HIPAA Training Program

Metro Government of Nashville and Davidson County

October 2014

Table of Contents

Overview

The Metropolitan Government of Nashville and Davidson County (“Metro”) **HIPAA Training Program** is comprised of **8 Chapters** which address key HIPAA compliance activities including various Privacy and Security topics. All Metro employees play a key role in ensuring our compliance with the HIPAA Standards.

Please ensure you spend the time required to gain an understanding of the **HIPAA Training Program** content and the referenced policies and procedures.

Chapter 1: Introduction to HIPAA

What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a federal law that was created to improve efficiency and effectiveness of the healthcare system while protecting patient privacy by establishing a set of standards and requirements for transmitting certain health information.

HIPAA Regulates:

✓ **Covered Entities –** Healthcare Providers, Health Plans, and Healthcare Clearinghouses

✓ **Business Associates –** A person or entity that provides services to or on behalf of a Covered Entity that involves the use or disclosure of Protected Health Information (PHI)

What is Protected Health Information?

Protected Health Information ("PHI") is any oral, electronic, or paper record that is created or received by a Healthcare Provider, Health Plan, or Healthcare Clearinghouse ("Covered Entities") and Business Associates that contains any individually identifiable information AND any health information.

Some examples may include:

- Patient name and prescription information
- Patient birth date and medical condition
- Patient phone number and medical diagnosis
- Driver's license number and medical records

PHI can also be in the form of electronic PHI **("ePHI")**, which is PHI that is created, stored, transmitted, or received **electronically.**

PHI does not include information on Americans with Disabilities Act accommodations, Worker's Compensation, Life Insurance, Accidental Death & Dismemberment, or Federal Medical Leave Act.

The Different Components of HIPAA

HIPAA is comprised of five main parts, referred to as **"Titles",** which cover a range of activities and content related to PHI.

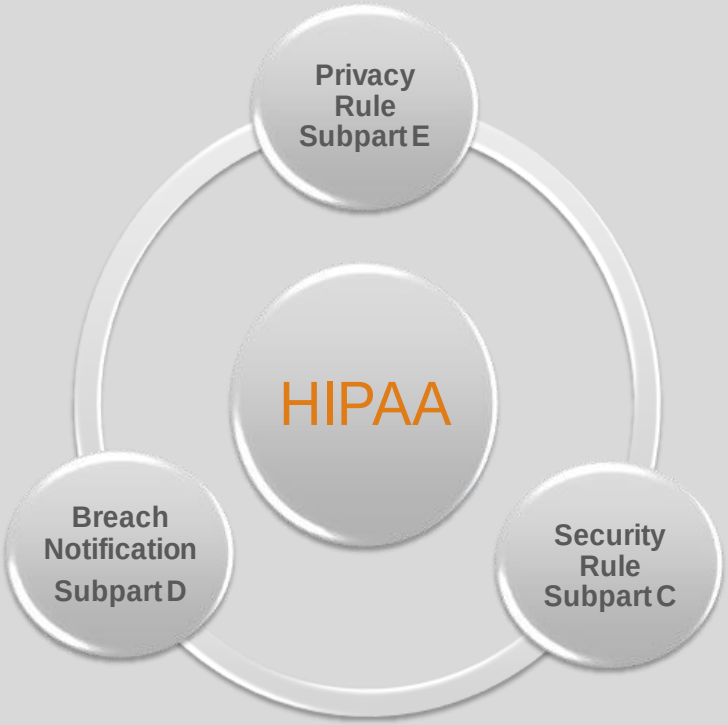
While HIPAA covers a number of important healthcare issues, the focus of this training is on the preventative portion of the law, specifically the **Administrative Simplification Rule** under Title II which defines policies, procedures, and guidelines for maintaining the **privacy** and **security** of PHI.

Title I	Title II	Title III	Title IV	Title V
• Healthcare access, portability, and renewability	• Preventing Healthcare fraud and abuse, administrative simplification, medical liability reform	• Tax related health provisions	• Application and enforcement of group health plan requirements	• Revenue offsets

Privacy, Beach Notification, and Security Rules

Title II of the Administration Rule addresses three key important areas that will be discussed throughout this training:

- Privacy Rule
- Breach Notification Rule
- Security Rule



Privacy Rule

The Privacy Rule requires Covered Entities to implement policies and procedures to protect PHI and gives individuals certain rights with respect to access and disclosure of their PHI. In order to comply with the Privacy Rule, Covered Entities must:

- Protect PHI in all formats including oral, electronic, and paper;
- Use appropriate safeguards to protect the privacy of PHI;
- Set limits and conditions on the uses and disclosures that may be made of PHI without a patient's authorization; and
- Provide individuals with the right to access and amend their information and receive an accounting of disclosures.

Breach Notification Rule

The Breach Notification Rule requires HIPAA Covered Entities and Business Associates to provide notification following a breach of unsecured PHI.

Covered Entities and Business Associates must provide notification of the breach to affected individuals, the Secretary of the US Health and Human Services Department, and in some cases, to the Media.

Security Rule

The Security Rule specifies a series of administrative, physical, and technical safeguards to ensure the confidentially, integrity, and availability of ePHI:

- **Confidentiality:** ePHI should only be accessible by authorized people and processes.
- **Integrity:** ePHI should not be altered or destroyed in an unauthorized manner.
- **Availability** ePHI should only be accessible as needed by an authorized person.

Question

John is a full-time Nashville Fire Department employee. While walking home from work, he notices a paper on the sidewalk that contains the name, address, age, and gender of his friend, Martha.

Q: Does this file constitute a breach of PHI?

A: No. The information is not considered PHI because it does not contain health information.

Although Martha's information is considered personally identifiable information (PII) which may be protected by other federal and state regulations, this does not constitute PHI because there is no related health information.

Chapter Key Summary

HIPAA

- The Privacy Rule requires Covered Entities to implement policies and procedures to protect PHI.

HIPAA

- Breach Notification Rule requires HIPAA Covered Entities and Business Associates to provide notification following a breach of unsecured PHI.

HIPAA

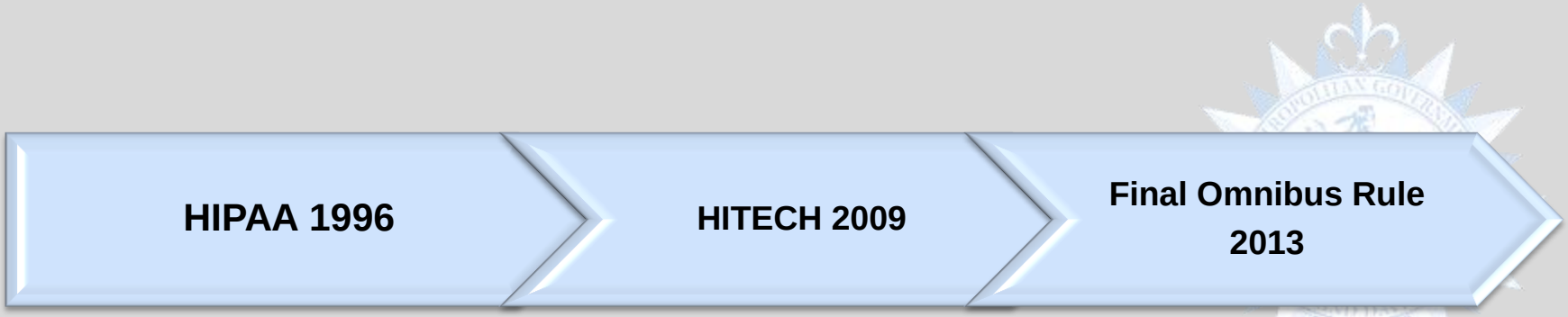
- The Security Rule specifies a series of administrative, physical, and technical safeguards to ensure the confidentially, integrity, and availability of ePHI.

Chapter 2: Recent Updates to HIPAA

Recent Updates to HIPAA

Since its enactment in 1996, the HIPAA requirements have evolved over the years. HIPAA has gone through two major amendments:

1. **The Health Information Technology for Economic and Clinical Health Act ("HITECH")** in 2009; and
2. **Final Omnibus Rule** in 2013.



What is the HITECH Act?

The HITECH Act is part of the American Recovery and Reinvestment Act of 2009 ("ARRA"). ARRA created specific incentives designed to accelerate the implementation of electronic health record (EHR) systems for healthcare providers.

Due to the significant increase in the exchange of ePHI that resulted from the ARRA, HITECH expanded the scope of privacy and security protections available under HIPAA.

Key areas that were enhanced through the **HITECH Act** include:

- Imposing data breach notification requirements for unauthorized uses and disclosures of "unsecured PHI";
- Providing individuals with a right to obtain their PHI in an electronic format; and
- Requiring Business Associates to comply with certain HIPAA regulations that previously only applied to Covered Entities.

What is the Final Omnibus Rule?

In 2013, the U.S. Department of Health and Human Services Office for Civil Rights announced the **Omnibus Rule** that fully implements a number of provisions of the HITECH Act in addition to new requirements.

The 2013 Final Omnibus Rule amended HIPAA in many ways, including enhancing regulations related to the following areas:

- Made Business Associates of Covered Entities directly liable for compliance with certain HIPAA Privacy Rule and Security Rule requirements;
- Limited the use of PHI for marketing and fundraising purposes;
- Prohibited the sale of PHI without an individual's authorization; and
- Increased civil monetary penalties related to HIPAA violations.

Question

Q: Since its enactment in 1996, how many times has HIPAA been amended?

A: Twice. HIPAA has undergone changes related to two major amendments: The HITECH Act and the Final Omnibus Rule.

Chapter Key Summary

HIPAA

- Since its enactment in 1996, HIPAA has undergone changes related to two major amendments: The HITECH Act and the Final Omnibus Rule.

HIPAA

- The HITECH Act expanded the scope of privacy and security protections available under HIPAA.

HIPAA

- The Omnibus Rule implemented a number of provisions of the HITECH Act in addition to new requirements.

Chapter 3:
Who is Required to Comply with HIPAA?

Who Must Comply with HIPAA?

Under HIPAA, all **Covered Entities** and **Business Associates** must adhere to minimum standards for accessing and handling PHI.

In addition, organizations that provide some functions of a Covered Entity may be considered a "**Hybrid Entity.**" The Privacy Rule may treat an organization that includes a Hybrid Entity as a Covered Entity (including both its covered and non-covered components), so that the entire organization must comply with HIPAA rules and regulations.

What is a Covered Entity?

Under HIPAA, a **Covered Entity** is one of the following:

Healthcare Provider

Organizations that actively provide health services to patients.

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Health Plan

Administrators of a health insurance plan that perform billing and claims related support tasks.

- Health insurance companies
- HMOs
- Company health plans
- Government programs

Healthcare Clearinghouse

This includes entities that process nonstandard health information they receive from another entity into a standard format.

Covered Entities in Metro

By applying the definitions of a Covered Entity to Metro departments and services, the following have been identified as having functions of **Covered Entities**:

Healthcare Providers	Health Plans
Metro Hospital Authority Metro Public Health Department • East Clinic • Oral Health Services • Primary Clinic • STD/HIV Prevention and Intervention • Tuberculosis Elimination • Woodbine Clinic Nashville Fire Department • Ambulance Billing Section • Emergency Management Services	Metro Human Resources • Benefits Department Metro Public Schools • Benefits Department Metro Transit Authority • Benefits Department

What is a Business Associate?

A Business Associate is a person or entity which performs functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity, and any entity that maintains PHI on behalf of a Covered Entity.

Some of these business functions include claims processing, data analysis, utilization review, and billing.

There are two types of Business Associates:

1. **External Business Associates**
2. **Internal Business Associates**

What is a Business Associate? (Cont.)

(1) External Business Associates

External Business Associates are outside third-party vendors who process Metro's PHI on behalf of the Covered Entities.

Some examples of these third party vendors include:

- Third-party vendors that provide language translation services to patients within the Metro Public Health Department.
- Third-party vendors that provide shredding services for hard copy documents that contain PHI to all Metro Covered Entities.

What is a Business Associate? (Cont.)

(2) Internal Business Associates

Business Associates can also be internal Metro departments that perform the same types of support functions to Metro Covered Entities.

Metro Internal Business Associates:

- Metro ITS
- Metro Records Center
- Department of Law
- Metro Public Health Department (Human Resources, IT, Quality Management, and Vital Records)
- Nashville Fire Department (IT)
- Metro Nashville Public Schools (Audit and IT)

Question

Q: Is Metro considered a Covered Entity or a Business Associate?

A: Neither. Metro is considered a **HYBRID ENTITY.**

A **Hybrid Entity** is a Covered Entity that has business activities which include both covered and non-covered functions with a goal of focusing HIPAA compliance efforts on covered areas.

Chapter Key Summary

HIPAA

- HIPAA applies to Covered Entities and Business Associates.

HIPAA

- Metro is considered a Hybrid Entity.

HIPAA

- Within Metro, there are four Covered Entities that are either Healthcare Providers or Health Plans.

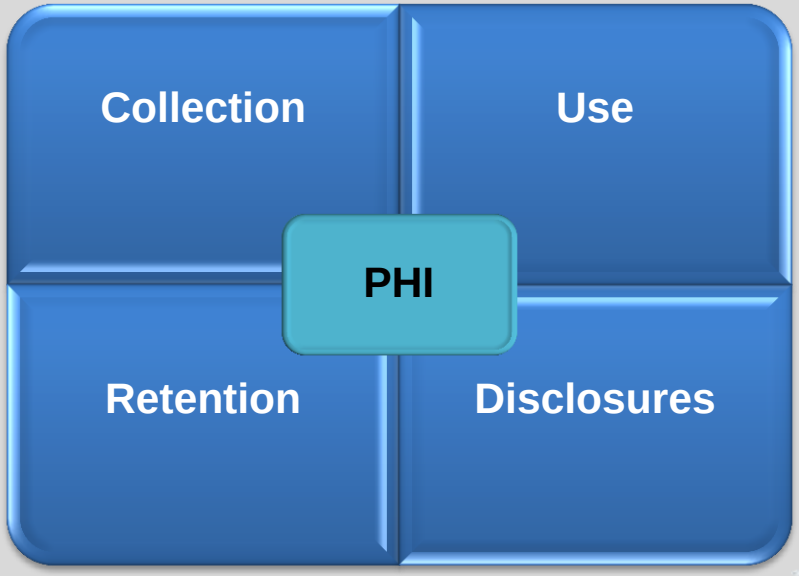
HIPAA

- Business Associates perform business functions on behalf of Covered Entities and may either be external or internal.

Chapter 4: Privacy

HIPAA Related Risks

The risks associated with privacy and security of PHI revolve around the inappropriate or unauthorized **collection, use, retention,** and **disclosure** of PHI.



Privacy

The Privacy Rule gives patients individual rights related to PHI. The privacy requirements apply to all Covered Entities, and some of these requirements also apply to Business Associates.

Some of the Privacy Rule requirements include:

- **Notice of Privacy Practices** that outlines individual's rights with regards to the privacy of their PHI and how it is used and disclosed.
- **Policies and Procedures** on how to protect PHI and sanctions for employees who fail to follow the guidelines.
- Limitation on the **Uses and Disclosures** of PHI.
- Adherence to use and disclose only the **Minimum Necessary.**

Notice of Privacy Practices

The Notice of Privacy Practices

The Notice of Privacy Practices ("NPP") is a document that is distributed to individuals who receive services from Metro's HIPAA Covered Healthcare Providers and Health Plans. The NPP describes how PHI may be used and disclosed by Metro Covered Entities and how individuals may access their own PHI. The NPP also describes the rights of individuals to control how their information is used and disclosed by Metro.

All Employees Should…

Ensure the NPP is properly posted in a clear and prominent location in the facility and distributed to all patients at the time of their first visit and plan participants at the time of enrollment and within 60 days of a material revision within Metro, where applicable.

The NPP must be posted on applicable Metro websites and on the Metro intranet.

Privacy Policies and Procedures

Metro Covered Entities and Business Associates maintain detailed policies and procedures to outline the "***HOW TO's***" for the appropriate use and handling of PHI.

Why are these Privacy Policies and Procedures Important?

There may be a variety of ways in which you will come into contact with PHI and it is your responsibility to act according to the Privacy policies and procedures.

What kinds of Privacy situations do these policies and procedures address?

- HOW TO acceptably use and disclose PHI
- HOW TO verify requests for PHI
- HOW TO disclose PHI to a Family Member or Friend
- HOW TO disclose PHI to law enforcement
- *…and more!*

Use and Disclosure of PHI

PHI is "***used***" within the organization and "***disclosed***" when it is transmitted outside the organization.

PHI that Metro collects may include:

- ✓ Patient-level Health Information
- ✓ Health Plan Member Enrollment Data
- ✓ Social Security Numbers
- ✓Human Resources Employee Data

Use and Disclosure of PHI (Cont.)

The Privacy Rule allows uses and disclosures of PHI in the following ways without obtaining an authorization from the individual:

- ✓ **Individual**: To the individual about whom the PHI pertains.
- ✓ **Payment**: Metro may use and disclose PHI to obtain payment health expenses.
- ✓ **Healthcare Operations:** To perform activities, such as quality assessment or administration, data management, or customer service.
- ✓ **Treatment**: To assist Healthcare Providers in diagnosis and treatment.

If you have a question about how to use or disclose PHI, contact the HIPAA Compliance Office, your designated Privacy Officer, or Manager.

External Requests for Access to PHI

Metro tracks all disclosures of PHI in accordance with regulatory requirements.

Metro procedures are designed to permit the department to account for:

- The date, nature and purpose of each external disclosure.
- The name and address of the person or agency to which the disclosure was made.

Minimum Necessary

A key component of Metro's privacy program is to ensure that any use or disclosure of PHI is limited to the **Minimum Necessary** to accomplish an authorized purpose.

- ✓ **Sensitive Information –** You should only share PHI with those who are authorized and have a business need to know. *Ask your manager if you have a question on whether to share PHI.*
- ✓ **PHI –** You should only share PHI with those who have been granted access in accordance with the applicable policies and procedures. *Ask the Privacy Officer if you have a question on sharing PHI.*

Examples of applying the Minimum Necessary Rule:

- The treating physician asks you for a copy of the patient's lab results - the "minimum necessary" production includes only the lab results.
- You are accessing patient records in order to treat the patient, the "minimum necessary" information is limited to the patients at the healthcare location where you work. You should not access PHI from other sites, unless relevant to treatment of that patient.

Organizational Safeguards

The Privacy Rule defines several safeguards aimed at protecting the confidentiality and integrity of PHI. Such safeguards include:

- Formal contracts between Business Associates and Covered Entities which outline the specific requirements for protecting PHI;
- Administrative policies and procedures that provide guidance on how to protect PHI and sanctions for employees who fail to follow the guidelines;
- Internal and external privacy statements that outline the Covered Entities' attitude towards protecting PHI and steps they take to protect it; and
- Forms that can be used by patients to authorize the disclosure of PHI to other individuals or organizations.

These safeguards are designed to provide patients rights with respect to the PHI that Covered Entities maintain while simultaneously providing Covered Entities with procedures for allowing the transfer of information to other entities with and without patient consent to perform the required business activities.

Question

Justin is a full-time Metro Public Health Department ("MPHD") employee and requests to obtain access to his wife's PHI who is a patient at Woodbine Clinic. Justin's hiring Manager submits a Help Desk ticket requesting immediate access to PHI for Justin in connection with an urgent project.

Q: Should you give Justin access to the data?

A: No. The approval of a hiring manager is not sufficient for access to PHI.

Please refer to the MPHD policy "Disclosures to Family, Friends, and Caregiver," which is located on the internal intranet for guidance on how to provide Justin authorized access to his wife's PHI.

Chapter Key Summary

HIPAA

- The Notice of Privacy Practices outlines individual's rights with regards to the privacy of their PHI and how it is used and disclosed.

HIPAA

- Reference Metro policies and procedures on how to protect PHI and sanctions for employees who fail to follow the guidelines.

HIPAA

- When using or disclosing PHI, always adhere to the Minimum Necessary standard.

Chapter 5: Security

Importance of Securing ePHI

It is vital to ensure that administrative, physical, and technical safeguards are in place to ensure the confidentiality, integrity and availability of ePHI.

Confidentiality	• ePHI should only be accessible by authorized people and processes.
Integrity	• ePHI should not be altered or destroyed in an unauthorized manner.
Availability	• ePHI should be accessible as needed by an authorized person.

Security

Metro security entails safeguards to ensure the protection and integrity of ePHI. These safeguards can be divided into three categories:

1. **Administrative Safeguards** refer to processes that promote the safeguarding of ePHI and PHI through proper training and documented policies and procedures.

2. **Physical Safeguards** refer to the physical safekeeping of electronic equipment, systems, and data by limiting physical access.

3. **Technical Safeguards** refer to automated processes used to protect data control and access to data (e.g. network login procedures, password complexity, etc.).

Administrative Safeguards

Administrative Safeguards create a strong security foundation by helping Metro ensure its employees are compliant, trained, and aware of privacy and security risks.

Examples of Administrative Safeguards include:

- Ensuring policies and procedures are in place to properly safeguard PHI; and
- Periodically training and reminding Metro employees of the importance of HIPAA and the policies and procedures supporting appropriate conduct.

Physical Safeguards

Physical Safeguards protect Metro from unwanted access to its systems and ensure that Metro can access ePHI in emergencies.

Various safeguards have been implemented to protect electronic systems, equipment, and the data they hold from environmental threats and unauthorized intrusions.

Examples of Physical Safeguards include:

- Limitation on Physical Access
- Workstation Security
- Secure Disposal of PHI

Physical Safeguards (Cont.)

Limiting Physical Access

Applicable access points are equipped with a badge reader and all Metro employees are provided with an identification badge to permit access.

Restricted areas are limited to employees with a business purpose and management approval.

Employees are prohibited from allowing others to borrow their identification badge or use their badges to permit entry for visitors.

Temporary access can be granted to specific individuals

- **Consultants/Contractors:** Consultants/Contractors will be provided with a temporary access card for access to secure areas as required for legitimate Metro business.

- **Visitors:** All visitors must sign the Visitor Log at the front desk and be escorted.

Technical Safeguards

Organizations are faced with the challenge of protecting ePHI from various internal and external risks. To reduce risks to ePHI, Metro has implemented technical safeguards such as Access Controls, Audit Controls, Integrity Controls, and Transmission Security.

Examples of technical safeguards include:

- Using complex passwords.
- Ensuring that critical electronic systems are automatically backed up on a periodic basis.
- Confirming that access to systems and ePHI is authorized.
- Ensuring that there is an updated version of anti-virus software installed on your workstation.

Note: If ITS is managing any of these technical safeguards for your Department please ensure that ITS is aware where your PHI is located and how they should treat your PHI in adherence with Metro's policies.

Technical Safeguards (Cont.)

Access Controls

In accordance with the ITS Acceptable Use of IT Assets Policy, Metro has implemented controls which limit access to systems containing PHI to those who need such access to perform their job functions.

- **Account Authorization:** Access will be granted based on specific job functions and only with explicit managerial approval.
- **Remote Access:** Employees often need to access the network after hours or from remote locations but this is limited to a specific job function.
- **Approval of Vendor and Contractor Remote Access:** Remote access for vendors and contractors must be specifically requested and approved.
- **Timeout:** Metro workstations have been configured to log users out after a certain period of inactivity.

Technical Safeguards (Cont.)

Malicious Codes

Malicious Code is software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Examples of malicious code and their goals include:

- Denial of Service: Participate in making another system unusable
- Keylogger: Capture every keystroke of a user
- Phishing: Trick user into revealing information
- Ransom-ware: Hold the user data “hostage” until payment received

Technical Safeguards (Cont.)

Phishing

Phishing attacks often happen via email and web pages, but can also happen over the phone. The cyber criminals are trying to steal bank account, credit card, social security numbers, medical records, and proprietary company information.

Phishing emails can look like:

- Legal Notices (e.g. IRS, parking ticket, foreclosure, unpaid taxes).
- Shipping Notification.
- Your account is suspended, locked, or being audited.
- Requests for Patient Information.

Question

You are headed out to lunch and notice a representative of the Metro shredding service company is standing by the back doors. Seeing you, he calls out, “Do you work here? Can you let me in?”

Q: What should you do?

A: Take him to reception so he can sign-in. Reception can then direct him to the appropriate person.

Chapter Key Summary

HIPAA

- Administrative Safeguards create a strong security foundation by helping Metro ensure its employees are compliant, trained, and conscious of security risks.

HIPAA

- Physical Safeguards protect Metro from unwanted access to its systems and help ensure that Metro can access ePHI in emergencies.

HIPAA

- Technical Safeguards reduce risks to ePHI through access safeguards such as complex passwords and workstation timeouts.

Chapter 6:
Privacy and Security Best Practices

How to Implement Privacy and Security

Privacy Rule	Security Rule
✓ Complete HIPAA training upon hire and annually. ✓ Read the Notice of Privacy Practices applicable to the area in which you work. ✓ Comply with Privacy policies and procedures. ✓ Ensure the proper Uses and Disclosures of PHI. ✓ Ensure compliance with the "Minimum Necessary" Rule. ✓ Implement Organizational Safeguards.	✓ Comply with Administrative Safeguards. ✓ Comply with Physical Safeguards. ✓ Comply with Technical Safeguards.

Using and Disclosing PHI

Any person to whom PHI is communicated must be authorized to receive the information and have a "need to know."

To use and disclose PHI, always:

- Notify your supervisor of all requests for PHI.
- All requests PHI must follow the appropriate Department level policies and procedures related to the Release of PHI.

Daily Activity Safeguards with HIPAA

FAX

- Use a Fax Cover Sheet that includes a confidentiality statement.
- Ensure that the Fax Cover Sheet does not include any PHI.
- Double check fax number.
- Confirm fax was received.

PHONE

- Verify the identity of caller.
- Confirm with the caller patient's name and date of birth.
- Never provide PHI to unknown individual.
- Take calls in a private area.

EMAIL/WEB

- Do not include any PHI in the subject line.
- Use ITS-provided encryption.
- Use ITS-provided secure FTP portal for file transfers.
- Include your information in the signature line.
- Do not email PHI to or from your personal email account.
- Limit distribution to those with a "need-to-know".
- Use "reply all" with caution.

MAIL

- Verify mailing address.
- Address mail to a specific individual.
- Include return address with contact information.
- Mark as "Confidential."
- Track the package.

Daily Activity Safeguards with HIPAA (Cont.)

PAPER DOCUMENTS

- Limit printing any PHI document.
- Keep paper in locked containers.
- PHI should be disposed of as soon as possible.
- PHI must be properly disposed (e.g. shredded).

SELECTING PATIENT RECORDS

- Verify that you are requesting PHI for the correct patient.
- Always double-check the name and date of birth of the patient.
- Triple-check the name and date of birth of the patient when sending PHI to outside agencies.

MEDIA, PHOTOGRAPHS, OTHER MEDIA

- Do not take any photographs or other media of PHI without prior authorization.

Strong Passwords

Employees are prohibited from sharing, writing down, or storing passwords in unsecure electronic files.

In accordance to ITS Password Management guidance and Standard Password documentation, employees, contractors, and third party users should always use strong passwords which:

- Are a minimum of 10 characters in length.
- Consist of at least one capitalized alphabetic character, one numeric, and one special character (*,%, @, #, $,^).
- Do **not** contain a word in any language, slang, dialect, jargon, etc.
- Do **not** contain 4 or more repeating characters or a predictable pattern.

Complex Passwords (Cont.)

All Metro employees must use **Complex Passwords** that are at least 8 characters and include letters, digits, and punctuation. Passwords must be changed regularly in order to reduce the likelihood that they can be guessed or breached.

Weak Password	Why is it Weak?	Make it Stronger!	How do I make it Stronger?
TitaNs	Plain text	The TiT@Ns R my Favorite Team^	Make it a phrase!
Kathy5	Name based	Tit@NsROCK^	Abbreviate the phrase!
12345	Keyboard sequence	M@k3 it a G00d d@y :0)!	Add an emoticon!
Abcabc	Repeating sequence	2BorNot2B_Th@tIsThe?	Make it memorable!
Driv3way	Word based with common letter or number substitute	$1$1TiT@nS$1$1	Pad with special characters and numbers!

Lock Workstations

All employees should lock their computers before leaving them unattended.

- Employees must lock all workstations, laptops, and mobile devices/media that contain PHI prior to leaving them unattended.
- Employees are expected to secure documents or mobile media such as USB devices that contain PHI by locking them in a drawer or filing cabinet prior to leaving them unattended.
- Leaving a workstation unlocked and unattended could cause unauthorized access to ePHI or a security breach that compromises Metro's network.
- Employees must log out of the applicable electronic health records system when not in use.

Media Controls

The term media includes all electronic storage devices such as laptop hard drives, external hard drives, SD cards in phones, and USB drives.

Media Use:

Staff should only use internal, Metro-owned and provisioned media for Metro-related work. Users are required to return all internal media to Metro when no longer needed. If external non-Metro owned media should ever be needed, staff must obtain Director level approval prior to utilizing any outside devices.

Export of PHI:

Copying PHI to non-Metro owned storage devices is **strictly prohibited.** PHI may only be copied to Metro-owned removable storage devices which are encrypted with technology that complies with Metro's Encryption Policy.

Re-Using Media

- Prior to media being re-issued internally within Metro (reassigned to another employee or re-purposed) or transferred to another party outside of Metro, all media must be given to IT for sanitation.
- IT will wipe reusable media, such as USB drives, portable hard drives, or CD/DVD after each use.
- Employees should not use a USB device or other portable storage media that they find without first bringing it to IT for sanitation and review.
- If a USB device or other portable storage media is found outside of Metro, employees should NOT bring it to Metro for use.

Wiping Media

All media must be securely destroyed when no longer needed or wiped when redeployed to another employee. Media must be wiped even if it is going to another employee with the same role.

- All media including, but not limited to, laptops, USB drives and hard drives, that are no longer needed or have reached end-of-life must be given to ITS for secure destruction.
- ITS will also wipe reusable media, such as USB drives, portable hard drives, or CD/DVD after each use.

Mobile Devices

Mobile Devices including tablets and smart phones must be approved through the Director of ITS prior to connection to the information. All Metro mobile devices and the information stored on those devices are subject to review and inspection by the CISO.

- **PIN/Password:** A PIN or password will be required on all mobile devices.
- **Inactivity Screen Lock:** All mobile devices must have a lock screen that activates within 15 minutes of user inactivity.
- **Remote Wipe:** Where feasible, Metro will implement remote wiping of mobile devices. If a device is reported lost or stolen or has suspicious activity, Metro may remotely purge the information from the mobile device.

Encryption

All PHI must be encrypted when stored or transmitted.

- All PHI stored on portable devices must be encrypted and laptops must have full disk encryption.
- All transmitted files containing PHI that will travel wirelessly or across public networks must be encrypted.
- PHI is never to be sent unencrypted through e-mail, instant messaging, or chat.
- Metro non-public information should never be posted on social media.
- Do not store Metro files in the cloud (i.e., Google Drive, DropBox, Amazon Cloud Storage, iCloud, etc.) unless you are using a Metro approved service or website.
- Contact ITS for guidance on usage of their secure FTP portal.

Email Usage

Always use Metro email for Metro business. However, email should not be relied upon as a secure method for communicating PHI.

- The ITS department has tools at its disposal which can eliminate the need to send PHI through email.
- Emails are almost impossible to recover after clicking on **"SEND"** and it is very easy to mistype email addresses which may result in the transmission of PHI to an unauthorized individual.
- **"REPLY ALL"** should NEVER be used to communicate PHI.

Internet Usage

All staff are provided with internet and email, but are expected to use these resources only for appropriate purposes. Inappropriate use of internet and email can result in security incidents including infected computers, loss of data, or alteration of information within Metro systems.

Examples of inappropriate internet and email use include:

- Websites which make anyone feel unwelcome or uncomfortable because of their race, age, gender, etc.
- Sending chain emails.
- Illegal copying of copyright protected works such as MP3 audio files, movies, software, articles, or puzzles.

Additional Guidance

Additional guidance and safeguards related to these topics can be found in **Metro's Acceptable Use of IT Assets Policy**.

In any instance where ITS manages components of your electronic equipment that house PHI, it is YOUR responsibility to notify ITS and work with them as your partner to ensure that your PHI is safeguarded to your satisfaction.

Question

You visit Ryan's desk to deliver some documents. At his desk, you notice that he has sticky notes with "Password -123123" and "ID- Ryan Jackson" written on them attached to his monitor with the name of programs and websites. You ask him if this is his log-on information. "Yes, but don't tell anyone," he says in a hushed tone, "I can't possibly remember all my passwords."

Q: Has Ryan violated Metro's password policy?

A: Yes. His password does not meet the minimum requirements and should not be posted on his computer.

Bonus Question: How could Ryan make the password stronger?

Bonus Answer: He could make it a phrase, abbreviate a phrase, or pad with special characters.

Chapter Key Summary

HIPAA
- **DO** keep your workspace clear of sensitive papers, cell phones, laptops, and other media that contain PHI or other sensitive information when not in use.

HIPAA
- **DO** use complex passwords.

HIPAA
- **DO** lock your workstations when unattended.

HIPAA
- **DO** use encryption techniques when transmitting PHI through email.

HIPAA
- **DON'T** install unapproved software on Metro assets (e.g. workstations, laptops, mobile devices).

HIPAA
- **DON'T** include PHI or other sensitive information in emails, unless there is a secure domain-to-domain pathway.

HIPAA
- **DON'T** discuss or share PHI unless there is a true business need.

HIPAA
- **DON'T** share, write down, store in electronic files, or email your passwords.

Chapter 7:
How to Identify and Report a HIPAA Violation

Risks to PHI

The risks to the confidentiality of PHI may come from many different sources, including:

Internal	Employees, contractors and consultants who may intentionally or unintentionally expose PHI.
External	Hackers, ex-employees, vendors, or criminals who expose or alter PHI.
Environmental	Equipment failure, fire, flood, wind storm, or community infrastructure failure which can cause PHI to be exposed or altered.

It is important to remain vigilant and report any suspicious or negligent behavior that compromises the integrity of PHI.

What is the Difference between a BREACH and an INCIDENT?

A Privacy **Incident** is any time an employee suspects that any unauthorized or inappropriate access, disclosure, modification or disposal of PHI, whether internal or external, has occurred. An **Incident** can also refer to known or suspected violations of security policies, security procedures, or acceptable use policies.

Whether a **Breach** has occurred is a legal determination made by Metro's legal counsel after review of the facts gathered by Metro's Incident Response Team.

The Metro Department of Law will determine if a breach has occurred and whether it will need to be reported to regulators.

Identifying a Potential HIPAA Breach

There are many activities that may lead to a breach of PHI.

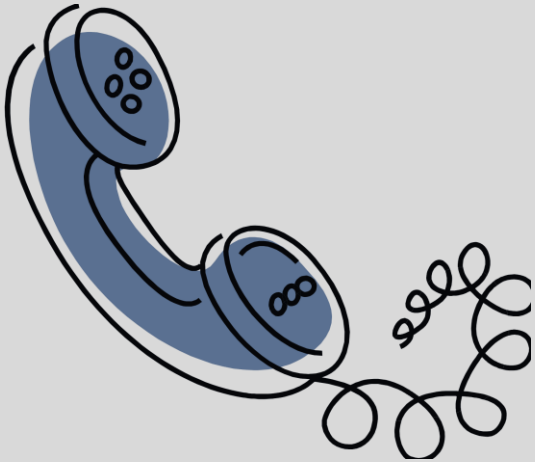
Some examples include:

- Lost or stolen hardware.
- Backup tapes lost in transit.
- Employees stealing information or allowing access to information.
- Information acquired for fraudulent purposes.
- Careless disposal of information (e.g. exposed via dumpster diving).
- A malicious attacker compromising Metro's technical infrastructure.

Where Do I Report Incidents?

In compliance with Metro policy, all Incidents must be reported as soon as you become aware by using one of these methods:

1. **Report directly to the appropriate Privacy Officer**
2. **Report anonymously to the HIPAA Compliance Office**



Reporting to the Privacy Officer

Metro Covered Entities	Designated Privacy Officer
Metro Public Health Department	Tonya Foreman, Medical/Vital Records
Metro Human Resources Department	Justin Stack, Human Resources Administrator
Nashville Fire Department	Joaquin Toon, Quality Improvement Commander
Metro Public Schools – Benefits Department	David Hines, Director of Health Benefits

IMMEDIATELY REPORT

Incidents or Potential Incidents involving PHI to the **HIPAA Compliance Office**

HIPAAComplianceOffice@Nashville.gov

(615) 880–1700

Are there Consequences for Reporting?

NO! Employees will not face any consequences for reporting incidents.

An Anti-Retaliation policy ensures personnel may not be punished or retaliated against for reporting a suspected violation of policies or an Incident.

However, a person who makes an improper report including knowingly making a false report or using reporting as a retaliation tool, may be subject to disciplinary action.

Question

Jennifer calls you and says, “I am not sure if we have a breach. I sent a box of CDs with **PHI** to a vendor. I don’t think the CDs had any protections like encryption or passwords. Also, the vendor is new. I am not sure we have a contract. Do I need to report this?”

Q: Does Jennifer need to report the situation?

A: Yes. Employees should report all suspected inappropriate disclosures to the HIPAA Compliance Office or the Privacy Officer.

Chapter Key Summary

HIPAA

- Threats to the integrity of PHI and ePHI may come from many sources.

HIPAA

- Always be vigilant when Protecting the Privacy and Security of PHI.

HIPAA

- Report any suspicious or negligent behavior to the HIPAA Compliance Office or the Privacy Officer.

HIPAA

- Metro enforces a strict Non-Retaliation Policy for reporting Incidents.

Chapter 8:
Consequences of Non-Compliance

Consequences of Non-Compliance

When PHI is disclosed or accessed by an unauthorized individual, Metro Nashville faces several consequences. A privacy related incident, or data breach, may result in various adverse actions, including:

Regulatory Action: Fines imposed by U.S. Human and Health Services Department, Office of Civil Rights.

Legal Action: Lawsuits from individuals whose information was disclosed.

Direct Financial Loss: Cost associated with providing credit-monitoring.

Indirect Financial Loss and Reputational Damage: Loss of public trust.

Monetary Fines

The U.S. Human and Health Services Department, Office of Civil Rights may fine Covered Entities, Business Associates, and Subcontractors responsible for a HIPAA violation. Several factors are taken into consideration when calculating these fines, such as:

- The number of persons affected by the violation
- The potential harm to reputations
- The expediency of response to the incident

Degree of Culpability / "State of Mind"	Potential Penalty Per Violation	Maximum for All Violations of Identical HIPAA Provision
Violation was not known and could not have been discovered with reasonable diligence	$100 - $50,000	$1,500,000
Reasonable cause for violation, not due to willful neglect	$1,000 - $50,000	$1,500,000
Violation due to willful neglect, but corrected in 30 days	$10,000 - $50,000	$1,500,000
Violation due to willful neglect, not corrected in 30 days	$50,000	$1,500,000

Sanctions

Sanctions are penalties imposed for disobeying laws or rules.

Metro may impose sanctions for violations of the HIPAA policies and procedures. All sanctions will follow normal Civil Service corrective/disciplinary action procedures (or departmental procedures for non-Civil Service employees).

Whistleblowers

Sanctions WILL NOT apply to disclosures made by employees who are whistleblowers or crime victims.

Employees are encouraged to report any unlawful or suspicious behaviors or practices to the HIPAA Compliance Office or applicable Privacy Officer.

Those who take actions based on a belief that their department has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that any services potentially endanger one or more patients, workers, or the public, will not receive disciplinary sanctions.

Everyone Must Comply with HIPAA!

There may be times where other departments may come in contact with PHI and Metro wants to ensure the same standards are applied.

Regardless of these classifications, it is everyone's responsibility to maintain HIPAA compliance and to protect health information within Metro. The cooperation of employees across all departments prevents Metro from facing serious legal, reputational and financial risks!

Question

Q: What are the risks of non-compliance?

A: Metro may face indirect and direct financial loss, legal action, adverse reputational impacts, or sanctions for non-compliance with HIPAA standards.

Chapter Key Summary

HIPAA

- Penalties for non-compliance are regulatory action, legal action, direct and indirect financial loss, and reputational damage.

HIPAA

- It is important that you ensure the confidentiality of PHI and ePHI, as applicable to the functions of your job.

HIPAA

- Always refer any and all questions or concerns related to HIPAA to the HIPAA Compliance Office or Privacy Officer.

HIPAA

- HIPAA imposes civil monetary penalties for non-compliance and violations of its outlined Rules and Regulations.