 TMLT

I. About This Guide

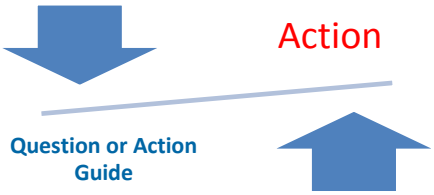
The purpose of this guide is to help physicians and their practices minimize their risk of violations from federal and Texas privacy and security laws. It is designed to guide the user through a review of the laws and requirements for physicians and their practices and identify action items and recent changes to federal and Texas laws.

Each section contains a learning objective or goal.

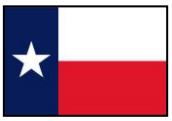
The objective or goal is an easy way for the user to identify what will be discussed in this section of the guide.



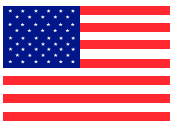
Throughout the guide, action items are designated with this symbol, designed to easily identify action items for the user.



Throughout the guide, text boxes containing the Texas flag are used to highlight changes to Texas laws.



Throughout the guide, text boxes containing the U.S. flag are used to highlight changes to federal laws and rules



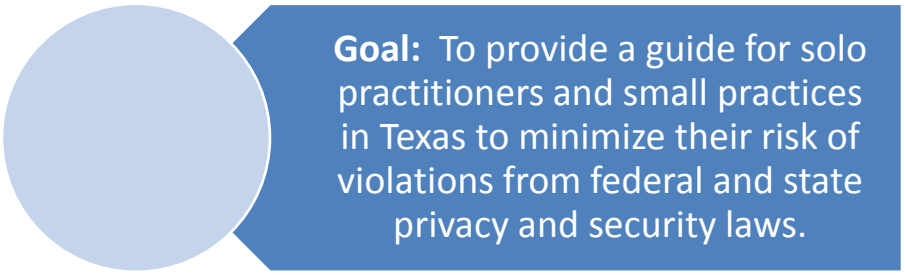
Throughout the guide, links to additional online information are noted with a lightning bolt.



Objectives

TMLT is pleased to bring Texas solo practitioners and small physician practices a *Guide to Getting Started* to minimize the risk of violations for their offices as required by federal and Texas Privacy and Security Laws. This guide is designed to:

- present an overview of federal and Texas privacy and security laws; and
- develop a step-by-step process to assist practices in minimizing their risk of violations.



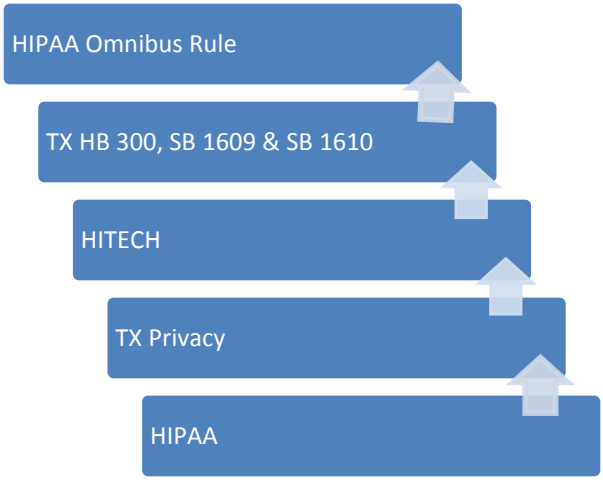
Introduction

HIPAA privacy and security rules are the foundation for the many changes we have seen at the federal and state level. As technology changes and immediate access to health records evolves, medical practices' policies and procedures must change as well. Continued changes to federal and Texas laws and rules will require practices to meet the requirements or face ever-increasing penalties.

In 2011, members of the Texas legislature passed House Bill 300 (HB 300) to add further safeguards for personal health information (PHI) and sensitive personal information (SPI) for patients being treated by Texas physicians. The HB 300 changes that were made to existing Texas privacy laws are more stringent than those found in the federal laws — Health Insurance Portability and Accountability Act (HIPAA) and Health Information and Technology for Economic and Clinical Health Act (HITECH) — and went into effect September 1, 2012. Texas physicians, working with the 2013 legislature, achieved rewording parts of the law amended by HB 300 (2011) to make the requirements on practices less burdensome and therefore, easier to comply. The changes are found in SB 1609 and SB 1610 discussed later in this guide.

It is important for physicians and their office staff to be familiar with the new and existing laws in order to minimize the risk of violations. Consequences may include the assessment of civil penalties under Texas law in addition to penalties for violating the federal laws.

TMLT has revised the previous Comparison Tool, a brief comparison of federal and Texas privacy laws. It is available for free to all policyholders, and is included in this toolkit.



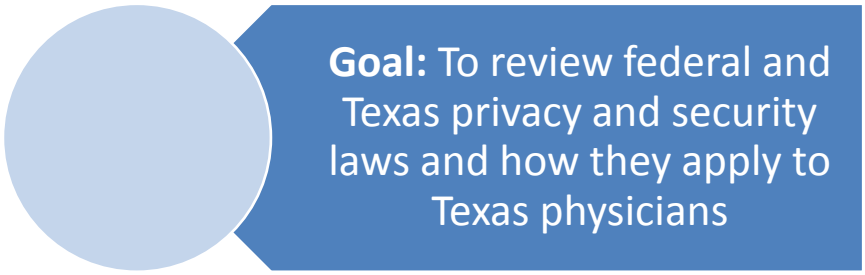
Physician practices should take this opportunity to review their existing HIPAA/HITECH policies, procedures, and practices. Modifications will need to be made to reflect the requirements under the revised Texas privacy laws.

Other statutes exist in Texas that address medical privacy. The following is a summary of these statutes from TMLT's *the Reporter,* 2012 Volume 3.[1]

Texas Privacy Statutes

Texas Statute	PHI/Information Type	General Provisions/Highlights
Texas Government Code, Chapter 420, Subchapter D	Sexual assault	Specifies elements to be included in a valid authorization to disclose this information and exceptions to those requirements.
Texas Health and Safety Code, Chapter 81, Section 81.103; see also Texas Administrative Code Section 8.288	HIV/AIDS test results	Protects test results used to determine if a person has AIDS or HIV infection, antibodies to HIV, or infections with any other probable causative agent of AIDS; results may not be released or disclosed; subject to certain exceptions. Defines required elements to be included in a valid authorization to disclose.
Texas Health and Safety Code, Chapter 81, Section 81.046	Communicable diseases	Reports, records, and information received from any source, including from a federal agency or from another state, furnished to a public health district, a health authority, a local health department, or the Department of State Health Services that relate to cases or suspected cases of disease or health conditions are confidential, subject to certain exceptions, including consent of each individual identified in the information.
Texas Health and Safety Code, Chapter 611	Mental health records/substance abuse	Communication between patient and professional, as professional is defined in Chapter 611, and records of the identity, diagnosis, evaluation, or treatment of a patient created or maintained by a professional regarding any mental/emotional condition or disorder including alcoholism or drug addiction are confidential. Exceptions include instances where provider has obtained written consent. Psychotherapy notes are also subject to more restrictive HIPAA authorization requirements in 45 CFR Section 164.508 and substance abuse information is also subject to more stringent requirements contained in 42 CFR Part 2.
Chapter 546, Subchapter C, Texas Insurance Code; Texas Labor Code Sections 21.403-04; Texas Occupations Code, Chapter 58	Genetic Information	Genetic information is confidential and privileged regardless of source. A person who holds such information may not disclose or be compelled to disclose, by subpoena or otherwise, genetic information about an individual unless disclosure is authorized, subject to certain exceptions. Also applies to a re-disclosure of genetic information. Statute contains required elements to be included in valid authorization to disclose where an exception does not apply.
Texas Civil Practice & Remedies Code §129.001; Texas Fam. Code §32.003	Disclosures regarding treatment of a minor	In Texas, the age of emancipation is 18. The Texas Family Code provides a number of instances under which a minor can consent to treatment without parental or a legal guardian's consent, but the Texas Family Code also allows physicians, dentists, and psychologists, with or without the consent of a child who is a patient, to inform parents, managing conservators, or guardians of that child about treatment given to or needed by the child.
Texas Business & Commerce Code §521 (Texas Identity Theft Enforcement & Protection Act)	SPI	Defines "sensitive personal information" SPI which includes PHI. Includes breach notification requirements for unauthorized access to SPI. Notification to individuals is required if there is an information security breach of the individual's computerized data. Notification must be done as quickly as possible. If sensitive data is encrypted and the data key is not accessed by unauthorized person, notification is not required under the Act. Provides for civil penalties for violations of the Act.
Texas Health & Safety Code §181	All PHI	Sometimes referred to as the Texas Medical Records Privacy Act. Establishes protections for PHI (PHI). Provides for civil penalties for violations of the Act.
Texas Business & Commerce Code §522.002	PHI and other information	Person commits a Class B Misdemeanor if the person uses a scanning device or re-encoder to access, read, scan, store, or transfer information encoded on the magnetic strip of a payment card without the authorized user's consent with the intent to harm or defraud another. This offense is a state jail felony if the information accessed, read, scanned, stored, or transferred is PHI.

Overview of Federal and Texas Privacy & Security Laws



Federal privacy and security – original rules

When Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it created a national standard for the protection of certain health information. Following passage of the Act, the U.S. Department of Health and Human Services (HHS) issued the Privacy Rule to implement the privacy requirements. These standards address the use and disclosure of individuals' health information, called Protected Health Information (PHI), by organizations that meet the federal definition of Covered Entities (CEs). Additionally, the standards address informing individuals of their privacy rights and the control of disclosure of their health information. With the release of the Omnibus Rule in 2013, Business Associates (BAs) of CEs must meet certain standards of the privacy rule as well.

The Office for Civil Rights (OCR) was given the responsibility to enforce HIPAA and assess civil monetary penalties for HIPAA violations.

According to HHS, "a major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing. Given that the health care marketplace is diverse, the Rule is designed to be flexible and comprehensive to cover the variety of uses and disclosures that need to be addressed." [2]

A timeline of effective dates was developed to allow CEs time to develop policies and procedures and documents needed to meet the requirements of the Act. The HIPAA Privacy Rule became effective two years before the HIPAA Security Rule. The additional two years allowed to comply with the Security Rule reflects the complexity of the rules.

Beginning on April 14, 2003, almost all physician offices were required to meet the requirements of the HIPAA Privacy Rule. Very few physician offices were exempt from HIPAA requirements because they did not meet the federal definition of a CE.

> Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a CE. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA transaction provisions in 45 CFR, Part 2.

"Using electronic technology such as email does not mean a health care provider is a CE; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether he or she electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care." [3]

The second major deadline for physician offices was April 20, 2005, when CEs were required to meet the HIPAA Security Rule requirements if PHI is maintained electronically.

Federal privacy and security – amended and codified into law

Four years later, after the enactment of the HIPAA Security Rule, the American Recovery and Reinvestment Act (ARRA) of 2009 was signed into law.

The Act allocated more than $25 billion for health information technology investment and incentive payments. The goal was to assist in the implementation and exchange of health information technology. The changes to privacy and security provisions fall under the HITECH Act.

HITECH required CEs to make changes to their existing policies and procedures to meet the enhancements of the HIPAA Privacy and Security Rules. The final rules for HITECH were included in the HIPAA Omnibus Rule (2013). Examples of changes that CEs should have made in 2009 include:

- new requirements for BAs of CEs;
- new breach notification requirements;
- additional patient rights regarding disclosure of PHI, restricting disclosure of PHI and requesting an account of disclosures of PHI; and
- increased penalties for violations.

HITECH has increased the number of physicians in Texas who are using electronic health records (EHRs). According to TMA in August 2012, "the percentage of respondents who currently use an EHR continues to rise (60 percent, up from 43 percent in 2009). Of the 18 percent of respondents with no plans to implement an EHR, 67 percent report prohibitive cost as the reason. Another reason physicians list for not planning to implement an EHR is having no decision making authority in their practice. Not surprisingly, older physicians are more likely to report nearing retirement as a reason for not planning to implement an EHR."[4] This compares to just fewer than 40% reported on a national level by the National Center for Health Statistics.[5] the TMA survey is shown in Appendix A.

Physician practices need to be aware that HITECH requires the HHS to conduct random audits of CEs. The first audits of health care providers regarding compliance with the HIPAA Privacy and Security Rules occurred in 2012.

HIPAA Omnibus Rule – 2013

In January, 2013, the HHS released a final Omnibus Rule to strengthen the patient privacy and security protections established by HIPAA. The rules expand the individual rights of patients and tighten federal breach notification requirements. According to the Summary in the Federal Register of the publication of the Omnibus rule, the goal of the changes is; "to strengthen the privacy and security protection for individuals' health information; modify the rule for Breach Notification for Unsecured Protected Health Information (Breach Notification Rule) under the HITECH Act to address public comment received on the interim final rule; modify the HIPAA Privacy Rule to strengthen the privacy protections for genetic information by implementing section 105 of Title I of the Genetic Information Nondiscrimination Act of 2008 (GINA); and make certain other modifications to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (the HIPAA Rules) to improve their workability and effectiveness and to increase flexibility for and decrease burden on the regulated entities."[6]

With the new rule, physicians will potentially face more scrutiny by the federal government as well as new administrative burdens.

The rule is effective March 25, 2013, but CEs have an additional six months to achieve compliance, making the deadline September 23, 2013.

Some of the important changes include:

- Changes to the breach notification — with the removal of the "no harm" provision, almost every breach will now be reportable.
- Changes for BAs and their subcontractors — they are now directly liable and must comply with certain HIPAA Privacy and Security Rule requirements.
- Business Associate Agreements — CEs should review and revise their BAAs to incorporate new requirements.
- Changes to use and disclosure of PHI
- Expanded patient rights
- There are now restrictions on disclosure when services are paid out of pocket
- Notice of Privacy Practices (NPPs) — CEs should review and revise their NPPs to incorporate new requirements.

The AMA advises that given; "the potential for $1.5 million fines, not to mention serious reputational injury, these new rules must be taken seriously. Clearly, physicians will need to develop a plan to make these required changes in a timely fashion." [7]

Texas Privacy and Security Laws

The Texas legislature has also passed and revised a number of laws designed to protect the private health records and information to be aligned with federal laws.

Texas Health and Safety Code §181, 182

Effective September 1, 2001, the Texas Medical Records Privacy Act (**Texas Health and Safety Code §181)** was enacted to bring the state into compliance with federal standards of patient privacy (HIPAA 1996). This law was revised effective September 1, 2012, by HB 300 (2011) and, as a result, affords more patient privacy than HIPAA and HITECH.

Effective June 2007, the Texas Health Services Authority (THSA) (**Texas Health and Safety Code §182)** was created as a public-private collaborative to implement the state-level health information technology functions. THSA is designed to be a catalyst for the development of a seamless electronic health information infrastructure to support the health care system in Texas and to improve patient safety and quality of care.

Texas Business and Commerce Code §521

Effective April 1, 2009, the Texas Identity Theft Enforcement & Protection Act (ITEP) (**Texas Business and Commerce Code §521)** requires businesses to implement and maintain reasonable procedures to protect sensitive personal information (SPI) collected or maintained in the regular course of business from unlawful use or disclosure. This law was revised effective September 1, 2012 to reflect the changes of HB 300.

House Bill 300

HB 300 (2011) amended several existing Texas Laws. Members of the Texas House of Representatives were concerned with the number of breaches of health and sensitive data that were occurring and their associated penalties despite federal laws of HIPAA and HITECH.

Senate Bill 1609

The three changes made by SB 1609 amending the Texas Medical Records Privacy Act which will affect training.

- CEs have up to 90 days (previously 60) to train new employees on federal and Texas privacy;
- CEs are required to conduct retraining of staff in a reasonable period, but not later than the first anniversary of the date of the effective law change if the law affects the duties of the employee (previously every two years); and
- CEs are still required to document that an employee has received training by a signed statement from the employee. The documentation must be maintained for six years.

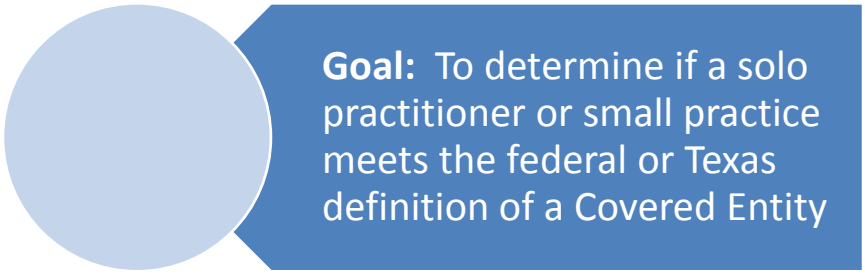
Senate Bill 1610

If the individual whose SPI was breached (or believed to be breached) resides in a state that requires a notice of a breach of system security, the notice may be provided under that state's law or under Texas law. A person may be give written notice as required at the last known address of the individual.

As you will see in this guide, practices have two broad areas of focus: privacy and security.

The goals of this guide are to help you review the requirements for privacy and security, how the federal and Texas laws differ, and what you can do to minimize your risk of violations.

Covered Entity



HIPAA (federal) definition of a CE

A CE means:

- a health plan;
- a health care clearinghouse; or
- a health care provider who transmits any health information electronically in connection with a transaction covered by this subchapter.[8]

After reviewing the definition of CEs under HIPAA, some physician practices have determined they were NOT a CE. If your practice has made such a determination, you will need to review the Texas definition.

Texas definition of a CE

The Texas Medical Records Privacy Act defines a CE as a person who:

- is in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information;
- comes into possession of PHI;
- obtains or stores PHI under this chapter; or
- is an employee, agent, or contractor of a person described above insofar as the employee, agent, or contractor creates, receives, obtains, maintains, uses, or transmits PHI.[9]

A physician who is not a CE under HIPAA is a CE under Texas Medical Records Privacy Act. As a physician in Texas you are required to create and maintain medical records; this makes you a CE, whether you have paper or electronic records.

Conclusion: solo practitioners and small medical practices in Texas are CEs under Texas law.

Business Associates & Business Associate Agreements



Business Associates

Under HIPAA Privacy, CEs are required to identify BAs. A BA of a CE is defined as a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a CE.[10]



AMA's HIPAA Omnibus Final Rule Summary states, "The new rules expand the universe of individuals and companies that must be treated as business associates to include Patient Safety Organizations and others involved in patient safety activities, health information organizations like e-prescribing gateways or health information exchanges that transmit and maintain PHI, and personal health record vendors physicians sponsor for their patients. Thus, physicians must review their relationships and determine if they must enter new BA agreements with these entities or others that create, receive, store, maintain, or transmit PHI on their behalf."[11]

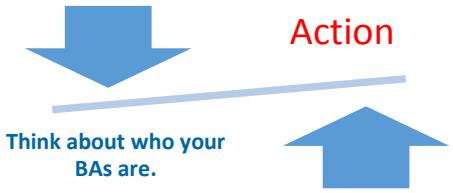
The Omnibus Final Rule has amended the definition of a BA. It is now defined to include:

- A person who creates, receives maintains or transmits PHI on behalf of a CE,
- Patient Safety Organization,
- e-prescribing gateway,
- health information organization (formerly known as a Health Information Exchange),
- other person or entity that (1) provides data transmission services to a CE with respect to its PHI and (2) requires routine access to the CE's PHI, or
- a person who offers a personal health record to individuals on behalf of the CE.

The rule also carves out an exception to the definition of a BA for those organizations that merely provide courier services to CE such as the US Postal Service or UPS and their electronic equivalents (internet service providers). These types of organization only have occasional or random access to PHI which, under the Final Rule, would not quality them as a BA.



BAs and their subcontractors have expanded obligations under the HIPAA Omnibus Rule. BAs and their subcontractors must comply with the new requirements by September 23, 2013.



Because of the new requirements placed on BAs and their subcontractors it is important to begin thinking about who your BAs are.

Consider the following questions:

- Who in your organization is responsible for determining who your BAs are?
- Do you have a procedure for determining if a vendor, contractor, or anyone else is a BA?
- Do you have a BAA with each BA?
- When was your BAA updated? HITECH, Omnibus and TX HB 300 (2011) had changes that should be reflected in your BAA. Does it meet the requirements?

If you do not have a current BAA on all your BAs, you should develop a plan to obtain one.

Examples of persons who <u>are NOT</u> Business Associates	Examples of persons who <u>are</u> Business Associates
In general, a member of the CE's workforce is not a Business Associate.	A health care provider, health plan, or health care clearinghouse of another CE.
A practice's employee who does billing	A third party administrator that assists a health plan with claims processing.
Employees who use the EMR	An electronic medical record vendor.
A practice's employee, not a contractor, who provides IT support	A local IT support person who helps maintain your network.
A practice's CFO or comptroller	A CPA firm that provides accounting services to a health care provider when work involves access to PHI.
Employees who provide transcription services	An independent medical transcriptionist that provides transcription services to a physician.
	A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.

Business Associate Agreements

Under the HIPAA Privacy Rule, CEs are required to have a BAA with all BAs. The CE must impose specific written safeguards on the PHI and SPI that is used or disclosed by its BAs. Specifically, a CE cannot contractually authorize BAs to use or disclose PHI that would be in violation of the Privacy Rule.

A CEs contract or other written arrangement with its BA must contain the elements specified at 45 CFR 164.504(e). A BAA must:

- be in writing;
- define the services the BA is to provide for the CE;
- describe permitted and required uses and disclosures of the PHI by the BA
- provide that the BA will not use or further disclose the PHI other than as permitted or required by the contract or as required by law; and
- require the BA to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.

Appendix C of this manual contains a sample BAA that has been modified for the HIPAA Omnibus Rule and Texas privacy requirements.

Under the HIPAA Omnibus Rule, BAs and their subcontractors who have access to PHI are now held accountable for assuring confidentiality and integrity of that PHI. They are also accountable for any breaches of PHI.

The changes to Texas Medical Records Privacy Act and Identity Theft Prevention and Enforcement Act by HB 300 (2011) required changes to BAAs in Texas. Additionally, the HIPAA Omnibus Rule further clarified BAs and contents of the BAA. The following chart describes the changes you will need to consider as you review and revise your BAA to meet these requirements. Even though BAs and their subcontractors are now directly accountable for many of the HIPAA provisions (clarified in the Omnibus Rule), HHS has reiterated there is a continued need for a CE to obtain BAAs from their BA.

Revision to BAA	Texas HB 300	HIPAA Omnibus Rule
• Include the following information in your BAAs to satisfy the requirements of ITEP: ○ define sensitive personal information (SPI); and ○ require immediate notification by BA to CE of unauthorized disclosure of SPI *From:* Texas Business and Commerce Code Chapter 521 [12]	X	
• Require compliance with applicable provisions of the Privacy Rule • Require compliance with all applicable provisions of the Security Rule • Require reporting of breaches of unsecured PHI in accordance with the Breach Notification Rule • Revise provisions related to subcontractors ensuring that the BA passes on the same or more stringent restrictions to any subcontractor that creates, receives, maintains, or transmits PHI on the BA's behalf • Ensure that, if the CE delegates to the BA any compliance obligations under the Privacy Rule, the BA will perform such obligations in compliance with the Privacy Rule as if the BA were the CE *From:* Complying with the new HIPAA Omnibus Rule: Part 2 [13]		X

Below is a form that is supplied in Appendix B to help you organization your BAs and BAAs. As you identify BAs, you will want to add them to your list and update as needed when revised BAAs are signed.

Business Associates of XYZ Clinic					
Name of Business Associate	**Address of Business Associate**	**Service Provided**	**Original Business Associate Agreement (BAA) Date Signed**	**BAA Update Date** **Date signed**	**BAA Update Date** **Date signed**
i.e. *U print We shred*	*1000 Anywhere Road* *Anywhere, USA 00000*	*Shredding and disposal of PHI*	*March 1, 2003*	*January 2009* *February 28, 2009*	*June 2013* *June 1, 2013*
i.e. *Wee, Winn, Foru Attorneys at Law*	*100 Park Avenue* *NY, NY 10011*	*Legal business for the practice*	*June 1, 2013*		
i.e. *The Best EHR*	*5555 Cyber Lane* *Boston, MA 05678*	*EHR vendor*	*January 1, 2009*	*You may need to get an updated BAA to reflect recent changes*	

II. Privacy

Goal: To provide basic information on HIPAA privacy and how it applies to CEs

HIPAA

After HIPAA was passed by Congress, the HSS issued the Privacy Rule. For the first time, the Privacy Rule established a national standard for the protection of certain health information.

The HIPAA Privacy Rule sought to strike a balance between permitted use of information and the protection of private information shared with providers when patients were seeking care.

A major goal of the Privacy Rule is to assure that the individual's health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.



CEs are required to comply with all of the applicable requirements of the HIPAA Privacy Rule. Full text of the HIPAA Privacy Rule is available at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

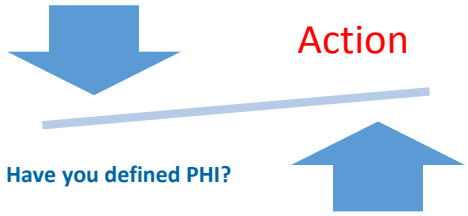
PHI

The Privacy Rule protects all "individually identifiable health information" that is transmitted or maintained by a CE or its BA and their subcontractors in electronic media or in any other form or medium. The rule terms this information as PHI.[14]

What is "individually identifiable health information"?

- Information that is a subset of health information, including demographic data collected from an individual that relates to:
  - the individual's past, present, or future physical or mental health or condition;
  - the provision of health care to the individual; or
  - The past, present, or future payment for the provision of health care to the individual.
- Information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number, etc.).

- The Privacy Rule excludes PHI in employment records that a CE maintains in its capacity as an employer; and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g. [15]



Review your policies and procedures and training material to confirm that you have defined PHI. Assure that all employees who have access to PHI know their role in protecting an individual's health information.



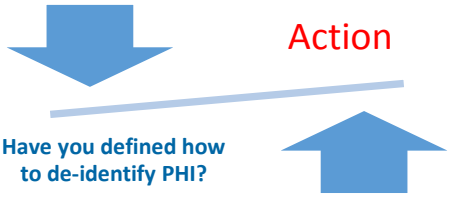
The Texas Medical Records Privacy Act requires all employees to be trained on federal and Texas laws.

- The training must also be completed within the first 90 days of employment.
- Retraining should occur when the law changes and those changes affect the job duties of the employee. Retraining should occur as soon as possible, but within one year of the effective date of the new law.[16]

De-Identified Health Information.

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information:

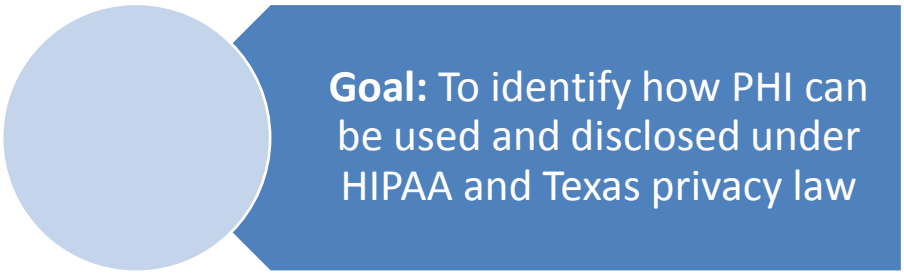
- a formal determination by a qualified statistician; or
- the removal of any of the eighteen specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the CE has no actual knowledge that the remaining information could be used to identify the individual.[17]



Review your policies and procedures and training material to confirm that you have defined the proper way to de-identify PHI and when it should be used.

In November 2012 the OCR published a new document, Guidance Regarding Methods for De-identification of PHI in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. It is available at: www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf

Uses and Disclosures of PHI



One of the main purposes of the HIPAA Privacy Rule was to define the circumstances in which PHI may be used or disclosed by a CE. Additionally, the rule defined limitations on disclosure.

A CE may not use or disclose PHI, except under the following circumstances:

1. As permitted or required under the Privacy Rule; and
2. as the individual who is the subject of the information (or their representative) authorizes in writing.

Required disclosures

A CE must disclose PHI in only two situations:

1. to individuals or their personal representatives specifically when they request access to or an accounting of disclosures of their PHI; and
2. to HHS when it is undertaking a complaint or compliance review, an investigation or enforcement action.

Additional reading on HHS or government access is available at:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/govtaccess.html

Permitted uses and disclosures

A CE is permitted, but not required, to use and disclose PHI, without an individual's authorization, for the following purposes or situations:

- as required by law;
- public health activities;
- disclosures about victims of abuse, neglect, or domestic violence;
- health oversight activities;
- judicial and administrative proceedings;
- law enforcement purposes;
- coroners, medical examiners, and funeral directors;
- research;
- organ and tissue donation;
- serious threat to health or safety;
- military, national security, intelligence activities and protection of the president;
- correctional institutions; and
- worker's compensation.

Authorized uses and disclosures

A CE must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment, health care operations, or as otherwise permitted or required by the Privacy Rule.[18]

Except in limited circumstances, a CE may not condition treatment, payment, enrollment, or benefits eligibility to an individual granting an authorization.



The HHS web site (HHS.gov) has HIPAA Frequently Asked Questions, which is a good resource for disclosure information. The site allows you to search by keyword or category such as "disclosures to law enforcement."

Available at: http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html

AUTHORIZED USES AND DISCLOSURES OF PHI		
	FEDERAL	**TEXAS**
Authorization	• A CE must obtain the individual's written authorization for any use or disclosure of PHI that is **not** for treatment, payment, or health care operations or as otherwise permitted or required by the Privacy Rule. [19]	A CE shall provide notice to an individual for whom the CE creates or receives PHI if the individual's PHI is subject to electronic disclosure. The attorney general has developed a standard authorization form for use in complying with this section. The form complies with HIPAA's Privacy Standards and this chapter [20]
Psychotherapy Notes	• A CE must obtain an individual's authorization to use or disclose psychotherapy notes. • Exceptions are outlined in the text below.	
Marketing	• A CE must obtain an individual's authorization to use or disclose PHI for marketing purposes. • Exceptions apply if (1) marketing is conducted in a face to face communication between the CE and the individual or (2) marketing is in the form of a promotional gift of nominal value provided by the CE to the individual	Marketing per the Texas Medical Records Privacy Act • a CE must obtain clear and unambiguous permission to use or disclose PHI for any marketing communication, except under the following conditions: ◦ A face-to-face communication made by CE to individual ◦ A promotional gift of nominal value provided by CE ◦ Communication necessary for administration of a patient assistance program or drug savings program ◦ Communication made at the request of the individual • CE sends marketing through the mail meeting specific requirements • CE shall remove the individual's name from mailing list within 45 days of the request Marketing communication made by oral request must be limited to scope of oral permission[21]
Sale of PHI	• **HIPAA Omnibus Rule** limits a CE or BA in receiving remuneration in exchange for PHI; • **HIPAA** *selling* PHI by CE is never allowed without authorization	• **Texas privacy law** prohibits sale of PHI without patient authorization • Exceptions: CE may disclose an individual's PHI (1) to another CE for purposes of treatment, payment, health care operations, to perform an insurance or health maintenance organization function as described in Texas Insurance Code §602.053 or (2) as otherwise authorized or required by state or federal law. • The direct or indirect remuneration a CE may receive for sale of PHI for an insurance or health maintenance organization function may not exceed the reasonable cost of preparing or transmitting the PHI.

The Omnibus Rule has made additional changes to Use and Disclosures of PHI.



HIPAA Omnibus Rule sets new limits on use and disclosure of PHI and CE and BA must comply with the new requirements by September 23, 2013.

Disclosures to Health Plans **–** a CE must comply with a patient's request to not use or disclose PHI to a health plan or BA of the health plan, if the patient paid out-of-pocket for the care at the time of service. According to AMA, "Of all the changes made by the new rules, this change is likely to have the greatest impact on physician practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to."[22]

Marketing Communications **–** the Omnibus Rule places limits on the circumstances when physicians may provide marketing communication to their patients without authorization. The AMA Omnibus Summary states that "generally speaking, the only time a physician may tell a patient about a third party's products or services without the patient's written authorization is:

- the physician receives no compensation for the communication;
- the communication is face to face;
- the communication involves a drug or biologic the patient is currently being prescribed and the payment is limited to reasonable reimbursement of the costs of the communication (no profit);
- the communication involves general health promotion, rather than the promotion of a specific product or service; or
- the communication involves government or government sponsored programs.
- the physician is still permitted to give patients promotional gifts of nominal value, such as a pamphlet."[23]

Sale of PHI **–** a CE is prohibited from selling PHI without written authorization if they receive remuneration in exchange for PHI; this is a change from HIPAA that never allowed the sale of PHI without authorization. Four exceptions that are not considered sale of PHI include:

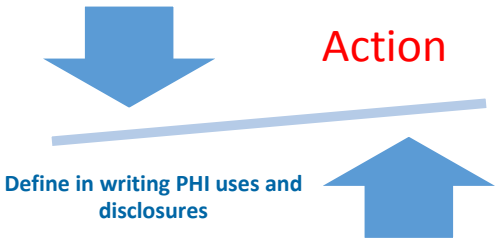
- disclosures made for treatment or payment;
- disclosures made for public health;
- disclosures made as part of the sale, transfer, merger, or acquisition of a CE to another CE; and
- disclosure is required by law.[24]

Fundraising **–** The Omnibus Rule expanded the use and disclosure of PHI for fundraising purposes. Before Omnibus, a CE could only disclose demographics and dates of service for fundraising. The Omnibus Rule now allows additional PHI to be disclosed, including the department of service, treating physician, outcome information and health insurance. HIPAA Privacy Rule and HITECH already required CE to provide individuals the opportunity to opt out of receiving fundraising communications. With Omnibus, the opportunity to opt out must be "clear and conspicuous," and must not be burdensome to the individual. Additionally, the Omnibus Rule requires the CE to include the opt out option for fundraising in their Notice of Privacy Practice.

Childhood Immunizations **–** The Omnibus Rule permits physicians to disclose proof of immunization to schools as long as physicians have and document an informal agreement to disclose such information from the patient's parent or guardian. The Texas Occupations Code Section 159.005 requires that physicians have a consent for release of confidential information that is written and signed by one of the persons specified.[25] Until further clarification is obtained on this issue; it is recommended that Texas physicians have a written authorization before disclosing proof of immunization.

Release of PHI concerning Decedents **–** The Omnibus Rule permits physicians to disclose PHI to a deceased patient's family and friends, as permitted when the patient was alive. The Texas Medical Practice Act requires that physicians have a valid consent for disclosure of PHI. Until further clarification is obtained on this issue, it is recommended that Texas physicians have a consent for the release of confidential information. The Texas Occupation Code Section 159.005, Chapter 13, Texas Probate Code, and Chapter 107 of the Texas Family Code include a provision that a personal representative may sign a release if the patient is deceased. A court appointed executor of an estate is a qualified personal representative. Practices should question anyone presenting as one.

Additionally, the Omnibus Rule eliminates protection of PHI 50 years after a patient's death.



Review your existing policies and procedures on PHI uses and disclosures. Do they clearly define permitted uses and disclosures as well as those that require authorizations?

Authorization requirements of the HIPAA Privacy Rule
The following are the authorization requirements under the HIPAA Privacy Rule as recorded in the OCR Privacy Rule Summary: [26]

An authorization must be in writing;

- it may allow use and disclosure of PHI by the CE seeking the authorization or by a third party;
- all authorizations must be in plain language and specifically describe: the information to be disclosed or used, the person(s) disclosing and receiving the information, expiration, right to revoke in writing, and other information.

Examples of disclosures that would require an individual's authorization under HIPAA Privacy:

- disclosures to a life insurer for coverage purposes;
- disclosures to an employer of the results of a pre-employment physical or lab test; and
- disclosures to a law firm for litigation purposes



Authorization requirements under Texas privacy law

With the revisions effective September 1, 2012, Texas Medical Records Privacy Act requires covered entities to:

- provide notice of electronic disclosure of PHI to patients if patients' PHI is subject to electronic disclosure (this may be provided in Notice of Privacy Practices or a separate document);
- post written notice of electronic disclosure of PHI in your place of business, on your web site or in other conspicuous places where patient is likely to see notice. It may be incorporated into current practice protocol that satisfies HIPAA requirements; and
- obtain patient authorization (written or in oral form if documented in writing) for each electronic disclosure of PHI except if electronic disclosure is made to another Covered Entity for purposes of treatment, payment, health care operations, performing an insurance or health maintenance organization function described in Texas Insurance Code §602.053 or as otherwise authorized or required by state or federal law. (Do not obtain blank, signed patient authorizations).

One of the HB 300 amendments to the Texas Medical Records Privacy Act is the provision requiring the Texas Attorney General to adopt a standard authorization form for electronic disclosures of PHI by January 2013 – it is not mandatory that practices use this form; any form that contains the required information is acceptable.

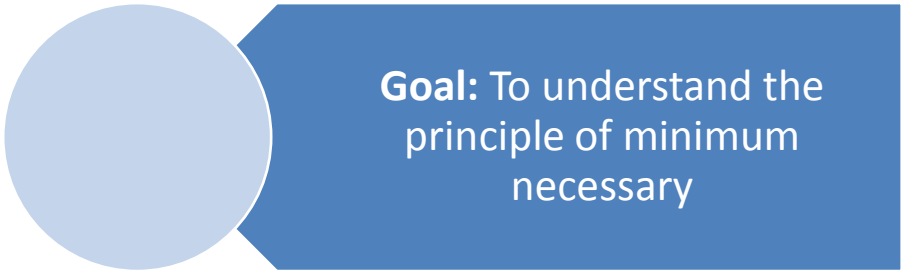
This form is available in Appendix F or on the Texas Attorney General's Website

Psychotherapy Notes

Psychotherapy notes and the release of the notes are often confusing for CEs. The psychotherapy notes are not the medical record. HIPAA defines psychotherapy notes as: "notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Psychotherapy notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."[27]

- A CE must obtain an individual's authorization to use or disclose psychotherapy notes.
- Exceptions which do not require an individual's authorization to use or disclose psychotherapy notes include but are not limited to the following:
    - CE who originated the notes and uses them for treatment;
    - CE may use for their own training programs;
    - CE may use for legal defense in action brought against the CE by the individual;
    - HHS to investigate or determine the CE's compliance with the Privacy Rule;
    - to avert a serious and imminent threat to public health or safety;
    - health oversight agency for lawful oversight;
    - lawful activities of a coroner or medical examiner; and
    - as required by law.

Minimum Necessary



The principle of minimum necessary is a key aspect to the Privacy Rule in protecting confidential information of individuals.

A CE and Business Associates and their subcontractors must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request.

The HIPAA Privacy Rule requires CEs to develop and implement policies and procedures to reasonably limit use and disclosures to minimum necessary.[28]

The Omnibus Rule states, “we also emphasize that as with any use or disclosure under the Privacy Rule, a CE must apply the minimum necessary standard at §164.502(b) to ensure that only the minimum amount of protected health information necessary to accomplish the intended purpose is used or disclosed.”[29]

How the Rule Works

The Privacy Rule generally requires CEs to take reasonable steps to limit the use or disclosure of, and requests for, PHI to the minimum necessary to accomplish the intended purpose. The minimum necessary standard does not apply to the following:

- disclosures to or requests by a health care provider for treatment purposes;
- disclosures to the individual who is the subject of the information;
- uses or disclosures made to an individual as permitted or required by the Privacy Rule;
- uses or disclosures made pursuant to an individual’s authorization;
- disclosures to the HHS when disclosure of information is required under HIPAA for compliance and enforcement actions; and
- uses or disclosures that are required by other law.[30]



Review your existing policies and procedures regarding limiting uses and disclosures to the minimum necessary. Do your policies address them? Does your training address minimum necessary requirements?

When thinking about HIPAA Privacy the concept of minimum necessary is key. CE and BA “must make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose.” For example, if a physician needs to access a past lab result from another provider for comparison to recent findings, it is not necessary to request “all medical records.” Likewise, if your practice receives a request for “all medical records” you may want to clarify with the requester what is actually needed.

> **Access and uses –** For internal uses, a CE must develop and implement policies and procedures that restrict access and uses of PHI based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to PHI to carry out their duties, the categories of PHI to which access is needed, and any conditions under which they need the information to do their jobs.
>
> **Disclosures and requests for disclosures –** CEs must establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures, or requests for disclosures, that limits the PHI disclosed to the minimum amount reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. For non-routine, non-recurring disclosures, or requests for disclosures that it makes, CEs must develop criteria designed to limit disclosures to the information reasonably necessary to

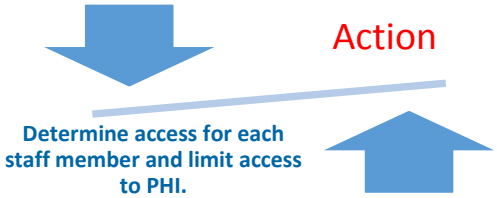
accomplish the purpose of the disclosure and review each of these requests individually in accordance with the established criteria.

Reasonable reliance – If another CE makes a request for PHI, a CE may rely, if reasonable under the circumstances, on the request as complying with this minimum necessary standard. Similarly, a CE may rely upon requests as being the minimum necessary PHI from: (a) a public official, (b) a professional (such as an attorney or accountant) who is the CE's Business Associate, seeking the information to provide services to or for the CE; or (c) a researcher who provides the documentation or representation required by the Privacy Rule for research. [31]

FAQs on minimum necessary are available at:

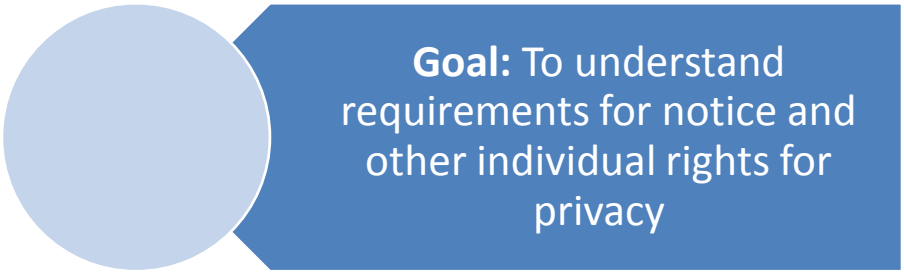
http://www.hhs.gov/ocr/privacy/hipaa/faq/minimum_necessary/index.html

Staff members should only have access to PHI that is necessary to do their job. Many EHR and practice management systems allow limiting access through permissions. This may help to assure that your staff is only accessing the minimum necessary PHI.



Review your existing policies and procedures on minimum necessary. Do they address access to PHI by staff members? Make a list of all the positions of staff members you employ; next to each position describe what PHI (minimum necessary) they need access to do their job.

Notices and Individual Rights



This section contains information on the individual's rights regarding privacy and will cover the following topics:

- privacy practices notice;
- individual access;
- amendment;
- disclosure accounting;
- restriction requests; and
- confidential communications requirements.

Notice of Privacy Practices

CEs that provide direct treatment are required under the HIPAA Privacy Rule to provide a notice of their privacy practices to patients. Sample *Notice of Privacy Practices* is available on the AMA and TMA websites.

Required elements — notice of privacy practice:

- Description, including at least one example, of the ways in which the CE may use and disclose PHI for treatment, payment, and health care operations.
- Description of all other purposes for which the CE is permitted or required by the HIPAA Privacy Rule to use or disclose PHI without the individual's written authorization.
- Statement that other uses and disclosures will only be made with the individual's written authorization and that the individual may revoke such authorization in writing.
- A separate statement for certain uses and disclosures, including communications regarding appointment reminders, information about treatment alternatives or other health-related benefits and services or fundraising, if the CE intends to engage in any of these activities.
- State the CE's duty to protect the privacy of PHI.
- State the CE's duty to provide notice of privacy practices to individuals.
- State the CE's duty to abide by the terms of the notice.
- Statement that the CE reserves the right to change the terms of its notice, make the new notice provisions effective for all PHI it maintains, and describe how it will provide individuals with the revised notice.
- The individual's rights with respect to PHI, including (1) the right to request restrictions on certain uses and disclosures of PHI (plus a statement that the CE is not required to agree to certain requested restrictions), (2) the right to receive confidential communications of PHI, (3) the right to inspect and copy the individuals PHI, (4) the right to amend the individual's PHI, (5) the right to receive an accounting of disclosures of PHI, and (6) the right of an individual to obtain a paper copy of the notice of privacy practices upon request, including an individual who has agreed to receive the notice electronically.
- How the individual may exercise these rights.
- Describe the individual's right to file a complaint with the CE and HHS if the individual believes his or her rights have been violated.
- Contact information for a person at the CE's office who the individual may contact to make a complaint or receive additional information pertaining to the notice.
- The notice must include an effective date.

A CE is required to promptly display and distribute its notice whenever it makes material changes to any of its privacy practices.



Review your existing notice of privacy practices and make sure it is posted in your office and on your web site.

Many changes have been made to federal and Texas privacy laws and rules in recent years. With each change, you need to evaluate your policies and procedures and make necessary changes. Changes to your policies and procedures should be included in your Notice of Privacy Practices. The following chart outlines changes that you may need to make to your Notice of Privacy Practices.

SUMMARY OF CHANGES TO YOUR NOTICE OF PRIVACY PRACTICES		
	FEDERAL	**TEXAS**
Posting of Notice of Privacy Practices	Post the notice in a clear and prominent location in your office and on website	
Providing Notice of Privacy Practices	Provide the notice no later than the date of the first service (unless an emergency)	
Notice regarding Electronic Disclosure of PHI		Include your Patient Notice Regarding Electronic Disclosure of PHI
Electronic Communications		Include how your practice uses electronic media to communicate with patients (if applicable)
Consent for Emailing PHI		Include that your practice will not email patients without a written consent
Unsecured PHI		Include a definition of unsecured PHI in your NPP
Breach Notification	Include the CE has a duty to notify the affected individual of a breach of unsecured PHI	Include that you will notify patients of a breach of PHI or SPI as required by federal and state law
Fundraising Opt Out	Include the individual has the right to opt out of fundraising communications from the CE	
Restrict Disclosures of PHI to health plan	Include for services paid in full, out of pocket, at the time of service, an individual's request not to disclose to a health plan must be honored	
Authorization for Marketing or Sale of PHI	Include your practice regarding marketing and sale of PHI only with authorization from the individual	
Authorization for Disclosure of Psychotherapy Notes	Include, unless otherwise required by law, psychotherapy notes will not be disclosed without authorization	
General Review of Privacy Practices	The Omnibus rule has made a number of changes affecting privacy practices; it is a good time to do a complete review of your NPP.	
Redistribution of Notice of Privacy Practices	Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision Providers must post the revised NPP in a clear and prominent location. Practices must make copies of the NPP available for individuals who request a copy. Providers are only required to give a copy of the NPP to, and obtain a good faith acknowledgment of receipt from, new patients.	

Notice distribution

The HIPAA Privacy Rule requires that all covered health care providers with a direct treatment relationship with individuals deliver a privacy practices notice to patients. This requirement has been in effect for health care providers since April 14, 2003. The distribution requirements include:

- The notice must be provided no later than the first service encounter.
- A good faith effort must be made to obtain a written acknowledgment of receipt of the notice and if not obtained, document the health care provider's good faith efforts that were made to obtain such acknowledgment and the reason why it was not obtained;
- Have the notice available at the delivery site for individuals to request to take with them;
- The notice is to be posted at each service delivery site in a clear and prominent place where people seeking service from the health care provider may reasonably be expected to read the notice;
- In emergency situations, the provider must furnish its notice as soon as practicable after the emergency abates; and
- Make revised notices available upon request on or after the effective date of the revisions and post the revised notice in a clear and prominent place where people may reasonably be expected to read the notice.

All CEs — whether direct treatment providers or indirect treatment providers (such as laboratories) or health plans — must supply notice to anyone upon request. A CE must also make its notice electronically available on any web site it maintains for customer service or benefits information.

Acknowledgement of notice receipt

A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice. A sample Acknowledgement of Notice Receipt is provided in Appendix E. It is important to note that the Privacy Rule does not prescribe any particular content for the acknowledgement. The provider must document the reason for any failure to obtain the patient's written acknowledgement.

The law requires that you have patients sign an Acknowledgement of Privacy Practices once. If you change your notice of privacy practices, you must post your NPP in your clinic and on your web site, but patients do not need to sign a new acknowledgement form.



Review your existing policies and procedures on notice of privacy practices.

Checklist for reviewing your NPP:

- Assure the required elements included in your notice
- Notice posted in your waiting room
- Notice on your web site?
- All new patients (from April 14, 2003 to the present) signed an acknowledgment of receipt of privacy practices or you have documentation that they refused to sign
- All acknowledgement are scanned into the EHR when converting or was a new acknowledgment signed and scanned
- Adopt new patient authorization forms for electronic disclosures of PHI
- Adopt new patient notices regarding electronic disclosure of ePHI
- Update your notice of privacy practices and policies and procedures.
    - Include your Patient Notice Regarding Electronic Disclosure.
    - Establish your office policy regarding electronic communications with your patients (email, text, and other electronic communications) and include in your NPP.
    - Create and have patients sign email consent forms if your office permits email communications with patients.
    - Establish your office policy regarding workforce's use of Facebook and Twitter.
    - Include HITECH breach notification requirements in your NPP: "We will notify you of any unauthorized use, access, etc., of your unsecured PHI that presents a significant risk of financial, reputational, or other harm to you to the extent required by law."
    - Define unsecured PHI and include it in your NPP.



HB 300 (2011) added additional requirements for Texas Covered Entities regarding authorizations and notice of use of electronic disclosures.

Note: The authorization form for electronic disclosure is available on the Texas Attorney General's web site as of January 1, 2013.

https://www.oag.state.tx.us/AG_Publications/pdfs/hb300_auth_form.pdf

Individual access

With few exceptions, an individual has the right to review and obtain a copy of their PHI as contained in a CE's designated record set. The definition of a designated record set is: that group of records maintained by or for a CE that is used, in whole or part, to make decisions about individuals, or a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and case or medical management record systems.

Exceptions to right to review and obtain a copy:

- psychotherapy notes;
- information compiled for legal proceedings;
- PHI to which the Clinical Laboratory Improvements Amendments of 1988, as amended (CLIA) prohibits access; and
- PHI that is exempt from the Clinical Laboratory Improvement Amendments of 1998, as amended (CLIA) [31:]

Under HIPAA, a CE may deny an individual access in certain situations, such as when a health care professional believes access could cause harm to the individual or another. This is also consistent with Texas Medical Board Rule 165.2 Medical Records (see sidebar). HIPAA requires that if a CE denies access, based on reviewable grounds for denial, the individual must be given the right to have such denials reviewed by a licensed health care professional for a second opinion.

HIPAA allows CEs to impose reasonable, cost-based fees for the cost of copying, postage, and for the preparation of a summary of the PHI if applicable. Texas Medical Board rules are very specific about allowable charges for paper copies of medical records.

TEXAS MEDICAL BOARD RULES

Texas Administrative Code, Title 22, Part 9

§165.2. Medical Record Release and Charges

(a) Release of Records Pursuant to Written Request. As required by the Medical Practice Act, §159.006, a physician shall furnish copies of medical and/or billing records requested or a summary or narrative of the records pursuant to a written release of the information as provided by the Medical Practice Act, §159.005, except if the physician determines that access to the information would be harmful to the physical, mental, or emotional health of the patient. The physician must delete confidential information about another patient or family member of the patient who has not consented to the release. If by the nature of the physician's practice, the physician transmits health information in electronic form, the physician may be subject to the Health Insurance Portability and Accountability Act (HIPAA) 45 C.F.R. Parts 160-164. Unless otherwise provided under HIPAA, physicians subject to HIPAA must permit the patient or an authorized representative access to inspect medical and/or billing records and may not provide summaries in lieu of actual copies unless the patient authorizes the summary and related charges.

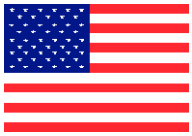
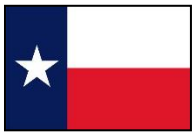
(b) Deadline for Release of Records. The requested copies of medical and/or billing records or a summary or narrative of the records shall be furnished by the physician within 15 business days after the date of receipt of the request and reasonable fees for furnishing the information.

(c) Denial of Requests for Records. If the physician denies the request for copies of medical and/or billing records or a summary or narrative of the records, either in whole or in part, the physician shall furnish the patient a written statement, signed and dated, within 15 business days of receipt of the request stating the reason for the denial and how the patient can file a complaint with the federal Department of Health and Human Services (if the physician is subject to HIPAA) and the Texas State Board of Medical Examiners. A copy of the statement denying the request shall be placed in the patient's medical and/or billing records as appropriate. [32]

A complete copy of TMB rules are available at:
http://www.tmb.state.tx.us/rules/rules/bdrules.php

Under HITECH and the HIPAA Omnibus Rule individuals are allowed to obtain a copy of their PHI in electronic format from a CE. Additionally, a CE can only charge a fee for the labor costs required to respond to the request when providing an electronic copy.

The following chart compares federal and Texas requirements for providing copies of medical records.

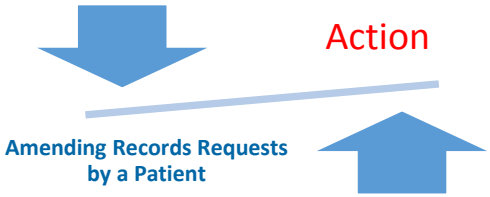
COMPARISON OF FEDERAL AND TEXAS REQUIREMENTS FOR PROVIDING COPIES OF MEDICAL RECORDS	
	
HIPAA Omnibus	**The Texas Medical Records Privacy Act Requirement for access as amended by HB 300 (2011)**
• The rule modifies the costs that may be charged to the individual for copies of his or her records. This includes labor costs for copying PHI (potentially to include skilled technical staff time or extracting, scanning and burning electronic PHI to media and distributing the media), supply costs if the patient requests a paper copy, or if electronic, the cost of any portable media (such as a USB memory stick or a CD), and postage assuming state law does not set a lower reimbursement rate. • The rule also clarifies that physicians may impose a separate charge for creating an affidavit of completeness when requested.	• CE must provide patients with an electronic copy of their medical records within 15 days of receipt of written request if CE uses EHR system capable of fulfilling request. • CE may provide records to the patient in another format if the patient agrees. • Texas law is silent on allowable charges for electronic copies of records.

Amendment to records

HIPAA Privacy Rule allows individuals the right to have covered entities amend their PHI, such as when the information is inaccurate or incomplete. A CE may deny the request to amend under certain circumstances. You should define in your policies and procedures:

- how an individual makes a request for amendment;
- the process of reviewing the request for amendment by the CE, including who will determine if the amendment is accepted;
- when an amendment is accepted, the CE must make reasonable efforts to provide the amendment to persons who the individual has identified as needing it, and to persons that the CE knows might rely on the information to the individual's detriment; and
- when the amendment is denied, the CE must provide the individual with a written denial within 60 days after receipt of such request and allow the individual to submit a statement of disagreement for inclusion in the record.

If a CE receives a notice from another CE that they have accepted an amendment to their records (now contained in your records) the CE must amend their designated record set to reflect the amendment.



Review your existing policies and procedures and notice of privacy practices.

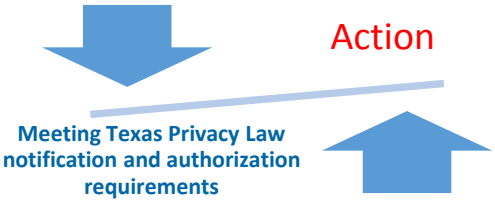
Disclosure accounting

The HIPAA Privacy Rule allows individuals the right to an accounting of certain disclosures of their PHI by a CE or the CE's BAs. There were a number of exclusions to the disclosure rule under the HIPAA Privacy Rule; however, with HITECH much of that changed.

HITECH specifically addresses CEs that maintain PHI in EHRs that require accounting of disclosures that are made for purposes of treatment, payment, and health care operations which were exceptions to the accounting of disclosure requirements under the HIPAA Privacy Rule.

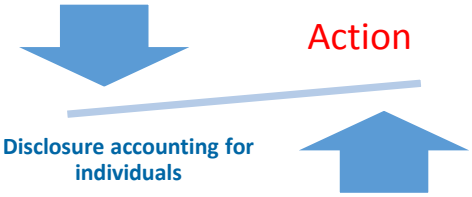
Under HITECH, CEs must provide disclosures that were made during the three years prior to the date on which the accounting is requested.

HITECH also requires that CEs either account for the disclosures of their BAs, or to require BAs to make their own accounting. BAs must respond to individual requests made directly to them.



Additional reading on accounting for disclosures:

- *HIPAA Privacy Rule Summary – Notice and Other Rights Disclosure Accounting – Privacy Rule Exclusions for Accounting for Disclosures:* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
- *Accounting for All Disclosures* from the Journal of AHIMA: http://journal.ahima.org/2009/03/25/accounting-for-all-disclosures/
- HHS Releases Request for Information for Accounting of Disclosures: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountingrfi.html



Review your existing policies and procedures on disclosure accounting for individuals. The original exceptions to the accounting of disclosure requirements under the HIPAA Privacy Rule are NOT applicable under HITECH if the practice has electronic health records. Be aware the HHS has not determined what information should be released under accounting of disclosures. When this is done, practices will need to review their policies again.

Restriction requests

Medical offices may be asked by patients to restrict the use of PHI in certain circumstances. The HIPAA Privacy Rule stated previously:

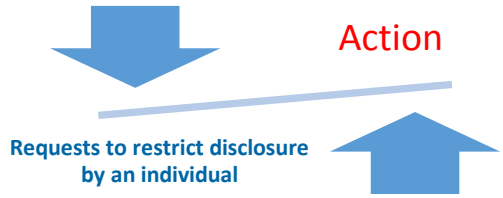
> Individuals have the right to *request* that a CE restrict use or disclosure of PHI for treatment, payment, or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.
>
> A CE is under no obligation to agree to requests for restrictions.

A CE that does agree must comply with the agreed restrictions, except for purposes of treating the individual in a medical emergency.[33]



Patients may request that a CE not disclose information about their care to their health plan if the patient (or someone on behalf of the patient) has paid for the service.

The Omnibus Rule requires a CE to comply with a patient's request for restrictions on disclosure of PHI to a health plan for purposes of carrying out payment or health care operations in circumstances where the patient has paid for the service out of pocket and in full. The Omnibus Rule states "Disclosures to health plans – At the patient's request, physicians may not disclose information about care the patient has paid for out-of-pocket to health plans, unless for treatment purposes or in the rare event the disclosure is required by law. This change updates the previous HIPAA Privacy Rule governing patient requests for restrictions on the use or disclosure of their PHI. Previously, while physicians could refuse to abide by any such request, the new rule *requires* physicians and other health care providers to abide by a patient's request not to disclose PHI to a health plan for those services for which the patient has paid out-of-pocket and requests the restriction. Of all the changes made by the new rule, this change is likely to have the greatest impact on physician practice workflow both in terms of documentation and follow up to ensure the restriction is adhered to."[34]

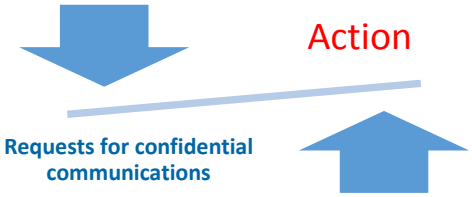


Review your existing policies and procedures on requests for restriction of use or disclosure. Does it include what circumstances under which you will accept and deny the request? Additionally, this will be something to include in your staff training.

Confidential communications requirements

Health care providers must permit individuals to request an alternative means or location for receiving communications of PHI by other than those the CE typically uses. For example:

- a patient may request that the provider communicate with them through a designated address or phone number; or
- a patient may request that communications sent by mail be sent only in a sealed envelope.
- Under HIPAA, any CE may condition compliance with a confidential communication request on the individual specifying an alternative address or method of contact and explaining how any payment will be handled.

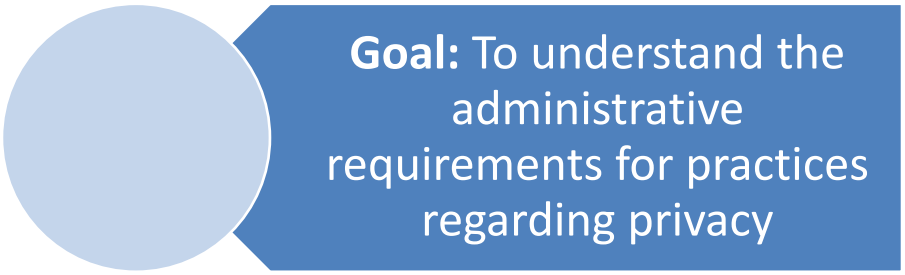


Review your existing policies and procedures on confidential communication requests. How do you handle and process requests, including acceptance and denial of the request? How is it communicated within the practice?

Patient portals are becoming a very popular way to communicate with patients. According to AHIMA, "portals that link to EHR systems provide patients with what they want — easy access to their health information and other savvy online tools." If you currently have a patient portal or are considering adding this feature to your EHR, you will need to address privacy and security issues and be able to answer patient questions when they arise.

Patient Portals: Express Lane on the Health Information Highway
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049724.hcsp?dDocName=bok1_049724

Administrative Requirements of the HIPAA Privacy Rule



In the HIPAA Privacy Rule Summary, the HHS acknowledges that the Privacy Rule recognizes that CEs vary in size and scope. "Therefore the flexibility and scalability of the Rule are intended to allow covered entities to analyze their own needs and implement solutions appropriate for their own environment." [35]

This section contains information on administrative requirements:

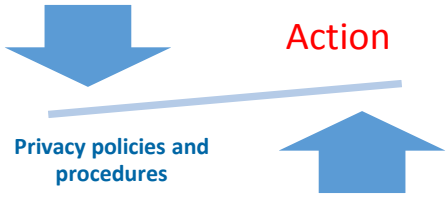
- privacy policies and procedures;
- privacy personnel;
- workforce training and management;
- mitigation;
- safeguards;
- complaints;
- retaliation and waiver; and
- documentation and record retention.

Privacy policies and procedures

CEs are required under the HIPAA Privacy Rule to develop and implement written privacy policies and procedures with respect to PHI.

Policies and procedures should be developed based on the size and type of business conducted by the CE. Policies and procedures need to be revised to reflect changes in the privacy laws and the CE's privacy practices.

Unfortunately, the HIPAA Privacy Rule does not provide a list of policies and procedures that are necessary to meet this requirement. Throughout this guide, suggested action steps often include review of your existing policies and procedures to ensure that they address the specific topic being discussed.



Review your existing policies and procedures on a routine basis. Make changes when laws and your office privacy practices change. Train staff on change.



Texas HB 300

The 2011 Texas Legislature's passage of HB 300 requires covered entities to revise existing policies and procedures to meet the new requirements. Some of the HB 300 provisions have been codified into the following laws:

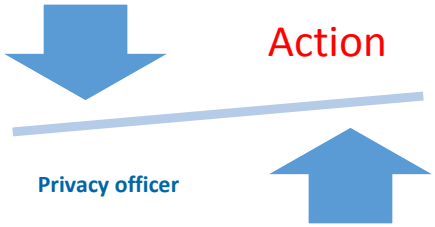
Texas Health and Safety Code §181, 182

- Texas Medical Records Privacy Act (Texas Health and Safety Code §181)
- Texas Health Services Authority (Texas Health and Safety Code §182)
- Texas Identity Theft Protection and Enforcement Act (Texas Business and Commerce Code §521)

Privacy officer

A CE must designate a privacy officer or official. That individual is responsible for developing and implementing the privacy policies and procedures for the CE.

The privacy officer is the contact person who is named by the practice to receive complaints and answer questions about the CE's notice of privacy practices. This information should be included in your notice of privacy practices.



Is your current Privacy Officer the one listed in your notice of privacy practices and in your policies and procedures? Does staff know who the privacy officer is? Are the duties of the privacy officer listed in his or her job description?

Workforce training and management

A CE is responsible for training all staff members on its privacy policies and procedures. The rule states, "as necessary and appropriate for them to carry out their functions," and thereafter to new staff members within a reasonable time after their hire date.

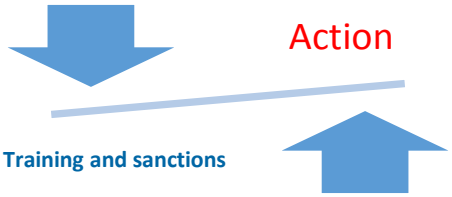
Definition of workforce members – members include employees, volunteers, trainees and other persons whose conduct is under the direct control of the CE; whether or not they are paid by the CE.[32]

The rule requires that the CE must have and apply appropriate sanctions against workforce members who violate privacy policies and procedures or the Privacy Rule.



The Texas Medical Records Privacy Act requirements for training as amended by HB 300 (2011) and SB 1609 (2013):

- Employees to be trained on state and federal laws on PHI;
- New employees must receive training by 90th day of employment;
- All employees are to receive training as soon as possible following a change in law or rule that materially affects their job, but no later than one year after the effective date
- Covered Entity must maintain signed statements from employees verifying attendance at training program.



Review your current privacy and security training. When was it last conducted? Does it comply with the recent changes to Texas Privacy law?

Mitigation

Under the Privacy Rule, a CE must mitigate, to the extent practicable, any harmful effects that are known to the CE and that result from a use or disclosure of PHI in violation of its own privacy policies and procedures or the Privacy Rule by the CE or its BAs.

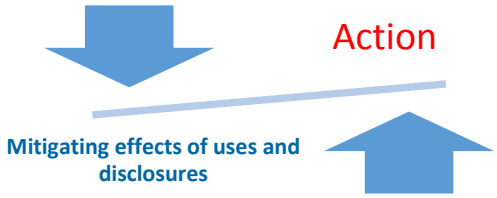
For example, an employee of a clinic copies patient information on 50 patients onto a flash drive. The information includes name, address, date of birth, health insurance policy number and the patient's active diagnosis from their electronic health records. The employee returns to work on Monday and reports that she lost the flash drive on the bus. The flash drive is not encrypted. The clinic has a policy that PHI and sensitive personal information may not be saved on portable devices. What should the clinic do?

Mitigation efforts will vary depending on the circumstances of the use or disclosure of PHI. Some of the steps to consider might include:

- notify your cyber liability carrier of the issue;
- identify the cause of the violations and amend your privacy policies and technical procedures to assure this does not happen again;
- notify the potentially affected individuals of the violation;
- consider offering credit monitoring to help avert identity theft for the affected individuals; and
- consider sanctions against the employee.

Additional reading:

Accountability this is a companion document to The Nationwide Privacy and Security Framework for Exchange of Individually Identifiable Health Information
http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/accountability.pdf



Review your current policies and procedures regarding mitigating effects of uses and disclosures of PHI. Do your policies and procedures address who will be responsible for mitigation efforts due to misuse or disclosure by a Business Associate?

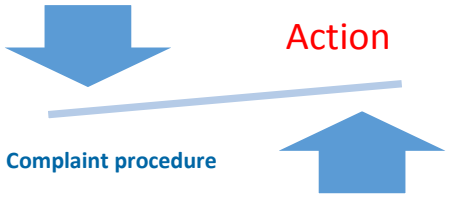
Safeguards

A CE must maintain reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of PHI. For practices that have EHRs, these topics will be discussed in greater detail in the Security section of this guide. For practices with paper records, examples of safeguards include, shredding documents containing PHI for disposal and limiting access to records with the use of locks.

Incidental Uses and Disclosures
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/incidentalusesanddisclosures.html

Complaints

A CE must have procedures for individuals to file complaints about compliance with the CE's own privacy policies and procedures and the Privacy Rule. The complaint procedure must be included in the CE's notice of privacy practices.



Review your current policies and procedures regarding how complaints are handled. Do your policies and procedures address who will be responsible for receiving and investigating complaints? Do all staff members know what to do if a patient complains about a privacy issue? Is the name or title of the person a patient can submit a complaint to included in your NPP? Is the information about how a patient can submit complaints to the Secretary of Health and Human Services included in your NPP?

Retaliation and waiver

A CE may not retaliate against an individual for:

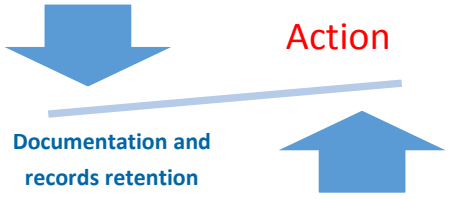
- filing a complaint for violations of the Privacy Rule or other HIPAA violations;
- exercising the individual's rights under the Privacy Rule; or
- assisting in an investigation by HHS or another appropriate authority.

A CE may not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment in a health plan or benefits eligibility.

Documentation and record retention

A CE must maintain documentation /records of the following for at least six years after the date of their creation or last effective date (whichever is later):

- its privacy policies and procedures;
- its notice of privacy practices;
- complaints received and their disposition; and
- other actions, activities, and designations that the Privacy Rule requires to be documented.



Review your current policies and procedures. Do they address retention of records related to privacy? Do they address retaliation and waiver of rights?



The Texas Medical Board Rules; Chapter 165.1 (b) Maintenance of Records requires:

(b) Maintenance of Medical Records.

(1) A licensed physician shall maintain adequate medical records of a patient for a minimum of seven years from the anniversary date of the date of last treatment by the physician.

(2) If a patient was younger than 18 years of age when last treated by the physician, the medical records of the patient shall be maintained by the physician until the patient reaches age 21 or for seven years from the date of last treatment, whichever is longer.

(3) A physician may destroy medical records that relate to any civil, criminal or administrative proceeding only if the physician knows the proceeding has been finally resolved.

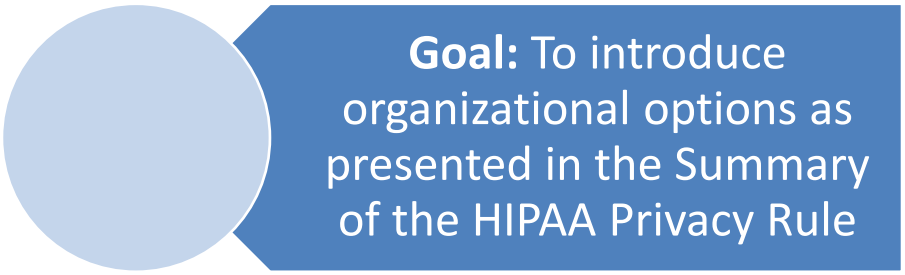
(4) Physicians shall retain medical records for such longer length of time than that imposed herein when mandated by other federal or state statute or regulation.

(5) Physicians may transfer ownership of records to another licensed physician or group of physicians only if the physician provides notice consistent with §165.5 of this chapter (relating to Transfer and Disposal of Medical Records) and the physician who assumes ownership of the records maintains the records consistent with this chapter.

(6) Medical records may be owned by a physician's employer, to include group practices, professional associations, and non-profit health organizations, provided records are maintained by these entities consistent with this chapter.

(7) Destruction of medical records shall be done in a manner that ensures continued confidentiality.[36]

Organizational Options



From the Summary of HIPAA Privacy Rule, "the rule contains provisions that address a variety of organizational issues that may affect the operation of the privacy provisions." If you, as a CE believe any of the following apply to your practice, you may want to seek legal advice about implementing them in your privacy policies and procedures. The following is quoted from the summary:

> **Hybrid entity –** The Privacy Rule permits a CE that is a single legal entity and that conducts both covered and non-covered functions to elect to be a "hybrid entity." (The activities that make a person or organization a CE are its "covered functions.") To be a hybrid entity, the CE must designate in writing 34its operations that perform covered functions as one or more "health care components." After making this designation, most of the requirements of the Privacy Rule will apply only to the health care components. A CE that does not make this designation is subject in its entirety to the Privacy Rule.
>
> **Affiliated CE –** Legally separate CEs that are affiliated by common ownership or control may designate themselves (including their health care components) as a single CE for Privacy Rule compliance. The designation must be in writing. An affiliated CE that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions.
>
> **Organized health care arrangement –** The Privacy Rule identifies relationships in which participating CEs share PHI to manage and benefit their common enterprise as "organized health care arrangements." CEs in an organized health care arrangement can share PHI with each other for the arrangement's joint health care operations.
>
> **CEs with multiple covered functions –** A CE that performs multiple covered functions must operate its different covered functions in compliance with the Privacy Rule provisions applicable to those covered functions. The CE may not use or disclose the PHI of an individual who receives services from one covered function (e.g., health care provider) for another covered function (e.g., health plan) if the individual is not involved with the other function. [37]

Group health plan disclosures to plan sponsors – A group health plan and the health insurer or HMO offered by the plan may disclose the following PHI to the "plan sponsor"—the employer, union, or other employee organization that sponsors and maintains the group health plan:

- Enrollment or disenrollment information with respect to the group health plan or a health insurer or HMO offered by the plan.
- If requested by the plan sponsor, summary health information for the plan sponsor to use to obtain premium bids for providing health insurance coverage through the group health plan, or to modify, amend, or terminate the group health plan. "Summary health information" is information that summarizes claims history, claims expenses, or types of claims experience of the individuals for whom the plan sponsor has provided health benefits through the group health plan, and that is stripped of all individual identifiers other than five digit zip code (though it need not qualify as de-identified PHI).
- PHI of the group health plan's enrollees for the plan sponsor to perform plan administration functions. The plan must receive certification from the plan sponsor that the group health plan document has been amended to impose restrictions on the plan sponsor's use and disclosure of the PHI. These restrictions must include the representation that the plan sponsor will not use or disclose the PHI for any employment-related action or decision or in connection with any other benefit plan.

Other Provisions: Personal Representatives and Minors



The Privacy Rule has two special provisions for use and disclosure of PHI to personal representatives in the case of minors.

> A Personal Representative is any adult that has decision-making capacity and who is willing to act on behalf of a patient. A personal representative would include an individual who has authority, by law or by agreement from the individual receiving treatment, to act in the place of the individual. This includes parents, legal guardians or properly appointed agents, like those identified in documents like Durable Power of Attorney for Healthcare, or individuals designated by state law.[38]

If a patient has an appointed personal representative, the Privacy Rule requires a CE to treat the "personal representative" the same as the individual, with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under the Rule. A personal representative is a person legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate. The Privacy Rule also specifies that a CE may elect not to treat a person through the personal representative if the CE has reason to believe that the personal representative may be abusing or neglecting the individual, or that treating the person as the personal representative could otherwise endanger the individual.

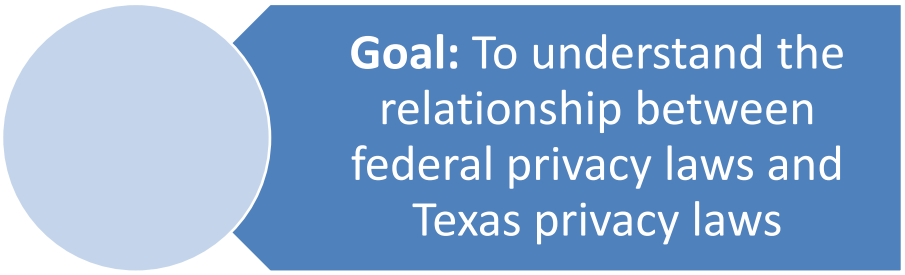
In most cases, parents are the personal representatives for their minor children. Generally speaking, parents can exercise individual rights, such as access to the medical record, on behalf of their minor children. There are cases in which the parent is not considered the personal representative. In these situations, the Privacy Rule defers to state and other law to determine the rights of parents to access and control the PHI of their minor children. If state and other law is silent concerning parental access to the minor's PHI, a CE has discretion to provide or deny a parent access to the minor's health information, provided the decision is made by a licensed health care professional in the exercise of professional judgment. [39]



According to the Texas Attorney General's Authorization to Disclose PHI form (1/2013):

A minor individual's signature is required for the release of certain types of information, including for example, the release of information related to certain types of reproductive care, sexually transmitted diseases and drug, alcohol or substance abuse, and mental health treatment (see Texas Family Code §32.003).

Relationship Between Federal and Texas Laws



In general, state laws that are contrary to federal laws are preempted by the federal laws. In the context of HIPAA, this means that the HIPAA Privacy Rule will apply or preempt state privacy laws that are contrary to the Privacy Rule. However, there are exceptions.



HIPAA preemption exceptions:

HIPAA provides for numerous exceptions to the general rule of federal preemption for contrary state laws including state laws that:

(1) Relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information than the privacy rule;
(2) Provide for the reporting of disease or injury, child abuse, birth or death, or for public health surveillance, investigation, or intervention; or
(3) Require certain health plan reporting or access to information for purposes of management or financial audits.

Texas privacy laws provide greater privacy protections than federal privacy laws.

The Texas Medical Records Privacy Act (Texas Health and Safety Code §181) was originally passed in an effort to bring the state into compliance with federal standards of patient privacy (HIPAA 1996). This law was revised, effective September 1, 2012, to reflect the changes of HB 300 (2011) and SB 1610. Members of the Texas legislature were concerned with the number of breaches of health and sensitive personal information that were occurring despite the existence of federal privacy laws such as HIPAA and HITECH and their associated penalties.

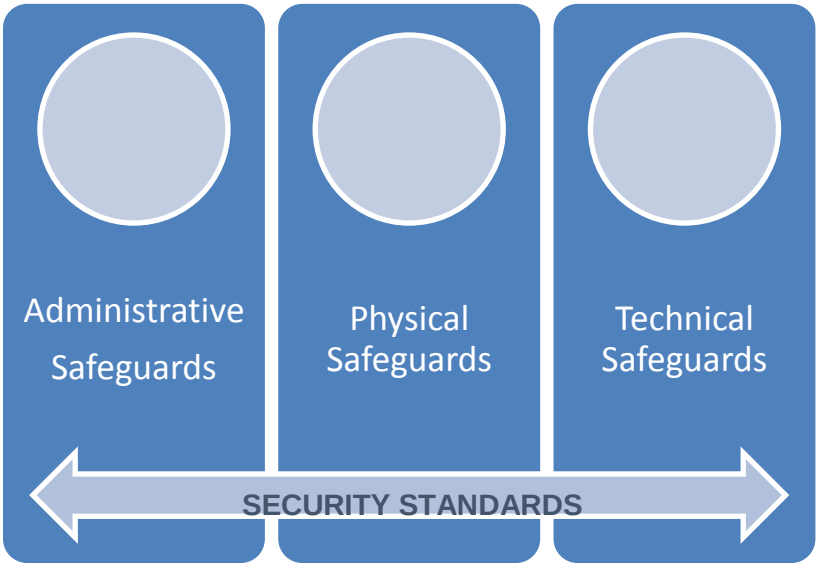
Effective April 1, 2009, the Texas Identity Theft Enforcement & Protection Act (ITEP) (Texas Business and Commerce Code §521) requires businesses to implement and maintain reasonable procedures to protect sensitive personal information (SPI) collected or maintained in the regular course of business from unlawful use or disclosure.

III. Security



It is important to understand the difference between HIPAA Privacy and Security Rules. The HIPAA Privacy Rule sets standards for who may have access to PHI; regardless of whether the PHI is in oral, written or electronic form. The HIPAA Security Rule sets standards for ensuring that only persons who should have access to ePHI can access it.

The Security Rule developed by the HHS reflects the concepts established by the Privacy Rule; administrative, physical, and technical safeguards.



.



HIPAA Omnibus Rule requires BAs and their subcontractors to meet the HIPAA Security Rule.

HIPAA Security Rule

Security is no longer accomplished by putting a lock on the door.

The HIPAA Security Rule is divided into three main sections or safeguards – each representing a set of standards and implementation specifications that must be addressed by all covered entities.

Each Security Rule standard is a requirement: a Covered Entity must comply with all of the standards of the Security Rule with respect to the ePHI it creates, receives, transmits or maintains.

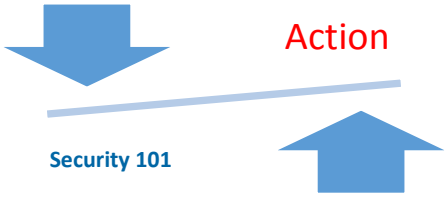
Security 101



Security 101 for Covered Entities is an overview of the Security Rule and how it works with the HIPAA Privacy Rule. It is an important document for you to reference as you develop your security policies and procedures.

As a solo practitioner or small practice you should focus your attention on number 1 and number 7 of the HIPAA Security Series publications.

HIPAA Security Series – 1: Security 101 for Covered Entities
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf



Bookmark the website for *Security 101 for Covered Entities*

Security 101 for Covered Entities sets out a framework for implementing the HIPAA Security Rule. According to *Security 101 for Covered Entities*:

> An implementation specification is an additional instruction for implementing a particular standard. Each set of safeguards comprises a number of standards, which in turn generally comprise a number of implementation specifications that are either required or addressable. If an implementation specification is required, the CE MUST implement policies and/or procedures that meet what the implementation specification requires. If the implementation specification is addressable, then the CE must assess whether it is a reasonable and appropriate safeguard in the entity's environment.[36]

The Security Rule has of a number of standards and implementation specifications. These are outlined in what is known as the Security Matrix. The matrix is printed at the end of *Security 101 for Covered Entities*. It is also included as Appendix G of this guide, with an additional column for you to make notes as you review your practice's current policies and procedures for meeting the Security Rule requirements and work through the implementation of the standards and implementation specifications.

Addendum to the HIPAA Security Matrix
http://aspe.hhs.gov/admnsimp/nprm/sec14.htm

The addendum notes: (1) While we have attempted to categorize security requirements for ease of understanding and reading clarity, there are overlapping areas on the matrix in which the same requirements are restated in a slightly different context. (2) To ensure that no Requirement or Implementation feature is considered more important than another, this matrix has been presented, within each subject area, in alphabetical order.

The appendix does not appear in the Code of Federal Regulations. This resource expands on the Security Standards Matrix and provides some additional implementation ideas. [41]

Security Rule Implementation for Small Providers



All CEs are required to demonstrate their compliance with the standards and implementation specifications in the Security Rule. *Security 101 for Covered Entities* outlines the following minimum processes for a CE. It is important to document what you do in each step, especially how you arrive at your decisions and develop your security policies and procedures.

Step 1 **Assess current security, risks and gaps**

Step 2 **Develop an implementation plan**

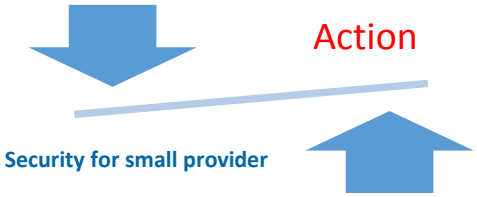
- **Read the Security Rule**
- **Review the addressable implementation specifications**
- **Determine security measures**

Step 3 **Implement solutions**

Step 4 **Document decisions**

Step 5 **Reassess periodically**

The seventh document in the CMS Security Series focuses on the special needs of small providers as they implement and maintain the requirements of the Security Rule. CMS recognized that implementing these rules as a small provider would represent unique challenges for compliance. CMS recognized that small providers are less likely to have IT staff to assist with compliance issues.



Bookmark the web site for Implementation for the Small Provider.

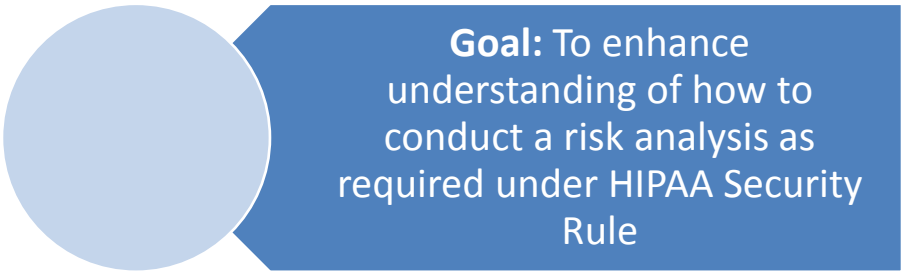
The majority of the document is devoted to helping small providers work through the Security Matrix. The matrix is slightly reformatted to include sample questions to help you assess compliance. You may want to use the sample questions in conjunction with the Security Matrix formatted in Appendix G.

Additionally you will see that the modified matrix divides implementation specifications into risk analysis and risk management. A risk analysis is an assessment of the risks and vulnerabilities that could negatively impact the confidentiality, integrity, and availability of the ePHI held by a CE, and the likelihood of occurrence. The risk analysis may include taking inventory of all systems and applications used to access and house data, and classifying them by level of risk. A thorough and accurate risk analysis would consider all relevant losses that would be expected if the security measures were not in place, including loss or damage of data, corrupted data systems, and anticipated ramifications of such losses or damage. Risk management is the actual implementation of security measures to sufficiently reduce an organization's risk of losing or compromising its e-PHI and to meet the general security standards. Both pieces are necessary for minimizing your risk of violations from federal and Texas privacy and Security Rules.

As you work through the matrix, you need to determine what is reasonable and appropriate for your practice. Consider cost, size of practice, technical structure and available resources. You may determine that you want to address the highest risk items first. Keep in mind that even implementation specifications labeled as addressable that you determine are not reasonable at this time does not exempt the CE from meeting the requirements.

> **Administrative safeguards –** The Security Rule defines administrative safeguards as "the administrative actions, policies, and procedures to manage the selection, development, implementation and maintenance of security measures to protect electronic PHI and to manage the conduct of the CE's workforce in relation to the protection of that information."
>
> **Physical safeguards –** The Security Rule defines physical safeguards as "physical measures, policies and procedures to protect a CE's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion."
>
> **Technical safeguards –** The Security Rule defines technical safeguards as "the technology and the policy and procedures that protect ePHI and control access to ePHI."[42]

Conducting a Risk Analysis



HIPAA Security Rule requires all CEs to perform a risk analysis. According to the HIPAA Security Series, "All ePHI created, received, maintained, or transmitted by a CE is subject to the HIPAA Security Rule."[1] One of the requirements of the security management process standard in the Security Rule states, that all CEs must "implement policies and procedures to prevent, detect, contain, and correct security violations."[43]

A risk analysis is defined as "conducting an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the CE."[44]

The Security Rule does not prescribe a required methodology to complete a risk analysis. It is essential that every practice that has ePHI conduct a risk analysis to determine their threats and vulnerabilities that then become the basis of their action plan to manage the risks.

Below are three options for the risk analysis process. Many others exist, including using consultants and attorneys who specialize in HIPAA privacy and security.

OPTION 1:

A very basic starting point for solo/small practices may be to print a copy of the HIPAA Security Matrix and Addendum, found in Appendix G or print a copy of the modified matrix found in the Security Series – 7 Security Standards: Implementation for Small Providers on pages 4 – 11. Physicians, office administrative staff, and IT support personnel can simply make notes in the margin in Appendix H of what you are currently doing and what you need to begin working on. It is recommended that you maintain your notes in an easily retrievable format; options include a three ring binder or a shared folder on your network. This may not fully meet the OCR requirements if audited or investigated.

OPTION 2:

The second option is based on HIPAA Security Series #6 – Basics of Risk Analysis and Risk Management. The steps below provide a guide for physicians and key staff to use to conduct a risk analysis as outlined in the publication. For each step the publication provides more details of what should be done.

- identify the scope of the analysis
- gather data
- identify and document potential threats and vulnerabilities
- assess current security measures
- determine the likelihood of threat occurrences
- determine the potential impact of threat occurrence

- determine the level of risk
- identify security measures and finalize documentation

OPTION 3:

A much more comprehensive risk assessment model can be found in the National Institute of Standards and Technology (NIST) publication, *Risk Management Guide for Information Technology Systems*.

See the flow chart on page 58 for a summary of the methodology for conducting a risk analysis contained in this publication.[45]

OPTION 4:

TMLT offers Risk Analysis services which includes review of both privacy and security rules. Customized proposals are developed to meet the needs of the practice. The time to complete the risk analysis is dependent upon the size and complexity of the practice. For more information call 800-580-8658 Extension 4884 or email consultingwebmail@tmlt.org.

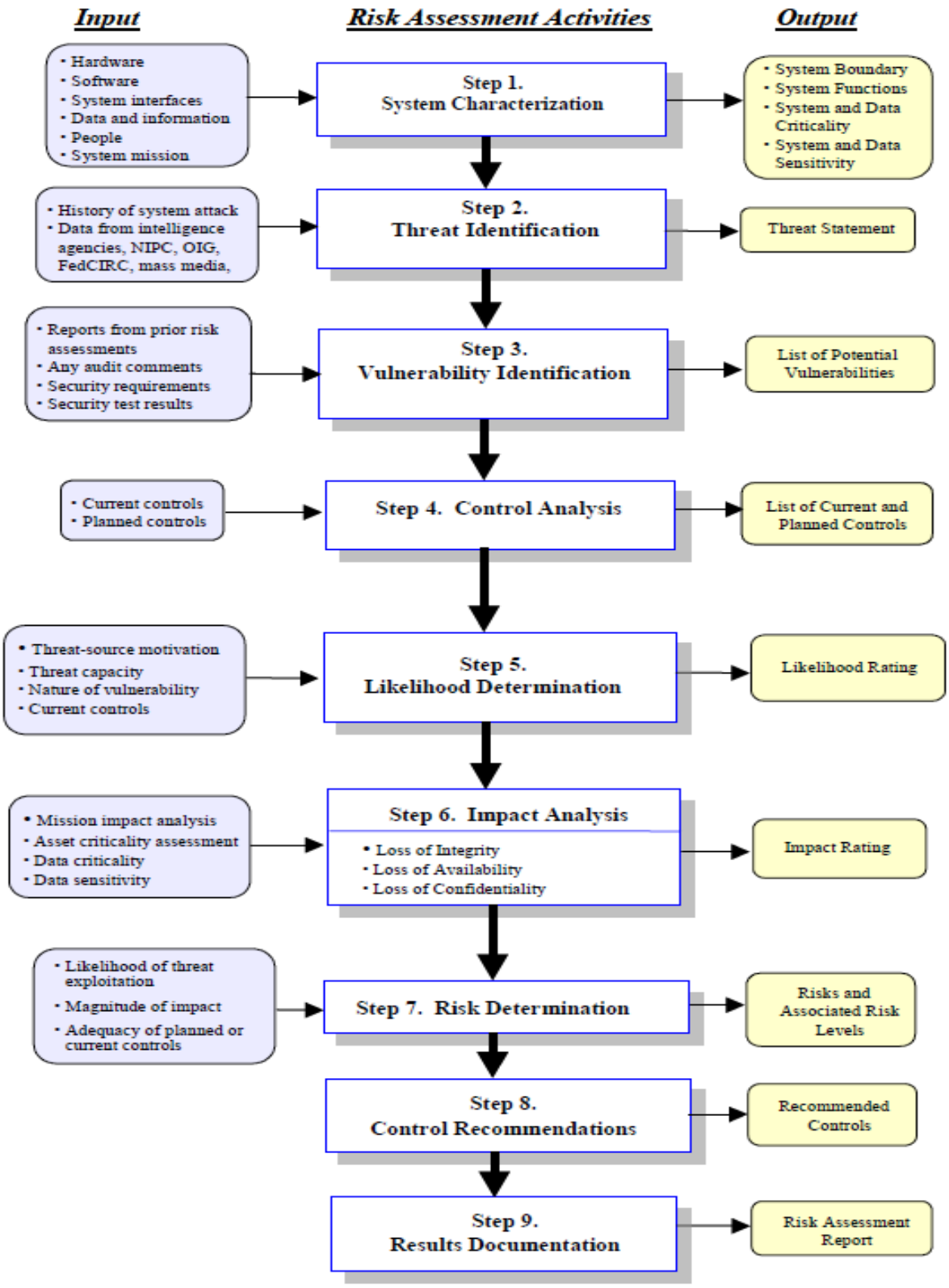
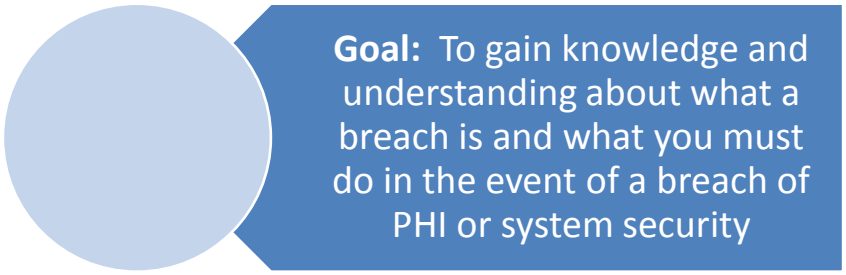


Figure 3-1. Risk Assessment Methodology Flowchart

IV. Breach and Breach Notification



Federal law requires all CEs and BAs to notify patients if there are breaches involving their PHI.

Texas law, effective September 1, 2012 added additional breach notification requirements for breaches of system security. These will be discussed in the section Texas Identity Theft Enforcement and Protection Act.

CEs and their BAs must comply with the new breach notification requirements as defined in the HIPAA Omnibus Rule.

Upon discovery of a breach of unsecured PHI (PHI), CEs must provide notification to:

- the affected individuals;
- the Secretary of the HHS; and
- in some cases, to the media.

What Constitutes Unsecured PHI?

PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by HHS is unsecured. Unsecured PHI (e.g., medical information such as a diagnosis plus a patient's name, address, social security number, etc.) can be in any form or medium including electronic, paper, or in oral form. Data is considered secure if it is encrypted in a manner that is acceptable to HHS.

BREACH

A breach is an unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of such information.[64]

Covered Entities must comply with breach notification requirements specified in HIPAA Omnibus Rule.

Breach notification

CEs are required to notify the affected individuals of any unauthorized acquisition, access, use, or disclosure of unsecured PHI without unreasonable delay but not later than 60 calendar days after discovery. Thus if the physician has compiled all of the necessary information to provide notification of a breach of unsecured PHI to affected individual(s) by day 10 (10 days from the day the breach was discovered) but waits until day 60 to send notifications, this could constitute an unreasonable delay.

BAs who have access to PHI are required to notify the CE of any such breach, including the name of any individual whose unsecured PHI has been released. Physicians should make sure that their agreements with BAs address the new breach notification requirements, including the timing of BA notification to a CE following a breach, who will make the notification to patients and the responsibility for paying costs resulting from a breach. While HHS has indicated that the parties to BA agreements have flexibility in this regard, it has encouraged the parties to ensure that individuals do not receive notification from both the BA and the CE, as this could be confusing.

With the issuance of the HIPAA Omnibus Rule, Breach notification requirements and the obligation to notify patients if a breach of their PHI has occurred has been expanded and clarified.



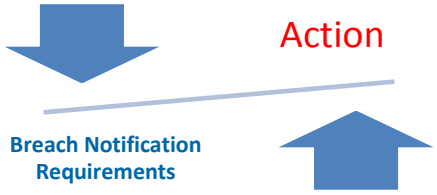
The HIPAA Omnibus Rule sets new standards for reportable breaches.

The AMA Omnibus Summary states; “Breaches are now presumed reportable unless, after completing a risk analysis applying four factors, it is determined, that there is a ‘low probability of PHI compromise.’ The physicians must consider **all** of the following four factors:

- the nature and extent of the PHI involved – issues to be considered include the sensitivity of the information from a financial or clinical perspective and the likelihood the information can be re-identified;
- the person who obtained the unauthorized access and whether that person has an independent obligation to protect the confidentiality of the information;
- whether the PHI was actually acquired or accessed, determined after conducting a forensic analysis; and
- the extent to which the risk has been mitigated, such as by obtaining a signed confidentiality agreement from the recipient.”[65]

It is important for CEs with cyber liability insurance to notify their carriers as soon as they believe a breach may have occurred. Most insurance carriers have specified timeframes in which an insured can report an incident. The carrier may have resources available (e.g. legal counsel) to assist with the investigation, reporting requirements, and notification to patients.

If your practice does not have cyber liability coverage, and you believe a breach of PHI has occurred, you should consider consulting with legal counsel for assistance in this process.



Review your existing policies and procedures on breaches and breach notifications. Review BAAs and assure they include breach notification requirements for the BA to notify the CE.

Discovery of breaches

Breaches are treated as discovered as of the first day on which the breach is known or should have been known to the physician (or where the BA). The date of discovery is when the timeline for notice starts.

How to provide notice

Notice to the affected individuals

Physicians should send written notification via first class mail to each affected individual (or if deceased, the individual's next of kin) at the last known address, unless the individual has indicated a preference for e-mail. In situations where a physician deems possible imminent misuse of unsecured PHI, the physician may provide other forms of notice, such as by telephone, in addition to the written notice.

If the address is insufficient or out of date for fewer than 10 individuals, then a substitute notice must be provided by other means reasonably calculated to reach the affected individual, such as by telephone. If the address is insufficient or out of date for 10 or more individuals, then a substitute notice must be provided by either a conspicuous posting on the front page of the entity's web site for 90 days or a conspicuous publication in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside. Further, the substitute notice must include a toll-free number that remains active for at least 90 days.

Notice to the media

If the breach of unsecured PHI affects more than 500 individuals of a state or jurisdiction, then the notice must also be provided to major media outlets serving the relevant state or jurisdiction. The notice to the media must contain the same information as the written notice to individuals, and must similarly be provided without unreasonable delay, but in no case later than 60 calendar days after discovery of the breach.

Notice to HHS

Additionally, CEs must notify HHS of all breaches of unsecured PHI in the manner specified on the HHS website. For breaches that involve 500 or more individuals, CEs must provide notification to HHS contemporaneously with the notice sent to the affected individuals. The HHS web site will have a list that identifies the CEs involved in breaches in which 500 or more individuals are affected. If less than 500 individuals are affected, then the CE must maintain a log or other documentation of the breaches and must report such breaches to HHS no later than 60 days after the end of each calendar year in which the breaches occurred.

V. Encryption

Goal: To provide information about encryption and the benefits it brings to ePHI security

CEs are required to develop policies and procedures to safeguard ePHI in accordance with HIPAA/HITECH and Texas privacy and security requirements. One of the most significant changes from HITECH and HB 300 is the requirement to notify patients and the HHS of a breach.

Encryption is "a method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (i.e., type of procedure or formula). If information is encrypted, there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt (i.e., translate) the text and convert it into plain, comprehensible text."[66]

"Encryption is a technique for transforming information in such a way that it becomes unreadable."[67]

Example of Unencrypted vs. Encrypted Data

Unencrypted	Encrypted
Patient: Jane Doe MRN: 1234567 DOB 01-01-1991 Current Medications: ASA 81 mg daily MVI 1 daily Lasix 40 mg BID	Πατιεντ: ϑανε Δοε Χυρρεντ Μεδιχατιονσ: 81 μγ δαιλψ ΜϛΙ 1 δαιλψ Λασιξ 40 μ γ ΒΙΔ

ENCRYPTION



When it comes to HIPAA Security, encryption is the key for protection of ePHI from a breach.

The goal of encryption is to protect ePHI from being accessed and viewed by unauthorized users.

The Security Series states, "Technical safeguards are becoming increasingly more important due to technology advancements in the health care industry. As technology improves, new security challenges emerge. Healthcare organizations are faced with the challenge of protecting ePHI, such as electronic health records, from various internal and external risks. To reduce risks to ePHI, covered entities must implement technical safeguards."[68]

In Sang Lee's 2010 article "HIPAA encryption: Meeting Today's Regulations":

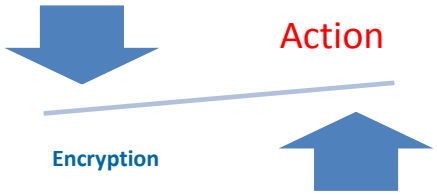
> "If you work with an organization that must adhere to HIPAA, you know by now that encryption is now a de facto primary aspect of HIPAA compliance after the passing of the HITECH Act.
>
> There are a couple of reasons for this increased focus on encryption.
>
> First, the HHS issued guidance wherein "unsecure PHI" is essentially any PHI that is not encrypted or destroyed. Under this definition, it doesn't matter how many chains, walls, doors, biometric gizmos and guards with lethal weapons you have at your service. As long as PHI is not encrypted, it is considered unsecured.
>
> A second and more compelling reason why encryption is now a requirement is the introduction of HITECH's breach notification initiative, which requires HIPAA-covered entities to send notification letters if there is a breach of unsecured PHI. However, as HHS pointed out, the use of encryption grants safe harbor in the event of a breach because encrypted PHI is not unsecured PHI.
>
> Oddly enough, in the same breath, HHS also notes that "Covered Entities and Business Associates are not required to follow the guidance." However, cleaning up the mess behind a breach notification can cost millions of dollars, so one would have to be supremely confident — or reckless — in not taking advantage of the encryption safe harbor. With such mixed signals, though, it is not hard to see why encryption is called a de facto requirement."[69]

The AMA FAQs on HIPAA security rule includes a few very pertinent questions for solo and small practices.

> **"Q:** I manage a small practice; why should I care about the changes to the HIPAA Security Rule?
>
> **A:** Perhaps the most significant of the changes to the HIPAA Security Rule is the requirement for a CE and their Business Associates to provide notification in the event of a breach of "unsecured PHI."
>
> The one and only exception to this new requirement is encryption technology: if the ePHI is stored and transmitted in encrypted form, then you do not need to notify patients, even if there is a security breach.
>
> **Q:** How can I encrypt the data on my computers?
>
> **A:** You have several choices. There are built-in encryption programs, such as Microsoft Encrypting File System (EFS), which you can use simply by changing the properties of the folder in which sensitive data is kept (if you use a computer with Microsoft Windows). Most of the popular database technologies, such as Microsoft SQLServer, Oracle, and Sybase, include an encryption option you can use. There are also several encryption products, such as Pretty Good Privacy, that you can purchase and install on your computer.
>
> **Q:** What is the best encryption technology to use?
>
> **A:** In 2000, NIST sponsored a competition to identify the best available encryption algorithm. The Rijndael algorithm won the competition hands down. This algorithm has been designated as the current advanced encryption standard (AES). AES is a good choice for protecting ePHI." [70]

Encryption has been referred to as a "free pass" or "get out of jail free card" in the event of a breach if encryption is done in accordance with the stated NIST guidelines and the key is kept on a device other than

the one on which the data is stored. Keep in mind that technology has advanced very quickly and encryption on certain types of devices may or may not provide the "free pass." Medical practices are strongly encouraged to involve IT personnel or consultants when considering the purchase and use of encryption.



Get help from an IT expert when considering encryption

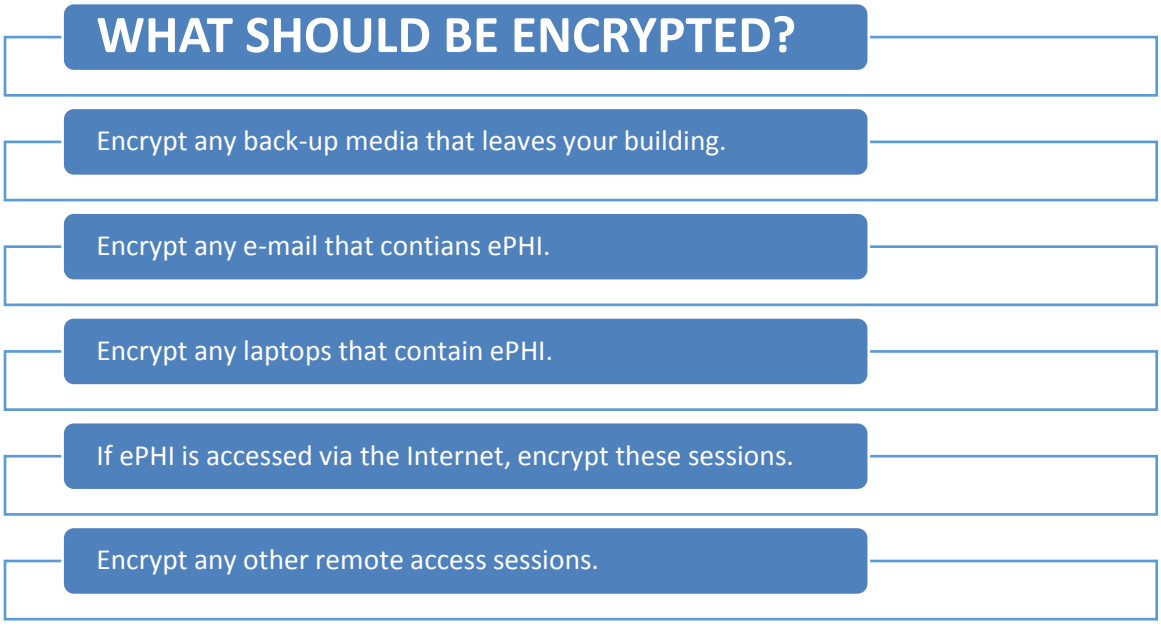
Remember, it is essential that all devices that may contain ePHI are encrypted if you choose encryption as a technical safeguard. Be sure to keep your device inventory current and indicate that encryption is in place as new devices are added.

The NIST's Guide to Storage Encryption Technologies for End User Devices states:

> "In today's computing environment, there are many threats to the confidentiality of information stored on end user devices, such as personal computers, consumer devices (e.g., personal digital assistant, smart phone), and removable storage media (e.g., universal serial bus [USB] flash drive, memory card, external hard drive, writeable CD or DVD). Some threats are unintentional, such as human error, while others are intentional.
>
> Many threats against end-user devices could cause information stored on the devices to be accessed by unauthorized parties. To prevent such disclosures of information, particularly of personally identifiable information (PII) and other sensitive data, the information needs to be secured. Securing other components of end user devices, such as operating systems, is also necessary, but in many cases additional measures are needed to secure the stored information. This publication explains the basics of storage security, which is the process of allowing only, authorized parties to access and use stored information. The primary security controls for restricting access to sensitive information stored on end-user devices are encryption and authentication.
>
> It is important to note, that NIST standards are not requirements of covered entities. Only federal departments and agencies are required to meet these standards. However, during a privacy or breach investigation, being able to show that a practice meets these standards could be very helpful to a CE.
>
> It is recommended that all physicians should encrypt any systems and individual files that contain ePHI. Examples of what should be encrypted include (but not limited to) your practice management system; electronic medical records, documents containing ePHI (claims appeals), scanned images, copies of remittance advices, emails containing ePHI and ePHI that you transmit, such as the claims sent to a clearinghouse.
>
> There are two types of data to consider for encryption, data at rest and data in motion. Data at rest is stored data. Data at rest is subject to breach if your network defenses are penetrated by hackers or other unauthorized persons. Some covered entities choose to only encrypt data in

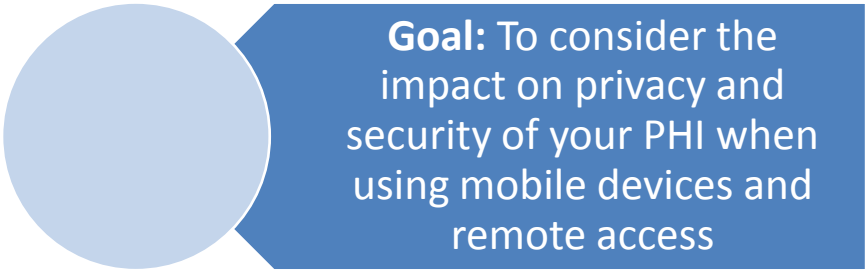
motion or data that is being transmitted. It is important to consider both data at rest and data in motion. This is a critical decision that needs to be made by a practice." [71]

The AMA recommends you encrypt the items listed in the diagram below, examples of data in motion.[72]



Additional reading on Encryption is available from NIST:
http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800111.pdf

VI. Mobile Devices, Texting and Remote Access



As practitioners embrace EHRs and technology continues to change in healthcare, vendors are creating applications to allow access to PHI from mobile devices or through remote access connections. The concept of BYOD (Bring Your Own Device) is widespread. Mobile devices continue to get smaller, lighter weight and more affordable, making BYOD even more prevalent. Devices that are small and less expensive can now contain large amounts of information, including PHI. Mobile devices may impose one of the greatest threats to the security of your PHI today.

HIPAA implications

According to the Department of Health and Human Services, the HIPAA Security Rule outlines national standards designed to protect individuals' electronic protected health information (ePHI) that is created, received, used, or maintained by a CE. Unauthorized disclosure of PHI is a risk because mobile devices are capable of storing data. Most mobile devices used to exchange PHI retain a record of that data on the device.

CEs must carefully evaluate the HIPAA Security Rules and apply them to mobile devices before deciding to grant access to users. Mobile devices are vulnerable to loss and theft because of their small size and portability.

The Health & Human Services has a publication on HIPAA Security Guidance, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf. In it they state:

> There have been a number of security incidents related to the use of laptops, other portable and/or mobile devices and external hardware that store, contain or are used to access ePHI under the responsibility of a HIPAA CE. All covered entities are required to be in compliance with the HIPAA Security Rule, which includes, among its requirements, reviewing and modifying, where necessary, security policies and procedures on a regular basis. This is particularly relevant for organizations that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the CE.[73]

Mobile devices

Mobile devices may include any device that is easily portable with electronic storage capacity; including but not limited to laptops, smart phone, tablet computers, external hard drives, thumb drives and an array of other medical devices which may contain PHI.

Practices must apply the HIPAA Security Rule to any device that stores or transmits PHI, including conducting a risk analysis to identify vulnerabilities associated with the device(s).

Additional Resources on Mobile Device Use:



Mobile Device Best Practices and Recommendations: http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049463.hcsp?dDocName=bok1_049463



Your Mobile Devices and Health Information Privacy and Security: http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

Texting

Texting has become a convenient and popular way to communicate using mobile devices. The practice of texting information about patients between practitioners or staff and practitioners can present a risk of breach and extreme caution must be used to protect PHI.

Texting provides a quick and efficient way to communicate short messages; however, if the text includes PHI, they have implications under HIPAA.

The Omnibus Rule clarifies that if patients want to receive their health information via an unsecure means, such as email, the provider must provide an explanation of the risks associated with this method of communication.[74] Based on the explanation the patient receives, they will make an informed decision to accept or reject this method of communication. Sheldon-Dean and Phalke suggest in a recent article in Compliance Today, "the same logic may apply to texting."[75]

Assessing the risks of use of texting as part of your risk analysis is an important step when deciding whether or not to use texting technology.

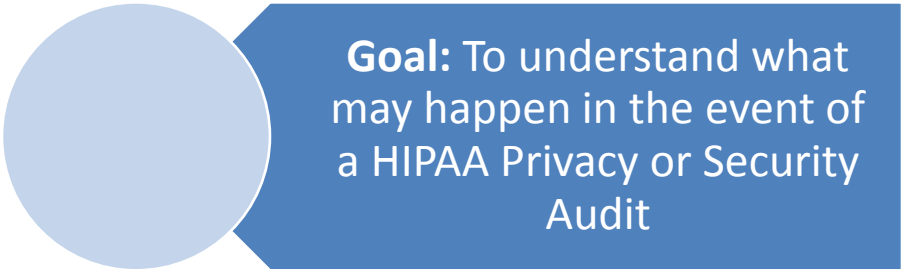
Remote access

Whenever your PHI is accessed remotely, the CE needs to determine the most secure manner to transmit it. The HHS document on HIPAA Security Guidance suggests the following possible risk management strategies when dealing with remote access requests:

- Prohibit transmission of ePHI via open networks, such as the Internet, where appropriate
- Prohibit the use of offsite devices or wireless access points (e.g. hotel workstations) for non-secure access to email
- Use more secure connections for email via SSL and the use of message-level standards
- Implement and mandate appropriately strong encryption solutions for transmission of ePHI
- SSL should be a minimum requirement for all Internet facing systems which manage ePHI in any form, including corporate web-mail systems.[76]

The HIPAA Security and Privacy Rules require all covered entities to protect the EPHI that they use or disclose to business associates, trading partners or other entities. New standards and technologies have significantly simplified the way in which data is transmitted throughout the healthcare industry and created tremendous opportunities for improvements in the healthcare system. However, these technologies have also created complications and increased the risk of loss and unauthorized use and disclosure of this sensitive information.[77]

VII. HIPAA Privacy and Security Audits and Investigations



Random audits:

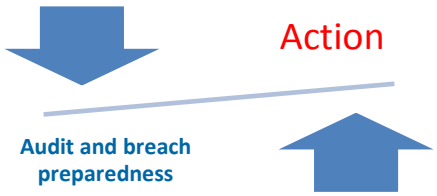
The American Recovery and Reinvestment Act of 2009, in Section 13411 of the HITECH Act, required the HHS:

- to provide for periodic audits to ensure CEs and BAs are complying with the HIPAA Privacy and Security Rules and breach notification standards; and
- to implement this mandate, OCR piloted a program to perform 115 audits of CEs to assess privacy and security compliance. Audits conducted during the pilot phase began November 2011 and concluded in December 2012.

At this time it is unclear when HHS may resume random compliance audits. It is recommended that CEs be prepared for an audit in the event they are resumed.

Investigation for a complaint or as a result of a breach notification

All CEs are required to demonstrate their compliance with the security standards. "The U.S. Department of Health and Human Services (HHS) and the Office of Civil Rights (OCR) has been cracking down on its enforcement of the HIPAA/HITECH Privacy, Security and Data Breach Notification Rules, by investigating entities that have reported data breaches and other privacy incidents" according to an article in *Healthcare IT News.*[50] As a result, CEs need to be prepared to respond should the OCR investigate a breach.



Review your cyber liability coverage. Review your breach response procedure.

12 Steps for Surviving an OCR Breach Investigation

"ID Experts offers 12 steps to help covered entities identify key items in their privacy and security programs that will protect the privacy of their patients before a data breach, and ensure compliance with breach notification regulations after a data breach.

1. Assign privacy and security responsibility. Ensure accountability for patient privacy with a specifically designated privacy official in your organization.

2. Annual risk analysis. Carry out an annual risk analysis intended to identify privacy/security risks and vulnerabilities.

3. Address security vulnerabilities. Implement security measures to reduce risks and vulnerabilities identified in most recent risk assessment.

4. Workforce privacy awareness. Train workforce members including management and volunteers in patient privacy and security requirements, and document evidence of security awareness enforcement.

5. Policy and procedure completeness. Develop thorough policies and procedures for safeguarding PHI (PHI) and for unauthorized disclosure of PHI.

6. Prepare for privacy incidents. Develop procedures and tools for compliant investigation, analysis, and review.

7. Incident reporting. Capture and maintain a copy of the incident report that was created/submitted that triggered concern that a potential breach has occurred.

8. Analysis of incident. Develop and document a detailed description of the facts of the incident and the incident risk assessment that you carried out to determine if the incident requires notification to affected individuals and authorities.

9. Patient notification. Develop and document your notification to individuals/patients affected by the data breach, including all means used to ensure delivery of the notification.

10. Mitigate harm to affected individuals. Describe decisions/actions taken to mitigate the harm to individuals/patients affected by the breach.

11. Notifications to regulators and media. Develop and document your notifications to necessary regulatory authorities including HHS/OCR as well as media.

12. Determine root cause and corrective actions. Determine and document actions to determine the root cause of the incident and to address the root cause with corrective actions."[78]

VIII. Texas Medical Records Privacy Act

Goal: To provide an overview of Texas Medical Records Privacy Act

Texas HB 300 (2011) added even more reporting requirements for CEs. Throughout this guide additional information has been highlighted in appropriate sections. Below is a snapshot of the changes:



The Texas Medical Records Privacy Act, as amended by HB 300 (2011) and further amended by SB 1609 and 1610 (2013)

The Texas Medical Records Privacy Act's privacy requirements exceed those found in the HIPAA Privacy Rule. The bill amends the Texas Medical Records Privacy Act and places the following requirements on covered entities regarding PHI.

HB 300 Changes According to HIMSS Fact Sheet:

- Covered Entities must provide customized employee training regarding the state and federal law concerning PHI and maintain records of completion of training. Training will be required every two years and new employees must be trained no later than 60 days after their hire date.
- If a health care provider is using an EHR that is capable of fulfilling a patient's record request, patients must be provided with electronic copies of their health records (unless the patient is willing to accept this in another form) within 15 days of the patient's written request for the records. This is stricter than HIPAA's requirement of 30 days.
- Covered Entities are required to provide patients with notice that their PHI is subject to electronic disclosure.
- A Covered Entity is prohibited from disclosing a patient's PHI to any other person in exchange for direct or indirect payment. However, covered entities may disclose a patient's PHI to other covered entities for treatment, payment, health care operations, insurance or HMO functions, or as authorized or required by federal or state law.[79]

SB 1609 Changes:

- Covered Entities must provide no later than 90 days after their hire date and as soon as possible after the law changes



The Texas Medical Records Privacy Act, as amended by HB 300

- The Texas Health and Human Services Executive Commissioner — in consultation with the Department of State Health Services, Texas Medical Board, and the Texas Department of Insurance — may recommend a standard electronic format for the release of requested health records that must be consistent, if feasible, with federal law regarding the release of EHRs.
- The Health and Human Services Commission, in consultation with the Texas Health Services Authority (THSA) and Texas Medical Board "shall review issues regarding the security and accessibility of PHI maintained by an unsustainable Covered Entity" and present recommendations by December of 2012. This includes recommending the state agency to which PHI from an unsustainable Covered Entity should be transferred for storage.
- The Attorney General must:
    - Maintain a web site: describing consumer privacy rights under state and federal law provide a list of state agencies that regulate covered entities and the types of entities each agency regulates, provide detailed information regarding each agency's enforcement process, and contact information for each agency for reporting violations of the Texas Medical Records Privacy Act. https://www.oag.state.tx.us/consumer/hipaa.shtml
    - Submit an annual report to the legislature detailing the number and types of privacy complaints filed with state agencies and the attorney general during the previous year and the enforcement action taken in response to each complaint. In the report, patient PHI must be de-identified.[80]

IX. Texas Identity Theft Enforcement & Protection Act (ITEP)

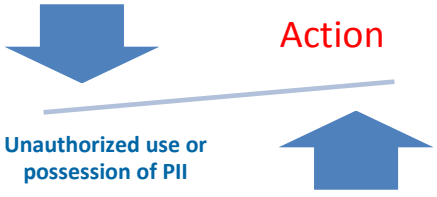
Goal: To provide an overview of the Texas Identity Theft Enforcement & Protection Act

Unauthorized Use or Possession of PII



Title 11, Personal Identity Information, Chapter 521 — Unauthorized use of Identifying Information of the Texas Business and Commerce Code, [also known as Texas Identity Theft Enforcement & Protection Act (ITEP)] defines Sensitive Personal Information (SPI) as:

- an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - social security number;
  - driver's license number or government-issued identification number; or
  - account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
- information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual.[81]



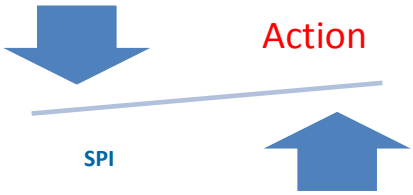
Do you have a policy on unauthorized use or possession of personal identifying information?

Under ITEP, a person may not obtain, possess, transfer, or use PII of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

PII is defined as information that alone or in conjunction with other information identifies an individual, including (1) an individual's name, social security number, date of birth or government-issued identification number, (2) mother's maiden name, (3) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image, (4) unique electronic identification number, address, or routing code and (5) telecommunication access device as defined by Section 32.51 of the Texas Penal Code.

Duty to Protect SPI

ITEP requires that you protect SPI by implementing and maintaining reasonable procedures to protect from unlawful use or disclosure of any SPI collected or maintained in the regular course of your business.



Do you have a policy on SPI including employee access to it and use of it?



Texas Identity Theft Enforcement & Protection Act (ITEP) changes made by HB 300 (2011):

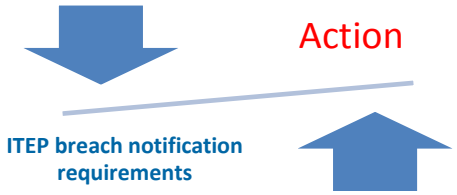
- Broad breach notification requirements were added to ITEP.
- CE must provide notifications to any affected individuals (previously only Texas residents).
- If the breach affects a person who is a resident of another state, notice is to be provided pursuant to the notification laws of the non-resident's state.
- If the affected person's state of residence does not have breach notification laws, ITEP notification rules apply.

ITEP Breach Notification Requirements

Any person who conducts business in Texas and owns or licenses computerized data that includes SPI must disclose any breach of system security, upon its discovery or upon receiving notification of the breach, to any Texas resident who's SPI was or is reasonably believed to have been acquired by an unauthorized person. The notification must be provided as quickly as possible. Delay in notification is permitted at the request of a law enforcement agency or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

ITEP also requires any person who maintains computerized data that includes SPI not owned by the person to notify the owner or license holder of that information of any breach of system security immediately after discovering the breach if the SPI was or is reasonably believed to have been acquired by an unauthorized person. A delay in notification is permitted at the request of a law enforcement agency.

"Breach of System Security" is defined as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.

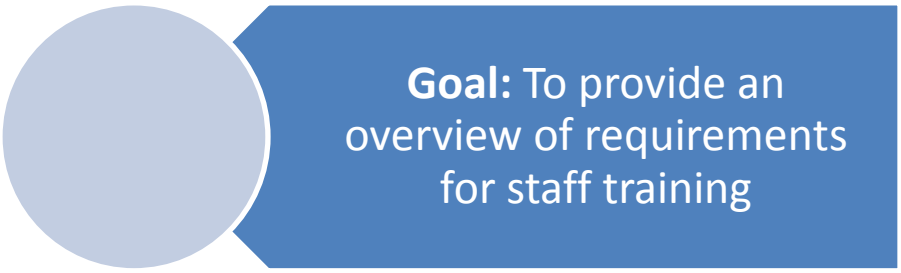


Review your policies and procedures on breach notification and revise to reflect ITEP requirements.

The Texas Attorney General has information on Identity Theft on their web site.

https://www.oag.state.tx.us/consumer/identity_theft.shtml

X. Training Requirements



CEs are required to develop policies and procedures, conduct training, and develop a notice of privacy practices and BAAs in accordance with HIPAA/HITECH privacy and security requirements.

Training requirements as mandated by the federal and Texas privacy and security laws include:

HIPAA

Training requirements under HIPAA are fairly broad and relatively easy for CEs to meet.

- Employees must be trained on HIPAA requirements regarding PHI
- Training is to be afforded as necessary and appropriate to carry out the employee's job function (i.e. not everyone needs to be trained to the level of the privacy or security officer if all they do is scheduling and have limited access to PHI)
- New employees must be trained within a reasonable period of time after being hired (i.e. larger CEs might do HIPAA training quarterly for new employees)
- All employees must receive training for any material changes in HIPAA (i.e. a practice trained employees in 2003 on HIPAA Privacy and additional training was done in 2005 for HIPAA Security. Another example might be retraining when a practice transitions from paper medical records to an electronic medical record.)
- CEs must document training (i.e. a new employee orientation checklist has HIPAA training listed; the date and initials/signature of employee and trainer are on the checklist.)

HITECH

HITECH does not specifically address training requirements. However, clearly under the training requirements of HIPAA "whenever there are material changes in HIPAA", retraining of employees was required as CEs made changes to meet HITECH.

Texas Medical Records Privacy Act

The Texas Medical Records Privacy Act includes more stringent training requirements than those found in HIPAA. However, the recently concluded 2013 Texas legislature again brought changes to the Texas Medical Privacy Act and Identity Theft Protection and Enforcement Act (ITEP). These changes were made to ease the burden of educating staff as well as clarifying reporting requirements of ITEP.

- Employees are to be trained on state and federal laws on PHI.
- Each CE shall provide training to employees of the CE regarding the state and federal laws concerning PHI as necessary and appropriate for the employees to carry out the employees' duties for the CE.
- CEs must train new employees by the 90th day of employment.
- If the duties of an employee of a CE are affected by a material change in state or federal law concerning PHI, the employee shall receive training within a reasonable period of time, but not later than the first anniversary of the date the material change in law takes effect.
- Employers must maintain signed statements from employees verifying training.



Review your current office training on state and federal laws.

Additional information is available in another volume in the toolkit, Introduction to Developing Customized Office Physician Training.

XI. Minimizing Your Risk



If you are not convinced that your practice should proactively be reviewing the requirements of privacy and security rules and laws, developing and implementing written policies and procedures, as well as train staff, consider the following:

- Lengthy investigations by the OCR over allegations of a breach
- Federal and Texas medical privacy and security laws have significant financial penalities for violations in the event of a breach
- Potential for reputational harm from reporting a breach
- Random audits by the OCR required under the HITECH Act

TMLT has additional help available if you need it, from risk analysis, to developing policies and procedures to educating your staff, we will develop a customized proposal to meet your needs; contact us at 800-580-8658 extension 4884 or email consultingwebmail@tmlt.org.

Footnotes

1	*the Reporter* 2012 Vol. 3 https://s3.amazonaws.com/resources.tmlt.org/PDFs/Reporter/2012_Volume3.pdf
2	Summary of HIPAA Privacy Rule page 2 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
3	Summary of HIPAA Privacy Rule page 2 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
4	TMA 2012 EHR Survey Flyer http://www.texmed.org/WorkArea/DownloadAsset.aspx?id=25312
5	*Doc-office use of basic EHRs hits nearly 40%* Modern Healthcare http://www.modernhealthcare.com/article/20121206/NEWS/312069953#ixzz2EJ1C6rgi?trk=tynt accessed 12/6/12
6	https://federalregister.gov/a/2013-01073 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules Page 1
7	AMA HIPAA Omnibus Final Rule Summary http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf Page 5
8	Summary of HIPAA Privacy Rule page 2-3 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
9	HEALTH AND SAFETY CODE TITLE 2. HEALTH SUBTITLE I. MEDICAL RECORDS CHAPTER 181. MEDICAL RECORDS PRIVACY SUBCHAPTER A. GENERAL PROVISIONS http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm Page 1
10	Summary of HIPAA Privacy Rule page 3 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
11	AMA HIPAA Omnibus Final Rule Summary http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf Page 4
12	TEXAS BUSINESS AND COMMERCE CODE TITLE 11. PERSONAL IDENTITY INFORMATION SUBTITLE B. IDENTITY THEFT CHAPTER 521. UNAUTHORIZED USE OF IDENTIFYING INFORMATION http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm
13	*Complying with the new HIPAA Omnibus Rule: Part Two* Compliance Today; June 2013 pgs. 31-38
14	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf and https://federalregister.gov/a/2013-01073 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

15	Summary of HIPAA Privacy Rule page 1 http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
16	Texas Senate Bill 1609 (2013) http://legiscan.com/TX/bill/SB1609
17	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
18	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
19	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
20	HEALTH AND SAFETY CODE TITLE 2. HEALTH SUBTITLE I. MEDICAL RECORDS CHAPTER 181. MEDICAL RECORDS PRIVACY SUBCHAPTER A. GENERAL PROVISIONS http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm
21	HEALTH AND SAFETY CODE TITLE 2. HEALTH SUBTITLE I. MEDICAL RECORDS CHAPTER 181. MEDICAL RECORDS PRIVACY SUBCHAPTER A. GENERAL PROVISIONS http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm
22	AMA HIPAA Omnibus Final Rule Summary http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf
23	AMA HIPAA Omnibus Final Rule Summary http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf
24	*Complying with the new HIPAA Omnibus Rule: Part 1* Compliance Today May 2013 Pages 36-42
25	Texas OCCUPATIONS CODE TITLE 3. HEALTH PROFESSIONS SUBTITLE B. PHYSICIANS CHAPTER 159. PHYSICIAN-PATIENT COMMUNICATION http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.159.htm
26	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
27	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
28	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
29	Omnibus Rule https://s3.amazonaws.com/public-inspection.feder47register.gov/2013-01073.pdf page 227
30	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
31	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
32	Texas Medical Board Rules Chapter 165 http://www.tmb.state.tx.us/rules/rules/bdrules.php
33	Summary of HIPAA Privacy Rule www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
34	Omnibus Rule https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf

35	Summary of the HIPAA Privacy Rule www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
36	Texas Medical Board Rules Chapter 165 http://www.tmb.state.tx.us/rules/rules/bdrules.php
37	Summary of HIPAA Privacy Rule http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
38	University of Texas Dallas Human Resources -HIPAA Manual http://www.utdallas.edu/hrm/fac-staff/hippa3persreps.php5
39	Summary of HIPAA Privacy Rule www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
40	*HIPAA Security Series – 1: Security 101 for Covered Entities* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf
41	Addendum to the Security Matrix http://aspe.hhs.gov/admnsimp/nprm/sec14.htm
42	*HIPAA Security Series – 7: Security Standards: Implementation for the Small Provider* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/smallprovider.pdf
43	*HIPAA Security Series - #6 Basics of Risk Analysis and Risk Management* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf Accessed 11/19/2012
44	*HIPAA Security Series - #6 Basics of Risk Analysis and Risk Management* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf Accessed 11/19/2012
45	Risk Management Guide for Information Technology Systems by the National Institute of Standards and Technology http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf
46	Breach Notification Rule http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/
47	AMA HIPAA Omnibus Final Rule Summary http://www.ama-assn.org/resources/doc/washington/hipaa-omnibus-final-rule-summary.pdf
48	HIPAA SECURITY SERIES: TECHNICAL SAFEGUARDS http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
49	HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf
50	HIPAA SECURITY SERIES: TECHNICAL SAFEGUARDS http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
51	HIPAA encryption: Meeting Today's Regulations http://www.scmagazine.com/hipaa-encryption-meeting-todays-regulations/article/173661/
52	HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf
53	NIST's Guide to Storage Encryption Technologies for End User Devices http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf
54	HIPAA Security Rule: Frequently asked questions regarding encryption of personal health information http://www.ama-assn.org/resources/doc/psa/hipaa-phi-encryption.pdf
55	HIPAA Security Guidance, Remote Use http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf
56	Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules page 276 https://s3.amazonaws.com/public-inspection.federalregister.gov/2013-01073.pdf
57	*Mobile Devices and Texting* Compliance Today, July 2013 page 32
58	HIPAA Security Guidance, Remote Use http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf

59	HIPAA Security Guidance, Remote Use http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse.pdf
60	Healthcare IT News 12 steps for surviving a privacy breach investigation www.healcareitnews.com/print/28001 accessed 10/25/2011
61	FACT SHEET Texas House Bill 300 November 7, 2011 http://himss.files.cms-plus.com/HIMSSorg/policy/d/HIMSSFactSheetTXHB300.pdf
62	FACT SHEET Texas House Bill 300 November 7, 2011 http://himss.files.cms-plus.com/HIMSSorg/policy/d/HIMSSFactSheetTXHB300.pdf
63	BUSINESS AND COMMERCE CODE TITLE 11. PERSONAL IDENTITY INFORMATION SUBTITLE B. IDENTITY THEFT CHAPTER 521. UNAUTHORIZED USE OF IDENTIFYING INFORMATION http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm

Appendices

Appendix	
A	TMA Survey of Texas Physicians Electronic Health Records 2012 Report
B	Business Associate Agreement Record
C	Sample Business Associate Agreement
D	Notice of Privacy Practices
E	Notice of Privacy Practices Acknowledgment
F	Texas Attorney General's Authorization to Disclose PHI
G	HIPAA Security Matrix

The forms, checklists, guidelines, and materials included herein are for generalized information only and should not be reviewed or referred to as primary legal sources nor construed as establishing medical standards of care for purposes of litigation including expert testimony. They are intended as resources to be selectively used and always adapted – with the advice of the attorney for the individual or organization – to meet the needs or requirements of a particular practice. They are distributed with the understanding that TMLT and its affiliates are not is engaged in rendering legal services.

Appendix A

TMA Survey of Texas Physicians Electronic Health Records 2012 Report



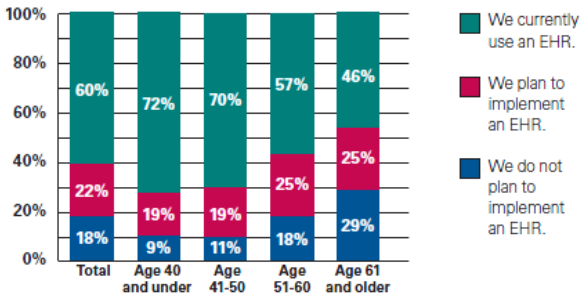
Texas Medical Association
Health Information Technology
Practice Management Services

TMA Survey of Texas Physicians
Electronic Health Records
2012 Report (Preliminary Research Findings)

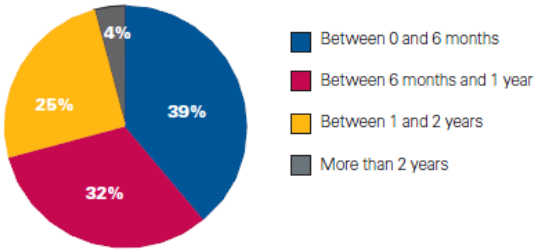
Background
Health information technology (HIT) such as electronic health records (EHRs), e-prescribing, and health information exchanges has the potential to improve quality of care, patient safety, and practice viability. TMA's goal is to help ensure HIT has a positive impact on physicians, patients, and practices. TMA has surveyed physicians on office technology use since 2005 and has noticed an upward trend since that time. Based on survey findings, TMA tailors services and resources to help physicians appropriately implement and utilize office technologies.

EHR Implementation Hits 60 Percent in Texas
The percentage of respondents who currently use an EHR continues to rise (60 percent, up from 43 percent in 2009). Of the 18 percent of respondents with no plans to implement an EHR, 67 percent report prohibitive cost as the reason. Another reason physicians list for not planning to implement an EHR is having no decisionmaking authority in their practice. Not surprisingly, older physicians are more likely to report nearing retirement as a reason for not planning to implement an EHR.

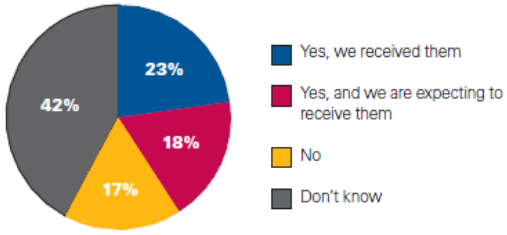
EHR Status by Physician Age



Plans to Implement an EHR
Among physicians who want to implement an EHR, the majority plan to do so in the next year (72 percent).

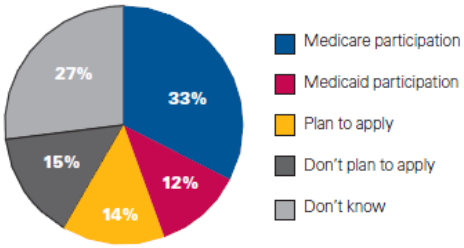


Qualified for EHR Incentive Payments
Forty-one percent of physicians report they qualified for stimulus incentives and either received them already or are expecting them. A large minority of physicians don't know if their practice qualified for the stimulus incentives (42 percent). This is most likely because these physicians are not involved in practice management decisions.



T7301.7.2012.SUMMARY

EHR Incentive Payments From Medicare or Medicaid
Physicians currently using an EHR were asked if their practice applied for Health Information Technology for Economic and Clinical Health (HITECH) incentive payments. Some 33 percent applied for funds from Medicare (up to $44,000), and 12 percent applied for incentives from Medicaid (up to $63,750).



Summary
The current survey is a benchmark of physician needs and experiences with EHRs. This survey is a follow-up to surveys conducted in 2009, 2007, and 2005. In April 2012, TMA emailed a survey to 33,808 physicians and residents. By the end of the month, TMA had received responses from 1,733 physicians, for a rate of 5 percent. For a complete report, contact TMA at (800) 880-5720 or go to www.texmed.org/HIT.

Source: TMA www.texmed.org

Appendix B

Sample Business Associate & Agreement List



Record of Business Associates of _____					
Name of Business Associate	**Address of Business Associate**	**Service Provided**	**Original Business Associate Agreement (BAA) Date Signed**	**BAA Update Date** **Date signed**	**BAA Update Date** **Date signed**

Appendix C

Sample Business Associate Agreement



TMLT Business Associate Agreement Information and Sample Agreement form

Introduction:

With the changes to HIPAA Privacy and Security from the Omnibus Rule, it is more important than ever for covered entities to identity their Business Associates and have a current BAA in place with them.

The following information and sample Business Associate Agreement (BAA) is developed primarily from the SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS
published January 25, 2013, by Health and Human Services on their website. Pages 1-4 are general information and the sample begins on page 5.

DISCLAIMER

The information presented in this document should be used as a resource and adapted with the advice of your attorney. It is distributed with the understanding that TMLT and its affiliates are not engaged in rendering legal services.

This document is intended merely as an aid to assist physicians and their office staff in understanding their obligations and developing their own business associate agreement, as covered entities under the provisions federal and Texas medical privacy and security rules. TMLT makes no representation that compliance with the provisions set forth in this tool will constitute full compliance with the various federal and state privacy and security laws.

Deadline to Update or Create Business Associate Agreements

Covered entities have been required to have agreements with their Business Associates by the original HIPAA Privacy (effective 2003) and Security Rules (2005). You may have current business associate agreements in place with your Business Associates.

Generally speaking, the Omnibus rule gives covered entities until ***September 23, 2014***, to bring all their BA agreements into conformance with the new rules. **However,** this applies only if the Covered Entity's BAA have not been renewed or modified between March 26, 2013, and September 23, 2013. Therefore, BAA existing prior to September 23, 2013 (but not renewed or modified between March 26, 2013 and September 23, 2013) will be deemed compliant until the date the BA agreement is renewed or modified or until September 22, 2014, whichever is earlier.

Why execute an updated BAA?

Under the Omnibus rule, business associates are now directly responsible for HIPAA criminal and civil liabilities.

BAs are now directly responsible for:

- Limiting use and disclosures of PHI to those permitted under the BAA
- Designating personnel responsible for security compliance if they have ePHI
- Performing a risk analysis if they have ePHI
- Establishing polices that incorporate technical and administrative safeguards for PHI (in whatever form)
- Investing in hardware and software to prevent and monitor internal and external breaches of ePHI
- Notifying the CE of breaches of unsecured PHI (set a time frame)

- Executing written assurances with subcontractors that pass on these same responsibilities
- Providing information in response to request for copy of PHI (to the individual or the CE as specified in the BAA)
- Keeping records and cooperating with OCR investigations and compliance reviews[1]

The following is quote from the HHS website:

> A "business associate" is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A "business associate" also is a subcontractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate may use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.
>
> A written contract between a covered entity and a business associate must:
>
> (1) establish the permitted and required uses and disclosures of protected health information by the business associate;
> (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law;
> (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information;
> (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information;
> (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings;
> (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation;
> (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule;

(8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity;
(9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and
(10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

This document includes a sample business associate agreement provisions to help covered entities and business associates more easily comply with the business associate contract requirements. While these sample provisions are written for the purposes of the contract between a covered entity and its business associate, the language may be adapted for purposes of the contract between a business associate and subcontractor.

This is only sample language and use of these sample provisions is not required for compliance with the HIPAA Rules. The language may be changed to more accurately reflect business arrangements between a covered entity and business associate or business associate and subcontractor. In addition, these or similar provisions may be incorporated into an agreement for the provision of services between a covered entity and business associate or business associate and subcontractor, or they may be incorporated into a separate business associate agreement. These provisions address only concepts and requirements set forth in the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, and alone may not be sufficient to result in a binding contract under State law. They do not include many formalities and substantive provisions that may be required or typically included in a valid contract. Reliance on this sample may not be sufficient for compliance with State law, and does not replace consultation with a lawyer or negotiations between the parties to the contract.[2]

Footnotes

[1] Compliance Today June 2013, Vol. 15 Issue 6, Complying with the new HIPAA Omnibus Rule Part 2; page 32
[2] HHS Sample BAA http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Sample Business Associate Agreement Provisions

Source http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

Note: Words or phrases contained in brackets are intended as either optional language or as instructions to the users of these sample provisions.

This Agreement ("Agreement") is made and entered into this ___ day of [Month], [Year] by and between [Business Name] ("Covered Entity"), [Type of Entity], whose business address is [Address of Covered Entity], and [Business Name] ("Business Associate"), [Type of Entity], whose business address is [Address of Business Associate].

Definitions

Catch-all definition: 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, Health Care 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 [Insert Name of 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 [Insert 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.

(d) **Individual**. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

(e) **Protected Health Information**. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(f) **Sensitive Personal Information (SPI).** Texas Business and Commerce, Chapter 521, Unauthorized use of Identifying Information defines SPI more broadly than HIPAA Protected Health Information; an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:

- social security number;
- driver's license number or government-issued identification number; or

- account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or information that identifies an individual and relates to:

    - the physical or mental health or condition of the individual;
    - the provision of health care to the individual; or
    - payment for the provision of health care to the individual

Obligations and Activities of Business Associate

Business Associate 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 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 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 parties may wish to add additional specificity regarding the breach notification obligations of the business associate, such as a stricter timeframe for the business associate to report a potential breach to the covered entity and/or whether 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.]

(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 protected health information in a designated record set to the [Choose either “covered entity” or “individual or the individual’s designee”] as necessary to satisfy covered entity’s obligations under 45 CFR 164.524;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for access that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to provide the requested access or whether the business associate will forward the individual’s request to the covered entity to fulfill) and the timeframe for the business associate to provide the information to the covered entity.]

(f) Make any amendment(s) to 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;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for amendment that the business associate receives directly from the individual (such as whether and in what time and manner a business associate is to act on the request for amendment or whether the business associate will forward the individual's request to the covered entity) and the timeframe for the business associate to incorporate any amendments to the information in the designated record set.]

(g) Maintain and make available the information required to provide an accounting of disclosures to the [Choose either "covered entity" or "individual"] as necessary to satisfy covered entity's obligations under 45 CFR 164.528;

[The parties may wish to add additional specificity regarding how the business associate will respond to a request for an accounting of disclosures that the business associate receives directly from the individual (such as whether and in what time and manner the business associate is to provide the accounting of disclosures to the individual or whether the business associate will forward the request to the covered entity) and the timeframe for the business associate to provide information to the covered entity.]

(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) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

Permitted Uses and Disclosures by Business Associate

(a) Business associate may only use or disclose protected health information

[Option 1 – Provide a specific list of permissible purposes.]

[Option 2 – Reference an underlying service agreement, such as "as necessary to perform the services set forth in Service Agreement."]

[In addition to other permissible purposes, the parties should specify whether the business associate is authorized to use protected health information to de-identify the information in accordance with 45 CFR 164.514(a)-(c). The parties also may wish to specify the manner in which the business associate will de-identify the information and the permitted uses and disclosures by the business associate of the de-identified information.]

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

(c) Business associate agrees to make uses and disclosures and requests for protected health information

[Option 1] consistent with covered entity's minimum necessary policies and procedures.

[Option 2] subject to the following minimum necessary requirements: [Include specific minimum necessary provisions that are consistent with the covered entity's minimum necessary policies and procedures.]

(d) Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by covered entity [if the Agreement permits the business associate to use or disclose protected health information for its own management and administration and legal responsibilities or for data aggregation services as set forth in optional provisions (e), (f), or (g) below, then add ", except for the specific uses and disclosures set forth below."]

(e) [Optional] Business associate may use protected health information for the proper management and administration of the business associate or to carry out the legal responsibilities of the business associate.

(f) [Optional] Business associate may disclose protected health information for the proper management and administration of business associate or to carry out the legal responsibilities of the business associate, provided the disclosures are required by law, or business associate obtains reasonable assurances from the person to whom the information is disclosed 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 to the person, and the person notifies business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(g) [Optional] Business associate may provide data aggregation services relating to the health care operations of the covered entity.

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

(a) [Optional] Covered entity shall 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 protected health information.

(b) [Optional] 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 protected health information, to the extent that such changes may affect business associate's use or disclosure of protected health information.

(c) [Optional] 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 protected health information.

Permissible Requests by Covered Entity

[Optional] 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. [Include an exception if the business associate will use or disclose protected health information for, and the

agreement includes provisions for, data aggregation or management and administration and legal responsibilities of the business associate.]

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of [Insert effective date], and shall terminate on [Insert termination date or event] or on the date covered entity terminates for cause as authorized in paragraph (b) of this Section, whichever is sooner.

(b) 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]. [Bracketed language may be added if the covered entity wishes to provide the business associate with an opportunity to cure a violation or breach of the contract before termination for cause.]

(c) Obligations of Business Associate Upon Termination.

[Option 1 – if the business associate is to return or destroy all protected health information upon termination of the agreement]

Upon termination of this Agreement for any reason, business associate shall return to covered entity [or, if agreed to by covered entity, destroy] all protected health information received from covered entity, or created, maintained, or received by business associate on behalf of covered entity, that the business associate still maintains in any form. Business associate shall retain no copies of the protected health information.

[Option 2—if the agreement authorizes the business associate to use or disclose protected health information for its own management and administration or to carry out its legal responsibilities and the business associate needs to retain protected health information for such purposes after termination of the agreement]

Upon termination of this Agreement for any reason, business associate, with respect to 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 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, if agreed to by covered entity, destroy] the remaining 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 electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as business associate retains the protected health information;
4. Not use or disclose the protected health information retained by business associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out at [Insert section number related to paragraphs (e) and (f) above under "Permitted Uses and Disclosures By Business Associate"] which applied prior to termination; and

5. Return to covered entity [or, if agreed to by covered entity, destroy] the 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 agreement also could provide that the business associate will transmit the protected health information to another business associate of the covered entity at termination, and/or could add terms regarding a business associate's obligations to obtain or ensure the destruction of protected health information created, received, or maintained by subcontractors.]

(d) Survival. The obligations of business associate under this Section shall survive the termination of this Agreement.

Miscellaneous [Optional]

(a) [Optional] Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended.

(b) [Optional] 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.

(c) [Optional] Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

APPROVED AND ACCEPTED BY:

_____ _____

Business Associate Date

Title

_____ _____

Covered Entity Date

Title

Appendix D

Sample Notice of Privacy Practices



Sample

Name of the Covered Entity

HIPAA Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED BY OUR PRACTICE AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

THIS NOTICE IS A REVISION AND BECAME EFFECTIVE [DATE EFFECTIVE]

If you have any questions about this notice, please contact _____.

PROVIDER/CLINIC OBLIGATIONS:

We are required by law to:

- Maintain the privacy of protected health information
- Give you this notice of our legal duties and privacy practices regarding health information about you
- Follow the terms of our notice that is currently in effect
- In Texas, Inform you that we disclose your PHI electronically
- In Texas [Describe how the practice uses electronic media to communicate with patients if applicable]
- In Texas we will not email patients without written consent
- Notify you of a breach of protected information as required by federal and state law

PROTECTED HEALTH INFORMATION:

Protected health information is defined by HIPAA as individually identifiable health information; it can be verbal, written or electronic.

HOW WE MAY USE AND DISCLOSE HEALTH INFORMATION:

The following describes the ways we may use and disclose health information that identifies you ("Health Information"). Except for the purposes described below, we will use and disclose Health Information only with your written permission. You may revoke such permission at any time by writing to our practice Privacy Officer.

For Treatment. We may use and disclose Health Information for your treatment and to provide you with treatment-related health care services. For example, we may disclose Health Information to doctors, nurses, technicians, or other personnel, including people outside our office, who are involved in your medical care and need the information to provide you with medical care.

For Payment. We may use and disclose Health Information so that we or others may bill and receive payment from you, an insurance company or a third party for the treatment and services you received. For example, we may give your health plan information about you so that they will pay for your treatment.

For Health Care Operations. We may use and disclose Health Information for health care operations purposes. These uses and disclosures are necessary to make sure that all of our patients receive quality care and to operate and manage our office. For example, we may use and disclose information to make sure the care you receive is of the highest quality. We also may share information with other entities that have a relationship with you (for example, your health plan) for their health care operation activities.

Appointment Reminders, Treatment Alternatives and Health Related Benefits and Services. We may use and disclose Health Information to contact you to remind you that you have an appointment with us. We also may use and disclose Health Information to tell you about treatment alternatives or health-related benefits and services that may be of interest to you.

Individuals Involved in Your Care or Payment for Your Care. When appropriate, we may share Health Information with a person who is involved in your medical care or payment for your care, such as your family or a close friend. We also may notify your family about your location or general condition or disclose such information to an entity assisting in a disaster relief effort.

Research. Under certain circumstances, we may use and disclose Health Information for research. For example, a research project may involve comparing the health of patients who received one treatment to those who received another, for the same condition. Before we use or disclose Health Information for research, the project will go through a special approval process. Even without special approval, we may permit researchers to look at records to help them identify patients who may be included in their research project or for other similar purposes, as long as they do not remove or take a copy of any Health Information.

SPECIAL SITUATIONS:

As Required by Law. We will disclose Health Information when required to do so by international, federal, state or local law.

To Avert a Serious Threat to Health or Safety. We may use and disclose Health Information when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person. Disclosures, however, will be made only to someone who may be able to help prevent the threat.

Business Associates. We may disclose Health Information to our business associates that perform functions on our behalf or provide us with services if the information is necessary for such functions or services. For example, we may use another company to perform billing services on our behalf. All of our business associates are obligated to protect the privacy of your information and are not allowed to use or disclose any information other than as specified in our contract.

Organ and Tissue Donation. If you are an organ donor, we may use or release Health Information to organizations that handle organ procurement or other entities engaged in procurement, banking or transportation of organs, eyes or tissues to facilitate organ, eye or tissue donation and transplantation.

Military and Veterans. If you are a member of the armed forces, we may release Health Information as required by military command authorities. We also may release Health Information to the appropriate foreign military authority if you are a member of a foreign military.

Workers' Compensation. We may release Health Information for workers' compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Public Health Risks. We may disclose Health Information for public health activities. These activities generally include disclosures to prevent or control disease, injury or disability; report births and deaths; report child abuse or neglect; report reactions to medications or problems with products; notify people of recalls of products they may be using; a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition; and the appropriate government authority if we believe a patient has been the victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Health Oversight Activities. We may disclose Health Information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.

Data Breach Notification Purposes. We may use or disclose your Protected Health Information to provide legally required notices of unauthorized access to or disclosure of your health information.

Lawsuits and Disputes. If you are involved in a lawsuit or a dispute, we may disclose Health Information in response to a court or administrative order. We also may disclose Health Information in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

Law Enforcement. We may release Health Information if asked by a law enforcement official if the information is: (1) in response to a court order, subpoena, warrant, summons or similar process; (2) limited information to identify or locate a suspect, fugitive, material witness, or missing person; (3) about the victim of a crime even if, under certain very limited circumstances, we are unable to obtain the person's agreement; (4) about a death we believe may be the result of criminal conduct; (5) about criminal conduct on our premises; and (6) in an emergency to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.

Coroners, Medical Examiners and Funeral Directors. We may release Health Information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We also may release Health Information to funeral directors as necessary for their duties.

National Security and Intelligence Activities. We may release Health Information to authorized federal officials for intelligence, counter-intelligence, and other national security activities authorized by law.

Protective Services for the President and Others. We may disclose Health Information to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or to conduct special investigations.

Inmates or Individuals in Custody. If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release Health Information to the correctional institution or law enforcement official. This release would be if necessary: (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) the safety and security of the correctional institution.

USES AND DISCLOSURES THAT REQUIRE US TO GIVE YOU AN OPPORTUNITY TO OBJECT AND OPT

Individuals Involved in Your Care or Payment for Your Care. Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, your Protected Health Information that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment.

Disaster Relief. We may disclose your Protected Health Information to disaster relief organizations that seek your Protected Health Information to coordinate your care, or notify family and friends of your location or

condition in a disaster. We will provide you with an opportunity to agree or object to such a disclosure whenever we practically can do so.

YOUR WRITTEN AUTHORIZATION IS REQUIRED FOR OTHER USES AND DISCLOSURES

The following uses and disclosures of your Protected Health Information will be made only with your written authorization:

1. Uses and disclosures of Protected Health Information for marketing purposes; and

2. Disclosures that constitute a sale of your Protected Health Information

Other uses and disclosures of Protected Health Information not covered by this Notice or the laws that apply to us will be made only with your written authorization. If you do give us an authorization, you may revoke it at any time by submitting a written revocation to our Privacy Officer and we will no longer disclose Protected Health Information under the authorization. But disclosure that we made in reliance on your authorization before you revoked it will not be affected by the revocation.

YOUR RIGHTS:

You have the following rights regarding Health Information we have about you:

Right to Inspect and Copy. You have a right to inspect and obtain a copy Health Information that may be used to make decisions about your care or payment for your care. This includes medical and billing records, other than psychotherapy notes. To inspect and copy this Health Information, you must make your request, in writing, to _____. In Texas, we have up to 15 days to make your Protected Health Information available to you and we may charge you a reasonable fee for the costs of copying, mailing or other supplies associated with your request. We may not charge you a fee if you need the information for a claim for benefits under the Social Security Act or any other state of federal needs-based benefit program. We may deny your request in certain limited circumstances. If we do deny your request, you have the right to have the denial reviewed by a licensed healthcare professional who was not directly involved in the denial of your request, and we will comply with the outcome of the review.

Right to an Electronic Copy of Electronic Medical Records. If your Protected Health Information is maintained in an electronic format (known as an electronic medical record or an electronic health record), you have the right to request that an electronic copy of your record be given to you or transmitted to another individual or entity. We will make every effort to provide access to your Protected Health Information in the form or format you request, if it is readily producible in such form or format. If the Protected Health Information is not readily producible in the form or format you request your record will be provided in either our standard electronic format or if you do not want this form or format, a readable hard copy form. We may charge you a reasonable, cost-based fee for the labor associated with transmitting the electronic medical record.

Right to Get Notice of a Breach. You have the right to be notified upon a breach of any of your unsecured Protected Health Information.

Right to Amend. If you feel that Health Information we have is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for our office. To request an amendment, you must make your request, in writing, to _____.

Right to an Accounting of Disclosures. You have the right to request a list of certain disclosures we made of Health Information for purposes other than treatment, payment and health care operations or for which you

provided written authorization. To request an accounting of disclosures, you must make your request, in writing, to _____.

Right to Request Restrictions. You have the right to request a restriction or limitation on the Health Information we use or disclose for treatment, payment, or health care operations. You also have the right to request a limit on the Health Information we disclose to someone involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not share information about a particular diagnosis or treatment with your spouse. To request a restriction, you must make your request, in writing, to _____. We are not required to agree to your request unless you are asking us to restrict the use and disclosure of your Protected Health Information to a health plan for payment or health care operation purposes and such information you wish to restrict pertains solely to a health care item or service for which you have paid us "out-of-pocket" in full. If we agree, we will comply with your request unless the information is needed to provide you with emergency treatment.

Out-of-Pocket-Payments. If you paid out-of-pocket (or in other words, you have requested that we not bill your health plan) in full for a specific item or service, you have the right to ask that your Protected Health Information with respect to that item or service not be disclosed to a health plan for purposes of payment or health care operations, and we will honor that request.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you by mail or at work. To request confidential communications, you must make your request, in writing, to _____. Your request must specify how or where you wish to be contacted. We will accommodate reasonable requests.

Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. You may obtain a copy of this notice at our web site, www._____. To obtain a paper copy of this notice, _____.

CHANGES TO THIS NOTICE:

We reserve the right to change this notice and make the new notice apply to Health Information we already have as well as any information we receive in the future. We will post a copy of our current notice at our office. The notice will contain the effective date on the first page of the notice.

COMPLAINTS:

If you believe your privacy rights have been violated, you may file a complaint with our office or with the Secretary of the Department of Health and Human Services. To file a complaint with our office, contact _____. All complaints must be made in writing. **You will not be penalized for filing a complaint**.

Appendix E

Sample Notice of Privacy Practices Acknowledgment



ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

FOR XXX CLINIC

Patient Name: _____

Date of Birth: _____

Social Security Number: _____

I acknowledge that XXX provided me with a written copy of his/her Notice of Privacy Practices.

I also acknowledge that I have been afforded the opportunity to read the Notice of Privacy Practices and ask questions.

_____ _____

Patient Signature Date

_____ _____

Personal Representative Signature (if applicable) Relationship to Patient

Appendix F

The Texas Attorney General's "Authorization to Disclose PHI"



This is a suggested form, CEs in Texas are not required to use this exact form, but they are required to use a form that meets this standard.

The form may be printed from the Texas Attorney General's Website:

https://www.oag.state.tx.us/AG_Publications/pdfs/hb300_auth_form.pdf

AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective January 1, 2013

Please read this entire form before signing and complete all the sections that apply to your decisions relating to the disclosure of protected health information. Covered entities as that term is defined by HIPAA and Texas Health & Safety Code § 181.001 must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing an insurance or health maintenance organization function, or as may be otherwise authorized by law. **Covered entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws.** Individuals cannot be denied treatment based on a failure to sign this authorization form, and a refusal to sign this form will not affect the payment, enrollment, or eligibility for benefits.

NAME OF PATIENT OR INDIVIDUAL

_____
Last First Middle

OTHER NAME(S) USED _____

DATE OF BIRTH Month _____ Day _____ Year _____

ADDRESS _____

_____

CITY _____ **STATE** _____ **ZIP** _____

PHONE (_____) _____ **ALT. PHONE** (_____) _____

EMAIL ADDRESS (Optional): _____

I AUTHORIZE THE FOLLOWING TO DISCLOSE THE INDIVIDUAL'S PROTECTED HEALTH INFORMATION:

Person/Organization Name _____
Address _____
City _____ State _____ Zip Code _____
Phone (_____) _____ Fax (_____) _____

WHO CAN RECEIVE AND USE THE HEALTH INFORMATION?

Person/Organization Name _____
Address _____
City _____ State _____ Zip Code _____
Phone (_____) _____ Fax (_____) _____

REASON FOR DISCLOSURE
(Choose only one option below)

- ☐ Treatment/Continuing Medical Care
- ☐ Personal Use
- ☐ Billing or Claims
- ☐ Insurance
- ☐ Legal Purposes
- ☐ Disability Determination
- ☐ School
- ☐ Employment
- ☐ Other _____

WHAT INFORMATION CAN BE DISCLOSED? Complete the following by indicating those items that you want disclosed. The signature of a minor patient is required for the release of some of these items. If all health information is to be released, then check only the first box.

- ☐ **All health information**
- ☐ Physician's Orders
- ☐ Progress Notes
- ☐ Pathology Reports
- ☐ History/Physical Exam
- ☐ Patient Allergies
- ☐ Discharge Summary
- ☐ Billing Information
- ☐ Past/Present Medications
- ☐ Operation Reports
- ☐ Diagnostic Test Reports
- ☐ Radiology Reports & Images
- ☐ Lab Results
- ☐ Consultation Reports
- ☐ EKG/Cardiology Reports
- ☐ Other_____

Your initials are required to release the following information:

_____Mental Health Records (excluding psychotherapy notes)
_____Drug, Alcohol, or Substance Abuse Records
_____Genetic Information (including Genetic Test Results)
_____ HIV/AIDS Test Results/Treatment

EFFECTIVE TIME PERIOD. This authorization is valid until the earlier of the occurrence of the death of the individual; the individual reaching the age of majority; or permission is withdrawn; or the following specific date (optional): Month _____ Day _____ Year _____

RIGHT TO REVOKE: I understand that I can withdraw my permission at any time by giving written notice stating my intent to revoke this authorization to the person or organization named under "WHO CAN RECEIVE AND USE THE HEALTH INFORMATION." I understand that prior actions taken in reliance on this authorization by entities that had permission to access my health information will not be affected.

SIGNATURE AUTHORIZATION: I have read this form and agree to the uses and disclosures of the information as described. I understand that refusing to sign this form does not stop disclosure of health information that has occurred prior to revocation or that is otherwise permitted by law without my specific authorization or permission, including disclosures to other covered entities as provided by Texas Health & Safety Code § 181.154(c) and/or 45 C.F.R. § 164.506(a)(1). I understand that information disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and may no longer be protected by federal or state privacy laws.

SIGNATURE X_____ _____
Signature of Individual or Individual's Legally Authorized Representative **DATE**

Printed Name of Legally Authorized Representative (if applicable): _____
If representative, specify relationship to the individual: ☐ Parent of minor ☐ Guardian ☐ Other _____

A minor individual's signature is required for the release of certain types of information, including for example, the release of information related to certain types of reproductive care, sexually transmitted diseases, and drug, alcohol or substance abuse, and mental health treatment (See, e.g., Tex. Fam. Code § 32.003).

SIGNATURE X_____ _____
Signature of Minor Individual **DATE**

IMPORTANT INFORMATION ABOUT THE AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Developed for Texas Health & Safety Code § 181.154(d)
effective January 1, 2013

The Attorney General of Texas has adopted a standard Authorization to Disclose Protected Health Information in accordance with Texas Health & Safety Code § 181.154(d). This form is intended for use in complying with the requirements of the Health Insurance Portability and Accountability Act and Privacy Standards (HIPAA) and the Texas Medical Privacy Act (Texas Health & Safety Code, Chapter 181). **Covered Entities may use this form or any other form that complies with HIPAA, the Texas Medical Privacy Act, and other applicable laws.**

Covered entities, as that term is defined by HIPAA and Texas Health & Safety Code § 181.001, must obtain a signed authorization from the individual or the individual's legally authorized representative to electronically disclose that individual's protected health information. Authorization is not required for disclosures related to treatment, payment, health care operations, performing an insurance or health maintenance organization function, or as may be otherwise authorized by law. (Tex. Health & Safety Code §§ 181.154(b),(c), § 241.153; 45 C.F.R. §§ 164.502(a)(1); 164.506, and 164.508).

The authorization provided by use of the form means that the organization, entity or person authorized can disclose, communicate, or send the named individual's protected health information to the organization, entity or person identified on the form, including through the use of any electronic means.

Definitions - In the form, the terms "treatment," "healthcare operations," "psychotherapy notes," and "protected health information" are as defined in HIPAA (45 CFR 164.501). "Legally authorized representative" as used in the form includes any person authorized to act on behalf of another individual. (Tex. Occ. Code § 151.002(6); Tex. Health & Safety Code §§ 166.164, 241.151; and Tex. Probate Code § 3(aa)).

Health Information to be Released - If "All Health Information" is selected for release, health information includes, but is not limited to, all records and other information regarding health history, treatment, hospitalization, tests, and outpatient care, and also educational records that may contain health information. As indicated on the form, specific authorization is required for the release of information about certain sensitive conditions, including:

- Mental health records (excluding "psychotherapy notes" as defined in HIPAA at 45 CFR 164.501).
- Drug, alcohol, or substance abuse records.
- Records or tests relating to HIV/AIDS.
- Genetic (inherited) diseases or tests.

Note on Release of Health Records - This form is not required for the permissible disclosure of an individual's protected health information to the individual or the individual's legally authorized representative. (45 C.F.R. §§ 164.502(a)(1)(i), 164.524; Tex. Health & Safety Code § 181.102). If requesting a copy of the individual's health records with this form, state and federal law allows such access, unless such access is determined by the physician or mental health provider to be harmful to the individual's physical, mental or emotional health. (Tex. Health & Safety Code §§ 181.102, 611.0045(b); Tex. Occ. Code § 159.006(a); 45 C.F.R. § 164.502(a)(1)). If a healthcare provider is specified in the "Who Can Receive and Use The Health Information" section of this form, then permission to receive protected health information also includes physicians, other health care providers (such as nurses and medical staff) who are involved in the individual's medical care at that entity's facility or that person's office, and health care providers who are covering or on call for the specified person or organization, and staff members or agents (such as business associates or qualified services organizations) who carry out activities and purposes permitted by law for that specified covered entity or person. If a covered entity other than a healthcare provider is specified, then permission to receive protected health information also includes that organization's staff or agents and subcontractors who carry out activities and purposes permitted by this form for that organization.

Authorizations for Marketing Purposes - If this authorization is being provided or obtained for marketing purposes and the covered entity will receive direct or indirect remuneration from a third party in connection with the use or disclosure of the individual's information for marketing, the authorization must also clearly indicate to the individual that such remuneration is involved. (Tex. Health & Safety Code § 181.152; 45 C.F.R § 164.508(a)(3)).

Limitations of this form - This authorization form should not be used for: (1) the disclosure of any health information as it relates to health benefits plan enrollment and/or related enrollment determinations (45 CFR §§164.508(b)(4)(ii), .508(c)(2)(ii)); or (2) the use or disclosure of psychotherapy notes (45 C.F.R. § 164.508(b)(3)). **Use of this form does not exempt any entity from compliance with applicable federal or state laws or regulations regarding access, use or disclosure of health information or other sensitive personal information (e.g., 42 CFR Part 2, restricting use of information pertaining to drug/alcohol abuse and treatment), and does not entitle an entity or its employees, agents or assigns to any limitation of liability for acts or omissions in connection with the access, use, or disclosure of health information obtained through use of the form.**

Charges - Some covered entities may charge a retrieval/processing fee and for copies of medical records. (Tex. Health & Safety Code § 241.154).

Right to Receive Copy - The individual and/or the individual's legally authorized representative has a right to receive a copy of this authorization.

Appendix G

Security Matrix



ADMINISTRATIVE SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Security Management Process	§ 164.308(a)(1)	Risk Analysis	(R)
		Risk Management	(R)
		Sanction Policy	(R)
		Information System Activity Review	(R)
Assigned Security Responsibility	§ 164.308(a)(2)		
Workforce Security	§ 164.308(a)(3)	Authorization and/or Supervision	(A)
		Workforce Clearance Procedure	(A)
		Termination Procedures	(A)
Information Access Management	§ 164.308(a)(4)	Isolating Health Care Clearinghouse Functions	(R)
		Access Authorization	(A)
		Access Establishment and Modification	(A)
Security Awareness and Training	§ 164.308(a)(5)	Security Reminders	(A)
		Protection from Malicious Software	(A)
		Log-in Monitoring	(A)
		Password Management	(A)
Security Incident Procedures	§ 164.308(a)(6)	Response and Reporting	(R)
Contingency Plan	§ 164.308(a)(7)	Data Backup Plan	(R)
		Disaster Recovery Plan	(R)
		Emergency Mode Operation Plan	(R)
		Testing and Revision Procedures	(A)
		Applications and Data Criticality Analysis	(A)
Evaluation	§ 164.308(a)(8)		
Business Associate Contracts and Other Arrangements	§ 164.308(b)(1)	Written Contract or Other Arrangement	(R)

PHYSICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Facility Access Controls	§ 164.310(a)(1)	Contingency Operations	(A)
		Facility Security Plan	(A)
		Access Control and Validation Procedures	(A)
		Maintenance Records	(A)
Workstation Use	§ 164.310(b)		
Workstation Security	§ 164.310(c)		
Device and Media Controls	§ 164.310(d)(1)	Disposal	(R)
		Media Re-use	(R)
		Accountability	(A)
		Data Backup and Storage	(A)

TECHNICAL SAFEGUARDS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Access Control	§ 164.312(a)(1)	Unique User Identification	(R)
		Emergency Access Procedure	(R)
		Automatic Logoff	(A)
		Encryption and Decryption	(A)
Audit Controls	§ 164.312(b)		
Integrity	§ 164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information	(A)
Person or Entity Authentication	§ 164.312(d)		
Transmission Security	§ 164.312(e)(1)	Integrity Controls	(A)
		Encryption	(A)

ORGANIZATIONAL REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Business associate contracts or other arrangements	§ 164.314(a)(1)	Business Associate Contracts	(R)
		Other Arrangements	(R)
Requirements for Group Health Plans	§ 164.314(b)(1)	Implementation Specifications	(R)

POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS			
Standards	**Sections**	**Implementation Specifications (R)= Required, (A)=Addressable**	
Policies and Procedures	§ 164.316(a)		
Documentation	§ 164.316(b)(1)	Time Limit	(R)
		Availability	(R)
		Updates	(R)

Glossary

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Addressable: The Security Rule classifies all implementation specifications as either addressable or required. The concept of "addressable implementation specifications" was developed to provide covered entities additional flexibility with respect to compliance with the security standards. In meeting standards that contain addressable implementation specifications, a covered entity will do one of the following for each addressable specification: (a) implement the addressable implementation specifications; (b) implement one or more alternative security measures to accomplish the same purpose; (c) not implement either an addressable implementation specification or an alternative. The covered entity's choice must be documented. The covered entity must decide whether a given addressable implementation specification is a reasonable and appropriate security measure to apply within its particular security framework.

Administrative Safeguards: Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. One of the three safeguards required under the HIPAA Security rule.

AES: Advanced Encryption Standard

AHIMA: American Health Information Management Association

AMA: American Medical Association

ARRA: American Recovery and Reinvestment Act of 2009 - allocated more than $25 billion for health information technology investment and incentive payments to assist in the implementation and exchange of health information technology. HITECH is part of the ARRA.

Authentication: The corroboration that a person is the one claimed.

Authorization: Formal permission allowing the release of a patient's health information to others, it may be written or verbal; if verbal, authorization should be documented.

Availability: The property that data or information is accessible and useable upon demand by an authorized person.

Breach: The acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy or Security Rule, which compromises the security or privacy of the protected health information.

BA: Business Associate - A person or entity who (1) on behalf of a covered entity performs or assists in a function or activity involving the Use or Disclosure of Individually Identifiable Health Information, including claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; repricing; and other functions and activities; or (2) provides legal, actuarial, accounting, consulting, Data Aggregation, management, administrative, accreditation or financial services that involves the disclosure of Individually Identifiable Health Information.

BAA: Business Associate Agreement – An agreement or contract between a Covered Entity and a Business Associate.

CE: Covered Entity - Entities to which the HIPAA rules apply and includes Health Plans, Health Care Clearinghouses and Health Care Providers who transmit any health information in electronic form in connection with a Transaction covered by HIPAA laws and regulations.

CLIA: Clinical Laboratory Improvements Amendments of 1988

CMS: Centers for Medicare & Medicaid Services

Confidentiality: The property that data or information is not made available or disclosed to unauthorized persons or processes.

Correctional Institution: Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by, or under contract to, the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Other persons held in lawful custody includes juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial

Cyber liability: Insurance coverage which offers protection for network security and privacy-related exposures.

De-identified Health Information: Health information that is not individually identifiable health information. A Covered Entity may determine that health information is not individually identifiable health information only if: (1) a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines that the risk is very small that the information could be used, alone or in combination with other available information, to identify an individual, and documents the methods and results of the analysis; or (2) the following identifiers of the individual, relatives, employers or household members of the individual are removed:

1. Name;
2. Street address, city, county, precinct, zip code and equivalent geocodes;
3. All elements of dates (except year) for dates directly related to an individual and all ages over 89;
4. Telephone number;
5. Fax number;
6. Electronic mail address;
7. Social Security Number;
8. Medical record numbers;
9. Health plan ID 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 addresses (URLs);
15. Internet IP addresses;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic or code.

Designated Record Set: Medical records and billing records that are used to make decisions about individuals and are maintained by or for a Health Care Provider. It also means the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a Health Plan. The term record means any item, collection, or grouping of information that includes Protected Health Information and is maintained, collected, used, or disseminated by or for a Covered Entity.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

EHR: Electronic Health Records

Electronic Media: Media used for storage of electronic data. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. It also includes transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet (wide-open), extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media.

Certain transmission, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

ePHI: Electronic Protected Health Information - Individually identifiable health information that is transmitted or maintained in electronic media.

Encryption: The use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

Facility: The physical premises and the interior and exterior of a building(s).

Group Health Plan:

1. Has 50 or more participants; or
2. Is administered by an entity other than the employer that established and maintains the plan

Health Care: Care, services, or supplies related to the health of an individual and includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health Care Clearinghouse: A public or private entity, including a billing service, repricing company, community health management information system or community health information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.

2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health Care Operations: Any of the following activities carried out directly by The practice or through an Organized Health Care Arrangement in which The practice participates:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.
3. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance);
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities including, but not limited to:
    a. Management activities relating to implementation of and compliance with the requirements of HIPAA laws and regulations;
    b. Customer service, including the provision of data analyses for policyholders, plan sponsors, or other customers,
    provided that Protected Health Information is not disclosed to such policyholder, plan sponsor, or customer.
    c. Resolution of internal grievances;
    d. Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a Covered Entity or, following completion of the sale or transfer, will become a Covered Entity; and
    e. Creating de-identified health information, fundraising for the benefit of The practice, and marketing for which an individual authorization is not required as described by HIPAA laws and regulations.

Health Care Provider: A provider of medical or health services and any other person or organization that furnishes, bills for, or is paid for health care in the normal course of business (generally, facilities and health care providers as defined for Medicare purposes).

Health Insurance Issuer: An insurance company, insurance service, or insurance organization that is licensed to engage in the business of insurance in a State and is subject to State law that regulates insurance. Such term does not include a Group Health Plan. See related definitions for Group Health Plan and Health Plan.

Health Oversight Agency: An agency or other governmental authority, including employees, agents or contractors of such agency or authority, authorized by law to oversee the health care system (whether public or private) or government programs in which PHI is necessary to determine eligibility or compliance or to enforce civil rights law.

Health Plan: An individual or group plan that provides or pays the cost of medical care and includes the following, singly or in combination:

1. A Group Health Plan, as defined herein
2. A Health Insurance Issuer, as defined herein
3. An HMO, as defined herein
4. Part A or Part B of the Medicare program under Title XVIII
5. The Medicaid program under Title XIX
6. An issuer or a Medicare supplemental policy
7. An issuer or a long-term care policy, excluding a nursing home fixed-indemnity policy
8. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers
9. The health care program for active military personnel under title 10 of the United States Code
10. The veterans' health care program under 38 U.S.C. chapter 17.
11. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)
12. The Indian Health Service program under the Indian Health Care Improvement Act
13. The Federal Employees Health Benefits Program
14. An approved State child health plan under Title XXI providing benefits for child health assistance
15. The Medicare + Choice program under Part C of Title XVIII
16. A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals
17. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care

HHS: U.S. Department of Health & Human Services

HIPAA: Health Insurance Portability and Accountability Act

HIPAA Omnibus Rule: Enhanced patient privacy and security protections and provides individuals new rights to their health information established under HIPAA

HIT: Health Information Technology

HITECH: Health Information Technology for Economic and Clinical Health Act, part of the ARRA

HB 300: House Bill 300 - New privacy law provision passed by the Texas legislature in 2011 adding further safeguards for the Protected Health Information (PHI) and Sensitive Personal Information (SPI) of patients treated by Texas physicians. It included more stringent training requirements than federal law.

Identifiers: Identifiers make up Protected Health Information:

1. Name
2. DOB
3. SSN
4. Address
5. Telephone Number

6. Email Address
7. Fax Number
8. Medical Record Number
9. Health Plan ID
10. Internet IP address
11. Certificate Number
12. Device Identifiers
13. Photograph
14. Biometric Identifiers
15. Web Address (URL)
16. Vehicle Identifier
17. Account Numbers
18. Any other unique identifying number, characteristic or code

Individual: The person who is the subject of Protected Health Information.

Individually Identifiable Health Information: Information that is a subset of health information, including demographic information collected from an individual, and:

1. Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of Health Care to an Individual; or the past, present, or future payment for the provision of Health Care to an Individual; and
    a. Identifies the Individual; or
    b. reasonably could be used to identify the Individual.

Information System: An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Integrity: The property that data or information have not been altered or destroyed in the unauthorized manner.

ITEP: Texas Identity Theft Enforcement & Protection Act - requires businesses to implement and maintain reasonable procedures to protect SPI collected or maintained in the regular course of business from unlawful use or disclosure.

Law Enforcement Official: An officer or employee of any agency or authority of the United States, a State or territory, political subdivision of a State or territory, or Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law or prosecute or otherwise conduct criminal, civil or administrative proceeding arising from an alleged violation of law.

Limited Data Set: The Omnibus Rule removes the exception for limited data sets that do not contain birth dates or ZIP codes. By removing this exception, the Omnibus Rule requires that the impermissible acquisition, access, use, or disclosure of limited data sets, even those that do not contain birth dates or ZIP codes, be subject to a risk assessment to demonstrate that breach notification is not required. Previously under HIPAA, Protected Health Information that excludes the following identifiers of the Individual, or of relatives, employers or household members of the Individual: names, postal address information other than town or city, state and zip code, telephone numbers, fax numbers, electronic mail address, social security number, health plan

beneficiary number, account number, certificate/license number, vehicle identifiers and serial numbers, including license plate numbers, device identifiers and serial numbers, web universal resource locators (URLs), Internet Protocol (IP) address numbers, biometric identifiers, including finger and voice prints and full face photographic images and any comparable images.

Malicious Software: Software, for example, a virus, designed to damage or disrupt a system.

Marketing: To make a communication about a product or service to encourage recipients of the communication to purchase or use the product or service. Communications are not considered marketing when they are:

1. a face-to-face communication made by a Covered Entity to an individual;
2. a promotional gift of nominal value provided by the Covered Entity;
3. for the purpose of describing the entities participating in a Health Care Provider network or Health Plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such) is provided by a Covered Entity or included in a plan of benefits;
4. for treatment of the Individual; or
5. for case management or care coordination for that individual or to direct or recommend alternative treatments, therapies, health care providers or settings of care to that individual.

Minimum Necessary: Term that applies when the practice Uses, Discloses or requests Protected Health Information other than for Treatment purposes. The amount of Protected Health Information shared among the internal or external parties shall be the minimum amount necessary to accomplish the purpose of the Use or Disclosure. For internal use, the amount of information necessary to accomplish the purpose varies by job title or job classification.

NIST: National Institute of Standards and Technology

NPP: Notice of Privacy Practices

OCR: Office for Civil Rights

OHCA: Organized Health Care Arrangement -

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
2. An organized system of health care in which more than one Covered Entity such as The practice participates, and in which the participating Covered Entities:
    a. Hold themselves out to the public as participating in a joint arrangement; and
    b. Participate in joint activities that include at least one of the following:
        i. Utilization review, in which Health Care decisions by participating Covered Entities are reviewed by other participating Covered Entities or by a third party on their behalf;
        ii. Quality assessment and improvement activities, in which treatment provided by participating Covered Entities is assessed by other participating Covered Entities or by a third party on their behalf; or
        iii. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating Covered Entities through the joint arrangement and if Protected Health Information created or received by a Covered Entity is reviewed by other participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

3. A Group Health Plan and one or more such plans each of which are maintained by the same plan sponsor; or
4. The Group Health Plans described in paragraph (3) of this definition and Health Insurance Issuers or HMOs with respect to such group health plan but only with respect to Protected Health Information created or received by such health insurance issuers and HMOs plans that relates to Individuals who are or have been participants or beneficiaries in any of such Group Health Plans.

ONC: Office of the National Coordinator for Health IT - The principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health IT and the electronic exchange of health information

Password: Confidential authentication information composed of a string of characters.

Payment: The activities undertaken by a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan or undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care that relate to the Individual to whom Health Care is provided. Example activities include, but are not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
2. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
3. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related Health Care data processing;
4. Review of health care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
5. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
6. Disclosure to consumer reporting agencies of any of the following Protected Health Information relating to collection of premiums or reimbursement:
    a. Name and address;
    b. Date of birth;
    c. Social security number;
    d. Payment history;
    e. Account number; and
    f. Name and address of the Health Care Provider and/or Health Plan.

PHI: Protected Health Information - Individually identifiable health information that is transmitted by electronic media; maintained in any electronic media; or transmitted or maintained in any other form or medium. Identifiers that make up PHI:

1. Name
2. DOB
3. SSN
4. Address
5. Telephone Number
6. Email Address
7. Fax Number
8. Medical Record Number
9. Health Plan ID
10. Internet IP address

11. Certificate Numbers
12. Device Identifiers
13. Photograph
14. Biometric Identifiers
15. Web Addresses (URL)
16. Vehicle Identifiers
17. Account Numbers
18. Any other unique identifying number, characteristic or code

Physical Safeguards: Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion. One of the three safeguards required under the HIPAA Security rule.

PII: Personally Identifiable Information - Information that can be used on its own or with other information to identify, contact, or locate a single person

Psychotherapy Notes: Notes, that are separated from the rest of the individual's medical record, which are recorded (in any medium) by a Health Care Provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and. Psychotherapy Notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public Health Authority: An agency or authority of the United States, a State, territory, political subdivision of a State or territory, Indian tribe, person or entity acting under a grant of authority from or contract with such public agency including the employees or agents of such public agency, its contractors or delegated persons that is responsible for public health matters as part of its official mandate.

Required: A classification of Security Rule implementation specification, if described as “required,” the specification must be implemented. If the practice does not implement a required specification they are not meeting that part of the security rule.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

Secretary: The Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Security Measures: Encompasses all of the administrative, physical, and technical safeguards in an information system.

Sensitive Personal Information (SPI): defined as two types

1. Personal identifying information
    a. An individual’s first name or first initial
        + Their last name
        + Any of their following
            i. Social security number;
            i. Driver’s license number;
            ii. Government-issued identification number; or
            iii. Account number or credit or debit card number plus any financial account security code, access code, or password

2. Medical identifying information
    a. Information that identifies an individual and relates to their:
        i. Physical or mental health or condition;
        ii. Provision of health care; or
        iii. Payment for provision of health care

Technical Safeguards: The technology and the policy and procedures for its use that protect electronic protected health information and control access to it. One of the three safeguards required under the HIPAA Security rule.

THSA: Texas Health Services Authority - created as a public-private collaborative to implement the state-level health information technology functions.

Transaction: The transmission of information between two parties to carry out financial or administrative activities related to Health Care. It includes the following types of information transmissions:

1. Health care claims or equivalent encounter information
2. Health care payment and remittance advice
3. Coordination of benefits
4. Health Care claim status
5. Enrollment and disenrollment in a Health Plan
6. Eligibility for a Health Plan
7. Health Plan premium payments
8. Referral certification and authorization
9. First report of injury
10. Health claims attachments
11. Other transactions that the Secretary may prescribe by regulation

Treatment: The provision, coordination, or management of health care and related services by one or more Health Care Providers, including the coordination or management of health care by a Health Care Provider with a third party; consultation between Health Care Providers relating to a patient; or the referral of a patient for Health Care from one Health Care Provider to another.

Unsecured Protected Health Information: Protected Health Information that is not secured through the use of encryption or manual destruction

Use: With respect to Individually Identifiable Health Information, the internal sharing, employment, application, utilization, examination, or analysis of such information maintained by The practice.

User: A person or entity with authorized access.

Workforce Member: Employees-both faculty and staff, volunteers, trainees, and other persons whose conduct, in the performance of work for the practice is under the direct control of the practice whether or not they are paid by the practice.

Workstation: An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions and electronic media stored in its immediate environment.



About the Author

Cathy Bryant is a Risk Management Representative at TMLT. Cathy has had more than thirty years' experience in health care as a nurse, risk manager, compliance officer, hospital executive, and consultant. Cathy is a member of the Health Care Compliance Association and is certified in Healthcare Privacy Compliance by the Compliance Certification Board.

A special thanks to the TMLT editorial team.