Welcome to THR's Privacy 2

Privacy Matters

About this Training

In the screens that follow, you will find answers to questions like:

- What is HIPAA?
- How is HIPAA impacting the health industry?
- What is THR doing to comply with HIPAA?
- How can I protect privacy?
- What do I do if I believe that someone's privacy has been violated?
- What is an information breach?
- What happens when it's determined that someone has violated privacy?
- What are the severity levels of a sanctions?

Reading and mastering the guidelines presented in this booklet should take less than 30 minutes. You are welcome to add your own notes to any of the pages. Answer keys for the "Check Your Knowledge" sections in this booklet are located on the bottom of the page to help you judge your understanding of the topic.

At the end of the booklet is a **Knowledge Assessment**. When you complete this Knowledge Assessment, please return it to your department manager or entity privacy officer.

As always, should you have questions with any of the facts, concepts or procedures outlined in the pages that follow, don't be silent. Your supervisor or entity privacy officer is here to answer your questions.

The Phone Call…

Bradley and Gretchen King got little sleep the first few nights after Gretchen's recent hospitalization. When the phone rang, Bradley's first thought was that nobody calls this early.

Mr. King hung up. Back at Newhurst Medical Supply, the sales rep began dialing the next number on the list.

The King family viewed their health information as confidential. It evidently wasn't a view shared by everyone.

This lesson's focus is on HIPAA, the Health Insurance Portability and Accountability Act.

There Should be a Law

Everyone has an opinion of the health care industry. Comments range from coverage concerns to privacy issues. For many, opinions are shaped by experiences with health care providers. Mr. King is a good example. He found information he considered private in the hands of others.

Faced with mounting public pressure for health care reform, Congress took action. In 1996, Congress passed the Health Insurance Portability and Accountability Act, commonly known as "HIPAA."

HIPAA was designed to:

- ensure health insurance portability
- reduce health care fraud and abuse
- guarantee privacy and security of health information
- provide standards for electronic exchange of health information

The following table shows examples of HIPAA's impact.

Examples	HIPAA's Impact
Portability	Guarantees medical coverage renewal, prohibits discrimination based on health status, and eliminates some preexisting conditions exclusions.
Transaction Standards	Creates standard formats and code sets for all major transactions that are processed electronically.
Unique Identifiers	Provides national identifiers for providers, employers, and health plans.
Security Rule	Provides a uniform level of protection of all electronic health information.
Privacy Rule	Addresses the rights of an individual, the procedures for exercising these rights and the uses and disclosures of health information. Privacy regulations have been developed to ensure confidential treatment of patient data.

HIPAA is changing the health care landscape. It impacts processes, people, and timelines. Here's how.

Processes. HIPAA standardizes how procedures are coded and electronic bills are submitted. It also prompts health care organizations to examine processes and change how patient information is:

- communicated,
- shared,
- disclosed, and
- protected.

People. HIPAA touches everyone in our organization. It requires our employees, physicians, volunteers, and contractors to be trained and follow new policies, procedures, and processes.

Timeline. HIPAA sets rules for how we should act and penalties should we fail to meet the new standards. Compliance with HIPAA occurs in phases, starting in April 2003.

HIPAA versus State Law

Many states, including Texas, passed their own versions of HIPAA. This could have caused a problem. What if state and federal law said two different things? It turns out that the final version of HIPAA solved the problem.

Here's the solution: when state and federal versions differ, the more restrictive version applies.

The more restrictive law is reflected in our privacy policies.

HIPAA Terminology

Think back to when you started with THR. You had to quickly come to speed with terms such **SOSC**, **RICE**, and **TLC**.

It's the same with HIPAA. HIPAA introduces its own terms. Those who must comply with HIPAA are called **covered entities**.

SOSC—Strengthening Our System Culture

RICE—Respect, Integrity, Compassion, Excellence

TLC—Total LifeCare Connection®

Covered entities include providers, plans/insurers, and clearinghouses.

Providers. THR is a health care provider. Providers range from large hospital systems to individual nursing homes, labs, and pharmacies. Health care providers are also doctors, nurses, dentists, psychotherapists, and others who care for patients.

Plans or insurers. Examples include Cigna, United Health Care, Blue Cross/Blue Shield, and Aetna.

Clearinghouses. These are systems that process information for other companies such as most billing services like WebMD Envoy® .

Those responsible for protecting privacy are a covered entity's **workforce** members. A covered entity's workforce is more than its employees. Workforce members also include volunteers, people whose conduct is under the direct control of a covered entity, and people involved in a covered entity's training programs.

HIPAA protects the rights of **individuals**, not just patients. An individual is the subject of health information. This can include patients and health plan participants and their covered dependents. These same rights extend to **legally authorized representatives**.

PHI stands for Protected Health Information. This is health information—in any form—that can identify an individual. HIPAA and Texas state law defines how PHI may be used and disclosed.

Legally Authorized Representative

1. A minor patient's parent or legal guardian;
2. A legal guardian appointed by a court;
3. A beneficiary, if the patient is deceased;
4. An attorney retained by the patient or by the patient's legally authorized representative.

Individually Identifiable Health Information (IIHI) is health information that either identifies an individual or provides a reasonable basis for identifying an individual, by virtue of containing one or more of 18 identifiers.

These identifiers are:

- Names
- Geographic subdivisions
- Dates
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers
- Device identifiers and serial numbers
- Web Universal Resource Locator (URL)
- Internet protocol (IP) address number
- Biometric information
- Full-face photographic images
- Any other unique identifying number, characteristic, or code

Making HIPAA Happen

There are two views about HIPAA. Some see it as a series of expensive legal mandates (the half empty view). Others see it as an opportunity to look inward and improve policies and processes (the half full view).

We see it as an opportunity. In fact, it is more than an opportunity. It's a chance to recommit to putting patients first by protecting their privacy.

TEXAS HEALTH RESOURCES

THR serves 5.4 million people in a geographic area larger than the state of Maine. We're also one of the largest, faith-based, non-profit health care systems in Texas and the USA.

At the same time, each THR entity is unique. They're reflections of the communities they serve.

How do we "make HIPAA happen?" It takes both system and local approaches.

System	Local
• Create HIPAA Program Management Office to coordinate all HIPAA efforts. • Appoint System Privacy Officer.	• Appoint Entity Privacy Officer to ensure Privacy Program implementation at entity.

System	Local
• Develop and maintain training materials for the workforce. • Develop courses (like this one). • HIPAA web site (http://thrhipaa).	• Train existing and new workforce members.

Policies and Procedures

System	Local
• Develop and revise system-level privacy-related policies through entity collaboration.	• Create entity-specific procedures and implementation plans.

Reporting Concerns

System	Local
• Promote and staff toll-free System Compliance Hotline.	• Contact manager or Entity Privacy Officer.

It's just before shift change. Jill Gerson is talking with her manager.

Pat's right. In this lesson, we've focused on what THR is doing to "make HIPAA happen."

It's more than that. Our success depends on you. To our patients, families and friends, you are THR. It's through your actions that we build the patient's trust.

Recap

Families like the Kings put their trust in health care organizations. They expect their **PHI** will be kept private and confidential.

Responding to mounting concerns of the health care industry, Congress passed HIPAA in 1996. The law was designed to:

- ensure health insurance portability
- reduce health care fraud and abuse
- guarantee privacy and security of health information
- provide standards for electronic exchange of health information

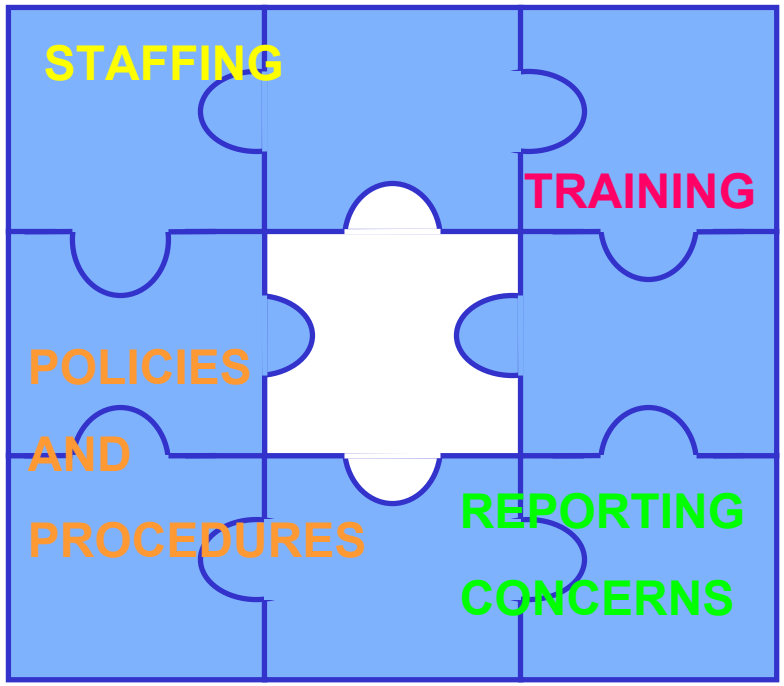
PHI

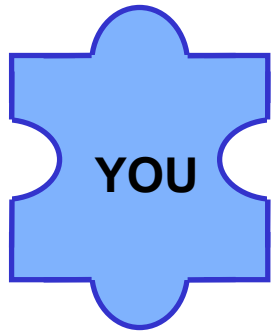
Protected health information is health information—in any form—that can identify an individual.

Some states, including Texas, passed their own version of HIPAA. In those instances when the state and federal version differ, the more restrictive standard applies.

HIPAA impacts each one of us who works in the health care industry, including employees, physicians, volunteers, and contractors.

It takes both system and local approaches to "make HIPAA happen." THR's approach addresses:





There is still one piece of the puzzle missing: You. To our patients, families, and friends—you are THR.

It's through all of our actions that we build the patient's trust.

Safeguarding PHI

Our patients hope, and expect, their privacy will be respected. Everyday we receive and manage health information about them. Even if you don't work directly with health information, it's all around you.

You must safeguard PHI so that it remains private and secure. Safeguards are the focus of this lesson. The following images will show you more about safeguards.

Ask questions …..if you see someone unfamiliar to you accessing PHI.

Conceal or secure PHI …..so that it can't be viewed on desks, door pockets, or in hallways. When not in use, ensure chart holders are closed.

• Print and/or copy from secure locations … so that PHI is not available to the public. Printers should be monitored for timely retrieval of printed documents.

• Keep your voice down …..when you have to discuss PHI in a public area, exercise care so that others don't accidentally hear you.

• Take precautions when discussing PHI over voicemail or the telephone… especially when you have to discuss PHI over the phone in public areas. Make sure that you are leaving a message for the right person.

• Control access…. to areas that contain PHI. This means that doors will be locked, card access systems and other physical access controls will be used as necessary. The number of designated entrances will be minimized after normal business hours.

• Identify...third party vendors, consultants, and others who provide services on our behalf by using sign-in, badge, and sign out procedures.

• Wear your badge…so you can be easily identified as a workforce member.

Because privacy may be violated when PHI is **not** safeguarded, we must recognize when it is not being protected. Let's look at the following examples. Place yourself in the following situation.

Example 1

A workforce member starts to put a surgery schedule in the trash.
What should you do?

Remind that workforce member the surgery schedule contains PHI and should be disposed of by shredding or placing it in a secure disposal container.

Example 2

You see an unfamiliar person looking at a patient chart. What should you do?

You should question any unfamiliar person you see accessing or using PHI. To safeguard PHI, each one of us needs to make sure that those accessing or viewing it have a valid need to do so. This even includes questioning workforce members.

Example 3

You enter a crowded elevator.

Workforce members are discussing a patient's condition. Our policies state we should not discuss patient information in common areas where those who are not authorized may overhear. What should you do?

It is difficult to confront others, especially our coworkers. You can remind a coworker of our commitment to privacy by placing your finger over your lips. What should you do if you need to discuss PHI in a public area?

Tip 1:

Sometimes we have to discuss PHI in public locations. In these cases, each one of us should be aware of our surroundings and keep our voices down so that those who don't have a need to know can't overhear it.

Tip 2:

Remember that PHI should only be discussed on a need to know basis. Gossip or careless discussion about PHI may be grounds for immediate termination.

Example 4

You place a call to the lab about a patient's tests and get voicemail.

What should you do?

When leaving a message containing PHI, you should listen to the mailbox greeting to ensure that the message is left for the right person.

Recap

Because THR uses PHI, safeguards need to be included as part of our daily routine. THR has established guidelines to help us safeguard health information.

It is your job to help protect health information in any form. If you are in doubt, or if something doesn't feel right, ASK!

You can find more information in the THR Safeguarding Health Information policy. This policy, as well as other THR policies can be found on the THR Intranet.





Information Breaches

When you think about it, health information is one of the most sensitive forms of personal information. It may contain information relating to substance abuse, depression, heart conditions, or other matters that individuals may want shared only with their caregiver.

Our goal is to safeguard health information. When PHI is not safeguarded, it can lead to an information breach. This lesson focuses on reporting potential information breaches, investigating these incidents, and consequences of violating an **individual**'s privacy.

Information breaches can result in the violation of an individual's privacy. An information breach occurs when PHI is:

- accessed by unauthorized individuals.
- discussed without a legitimate business purpose.
- revealed to those who don't have a need to know.

Individual

The subject of health information.

Anyone may report a potential information breach.

If you think an information breach has occurred you should report the incident to your supervisor or entity privacy officer. This can be done either verbally or using the Information Privacy Report form, which is shown in the next few pages. If you want to remain anonymous, you may call the THR System Compliance Hotline.

Remember the crowded elevator…

Workforce members are discussing a patient's condition. This could be an information breach. Your first responsibility is to safeguard this information. You can remind a coworker of our commitment to privacy by placing your finger over your lips.

Your next step is to report this incident to your supervisor or entity privacy officer. If possible, try to identify those employees when lodging this complaint.

Sanctions for Violating Privacy

Once a potential information breach is reported, your entity privacy officer will investigate promptly. If an investigation determines that a **workforce** member's actions resulted in an information breach, that person will be sanctioned. Sanctions are corrective actions that are based upon:

- information breach's severity level.
- information breach's impact.
- other factors such repeated offenses and patterns of abuse.

Workforce

Employees, volunteers, persons involved in THR training programs, and other persons whose conduct is under the direct control of an entity.

With HIPAA, violating an individual's privacy may result in criminal and civil penalties.

Severity level…	Minimum THR corrective action includes...	Possible civil and criminal penalties include…
Level-1: Carelessness		
Examples include: • Leaving documents with sensitive information on fax machines or printers • Failing to completely remove information that could lead to an individual's identity from a document • Accidentally modifying or altering data	• Administering corrective action as called for by severity of the impact • Requiring repeat of applicable privacy/security training	• Fines up to $25,000

Continued on next page.

Severity level…	Minimum THR corrective action includes…	Possible civil and criminal penalties include…
Level-2: Curiosity or Concern		
Examples include accessing or viewing health information on a family member, neighbor or co-worker when there is no need to know.	• Administering corrective action as called for by severity of the impact • Requiring repeat of applicable privacy/security training	• Fines up to $25,000

It really happened

Sometimes privacy is violated, even though things were done with the best of intentions……

A jury in Wuakesha, Wisconsin, found that an emergency medical technician (EMT) invaded the privacy of an overdose patient when she told the patient's co-worker about the overdose. The co-worker then told nurses at West Allis Memorial Hospital, where both she and the patient were nurses. The EMT claimed that she called the patient's co-worker out of concern for the patient. The jury, however, found that regardless of her intentions, the EMT had no right to disclose confidential and sensitive medical information, and directed the EMT and her employer to pay $3,000 for the invasion of privacy. (L. Sink, "Jurors Decide Patient Privacy was Invaded," Milwaukee Journal Sentinel, May 9, 2002)

Continued on next page.

Severity level…	Minimum THR corrective action includes…	Possible civil and criminal penalties include…
Level-3: Personal Gain or Malice		
Examples include: • Unauthorized access and use to health information for personal gain or malicious intent • Compiling mailing lists for personal use or to be sold or releasing celebrity information to the media	• Termination of employment • External reporting as necessary in compliance with federal and state regulations and statutory requirements • External reporting to boards, professional associations, and certification bodies as required	• Fines up to $250,000 • Up to 10 years in prison

It really happened

When privacy is violated…

Country singer Tammy Wynette's medical records were sold to the National Enquirer and Star tabloids by a hospital employee for $2,610. William Cox's position at the hospital entitled him to authorized access to several medical record databases. He retrieved medical information about Tammy Wynette and faxed it to the tabloids without her consent. In the end, Cox pleaded guilty to one count of wire fraud and was sentenced to six months in prison. ("Selling Singer's Files Gets Man Six Months," Houston Chronicle, December 2, 2000, p. A2)

Like any other corrective action, appeals may be made according to the Alternative Dispute Resolution policy.

Recap

Health information is one of the most sensitive forms of personal information. When PHI is not safeguarded, it can lead to an information breach resulting in the violation of an individual's privacy. An information breach occurs when PHI is:

- accessed by unauthorized individuals.
- discussed without a legitimate business purpose.
- revealed to those who don't have a need to know.

All potential information breaches should be reported.

Anyone may report a potential information breach. This can be done verbally or by completing the Information Privacy Report form. You should also report the incident to your supervisor or your entity privacy officer. If you want to remain anonymous, you may call the THR System Compliance Hotline.

Once reported, your entity privacy officer will investigate promptly. If an investigation determines that a workforce member's actions resulted in an information breach, corrective action will be taken.

Sanctions will be based on the severity of the information breach. With HIPAA, violating an individual's privacy may result in criminal and civil penalties. The severity levels are:

Level 1: Carelessness

Level 2: Curiosity/Concern

Level 3: Personal Gain or Malice

For more information, contact your entity privacy officer or review the Information Privacy and Security Inquiries, Complaints, and Breaches policy or the Information Privacy and Security Sanctions policy.