

The seal of the Metropolitan Government of Nashville and Davidson County is centered in the background. It features a central figure holding a scale and a sword, surrounded by a circular border with the text "METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY". The seal is topped with a fleur-de-lis and surrounded by a sunburst pattern.

HIPAA Refresher Training Program

Metro Government of Nashville and Davidson County
Metro HR Benefits (MHRB)

Table of Contents

Chapter 1: Introduction to HIPAA

Chapter 2: Privacy Rule

Chapter 3: Security Rule

Chapter 4: How to Identify and Report a HIPAA Violation

Chapter 5: Consequences of Non-Compliance



The seal of the Metropolitan Government of Nashville and Davidson County is centered in the background. It features a central figure, likely a personification of Justice or Liberty, holding a scale and a sword. The figure is surrounded by a circular border with the text "METROPOLITAN GOVERNMENT" at the top and "NASHVILLE AND DAVIDSON COUNTY" at the bottom. The seal is set against a starburst background.

Chapter 1: Introduction to HIPAA

Ch.1: Introduction to
HIPAA

Ch. 2: Privacy
Rule

Ch. 3: Security
Rule

Ch. 4: How to
Identify and
Report a HIPAA
Violation

Ch. 5:
Consequences of
Non-Compliance

Welcome to the HIPAA Refresher Training Program!

This HIPAA training is intended to provide Workforce Members of all levels with a basic understanding of the Privacy and Security Rules and how the Rules may affect their roles and responsibilities.

Why is HIPAA Compliance Important to MHRB?

- Transparency – Increases patient and plan participant trust and confidence.
- Accountability –Increases corporate goodwill.
- Reputation – Data breaches of patient information can be damaging in the eyes of the public, which could directly correlate to decreased funding from donors.

Completion of the refresher training is required at least once a year.



What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) is a federal law that was created to protect the security and privacy of patients’ and health plan participants’ protected health information (“PHI”).

The law was revised in 2009 with the passages of the “Health Information Technology for Economic and Clinical Health Act” (HITECH Act) and again in 2013 through the passage of the Final Omnibus Rule.

HIPAA’s primary goals:

- Establish a set of standards and requirements for protecting health information.
- Improve efficiency and effectiveness of the health care system.
- Guarantee individuals the right to access their health information.



What is PHI?

Protected Health Information (“PHI”) is any oral, electronic or paper record that contains any individually identifiable information as it 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.

Examples may include:

- Patient (or Plan Participant) name and treatment information.
- Billing information from a doctor.
- Patient’s appointment reminder with treatment alternatives.

Individually Identifiable Information	Health Information
Name	Prescription Information
Birth Date	Benefit Claim
Driver’s License	Medical Records
Address	Medical Condition
Phone Number	Medical Diagnosis



What is ePHI?

Electronic Protection Health Information (“ePHI”) is PHI that is created, stored, transmitted, or received electronically.

Examples may include:

- Medical insurance claims information
- Explanations of Benefits (EOBs) and medical providers’ bills
- Demographic information about a patient
- A digital photograph of a patient stored on a hard drive
- Patient names, procedures, and/or times on an electronic calendar



Who Must Comply with HIPAA?

Covered Entities include:



Health Care Providers

- Organizations that actively provide health services to patients and who electronically transmit health information in connection with certain transactions.
 - Ex: Doctors, clinics, laboratories, pharmacies



Health Plans

- Administrators of a health insurance plan that provide or pay the cost of medical care (e.g., health, dental, vision, HMOs, Medicare, etc.).
 - Ex: Health Insurance Companies, HMOs, Company Health Plans, Government Programs



Health Care Clearinghouses

- Organizations that receive health information from other parties in nonstandard formats and transform that data into a standard format for transmission to a final destination.



Who Must Comply with HIPAA?

HIPAA applies to **Business Associates**, which is any person or entity that performs functions, activities, or services on behalf of a Covered Entity in which the entity creates, receives, or transmits PHI.

Examples of Business Associates:

- Billing and collection agencies (including the Finance Department)
- Temporary or contracted employees hired from third party temp agencies
- Practice management companies
- Accountants
- Consultants
- Auditors
- Administrative services companies
- Similar service providers that receive, collect, analyze, maintain, review, or transmit PHI as the agent of, or on behalf of, a Metro Covered Entity.



Ch.1: Introduction to
HIPAA

Ch. 2: Privacy
Rule

Ch. 3: Security
Rule

Ch. 4: How to
Identify and
Report a HIPAA
Violation

Ch. 5:
Consequences of
Non-Compliance

HIPAA Breakdown

Privacy Rule – protects the privacy of individually identifiable health information.



- Individual Rights: Right to Notification, Right to Access, Right to Amend, Right to Restrict, Right to an Accounting of Disclosures, Right to Confidential Communications.
- Notice of Privacy Practices (“NPP”) provided to individuals.
- Rules for using and disclosing PHI collected from individuals (very DETAILED rules).
- Rules for protecting PHI in paper form.



Ch.1: Introduction to
HIPAA

Ch. 2: Privacy
Rule

Ch. 3: Security
Rule

Ch. 4: How to
Identify and
Report a HIPAA
Violation

Ch. 5:
Consequences of
Non-Compliance

HIPAA Breakdown

Security Rule – Sets national standards for the security of electronic protected health information.

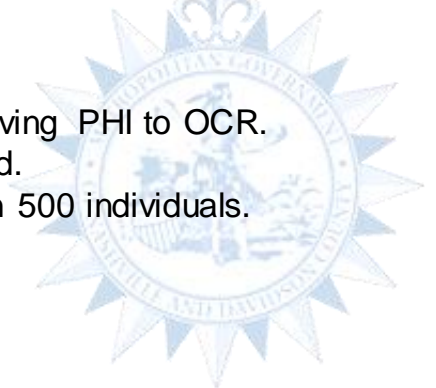


- Security mechanisms that must be in place for systems and applications maintaining electronic PHI (“ePHI”).
- Physical safeguards that must be in place to protect ePHI.
- Incident Response Plans.
- Information Security Training.

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

▪Think:

- Procedures that must be followed to identify and report incidents involving PHI to OCR.
- Procedures for notifying affected individuals when PHI is compromised.
- Procedures for notifying the media when the breach affects more than 500 individuals.





Chapter 2: Privacy Rule

Privacy Rule Requirements

The Privacy Rule includes the following key requirements that all Covered Entities must adhere to in order to comply with HIPAA:

- Designation of a Privacy Officer
- Privacy Policies and Procedures
- Notice of Privacy Practices
- Uses and Disclosure Limitations and Requirements
- Minimum Necessary Standard
- Individual Rights
- Business Associate Agreements



Patients' and Participants' Rights Under HIPAA

The Notice of Privacy Practices

Under HIPAA, individuals have the right to be provided a Notice of Privacy Practices (“NPP”). An 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.

Reminder:

- Individuals have the right to request a copy of the NPP and it may be provided electronically if requested.



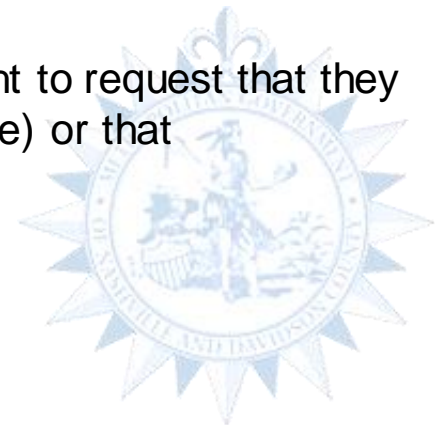
Patients' and Participants' Rights Under HIPAA

Right to Access: Individuals have the right to inspect and obtain electronic hard copies of their health records.

Right to an Accounting of Disclosures: Individuals have the right to request and receive a list (accounting) of each instance PHI was shared six years prior to the date of the request, the parties Metro Covered Entities disclosed this information to, and for what purpose.

Right to Amend PHI: Individuals have the right to request that PHI is corrected if PHI is incorrect or incomplete.

Right to Confidential Communications: Individuals have the right to request that they be contacted in a specific manner (i.e., home phone or office phone) or that communications be sent to a different address.



Patients' and Participants' Rights Under HIPAA

Right to File a HIPAA Complaint:

- Individuals have the right to file a HIPAA complaint with Metro Covered Entities and the Office for Civil Rights (OCR) if the individual believes his or her rights have been denied or that their PHI is or has been unprotected.
 - <https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html>
- The HIPAA Privacy Officer will promptly investigate and address the individual's concerns.



Minimum Necessary

The Privacy Rule requires that all uses, disclosures, and requests of PHI must be limited to the **“minimum necessary to accomplish the intended purpose”**.

How does the minimum necessary standard apply to Nashville?

- Employees should only use or disclose PHI with other employees who require the information in order to perform their job functions. Even in these circumstances, the amount of information shared must be limited to the minimum necessary.

There are certain situations in which the minimum necessary rule may not apply, including:

- When PHI is shared for treatment purposes.
- When speaking to an individual about their own health information.
- When disclosure to the Department of Health and Human Services (HHS) is required for enforcement purposes.
- When a law requires disclosure.



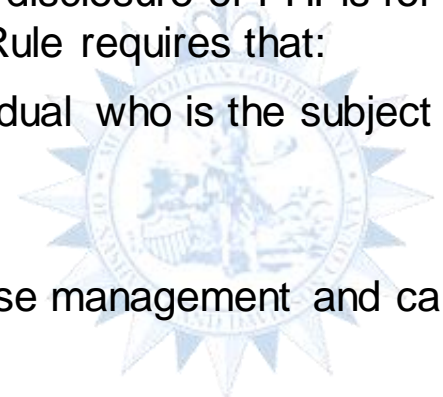
Use and Disclosure of PHI

HIPAA permits the uses and disclosures of PHI related to the following areas:

- ✓ **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 a quality assessment, administration, data management, or customer service.
- ✓ **Treatment:** To assist Healthcare Providers in diagnosis and treatment.

Does HIPAA permit one health plan to share PHI about individuals in common with a second health plan for care coordination purposes?

- Yes. A health plan may disclose PHI to another health plan if the disclosure of PHI is for the health care operations of the recipient health plan. The Privacy Rule requires that:
 - (i) each entity either has or had a relationship with the individual who is the subject of the PHI being requested,
 - (ii) the PHI pertains to that relationship, and
 - (iii) the disclosure is for a health care operation, such as case management and care coordination, as defined by HIPAA.
- All disclosures are still subject to the minimum necessary standard.



Ch.1: Introduction to
HIPAA

Ch. 2: Privacy
Rule

Ch. 3: Security
Rule

Ch. 4: How to
Identify and
Report a HIPAA
Violation

Ch. 5:
Consequences of
Non-Compliance

Business Associates

Under the Privacy Rule, Business Associates are held directly liable for complying the HIPAA regulations.

Items the Business Associates must perform include:

- ✓ Execute a **Business Associate Agreement** with Metro Covered Entities to provide assurances of their HIPAA safeguards that protect PHI.
- ✓ Obtain **satisfactory assurances** from their sub-contractors that they also have safeguards in place to protect Metro PHI.
- ✓ Notify Metro Covered Entities of any incidents or breaches involving any Metro Patient PHI.
- ✓ Ensuring that they do not engage in impermissible uses and disclosures of PHI.
- ✓ Adhering to the Minimum Necessary Standard.
- ✓ Recognizing individual rights under HIPAA.



Ch.1: Introduction to
HIPAA

Ch. 2: Privacy
Rule

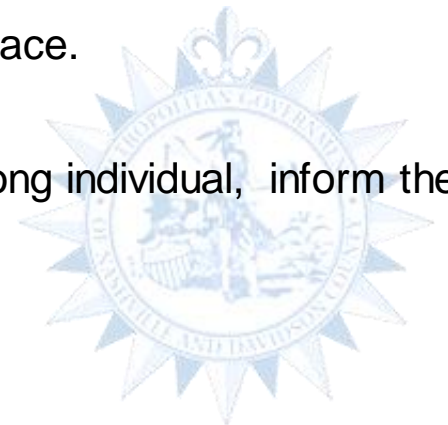
Ch. 3: Security
Rule

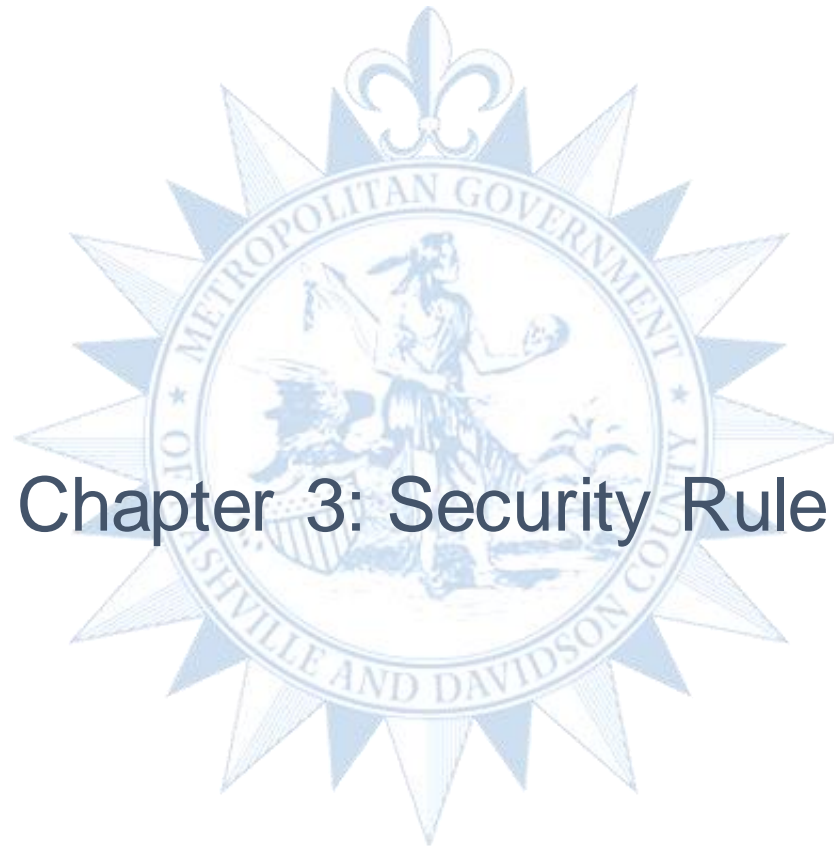
Ch. 4: How to
Identify and
Report a HIPAA
Violation

Ch. 5:
Consequences of
Non-Compliance

Remember

- ✓ Maintain an up-to-date Notice of Privacy Practices.
- ✓ Only use or disclose PHI with other employees who require the information in order to perform their job functions.
- ✓ The level of access to PHI should correspond with your title and job function. If you have access to PHI that you should not have, please escalate to your manager ASAP.
- ✓ Do not send PHI to third parties where required BAAs are not in place.
- ✓ Avoid sending PHI to the wrong individual. If PHI is sent to the wrong individual, inform the individual whose information was disclosed as soon as possible.





Chapter 3: Security Rule

Security Rule

The HIPAA Security Rule requires that Covered Entities and Business Associates have administrative, physical, and technical safeguards in place to protect electronic Protected Health Information (ePHI).

Administrative Safeguards

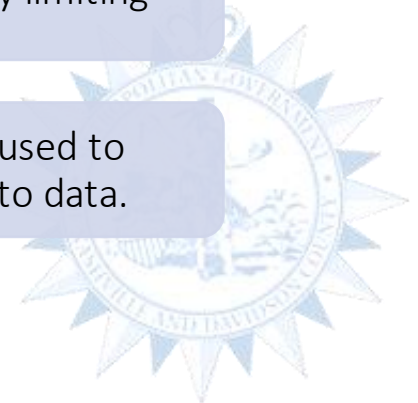
- Processes that safeguard ePHI and PHI through proper training and documented policies and procedures.

Physical Safeguards

- The physical safekeeping of electronic equipment, systems, and data by limiting physical access.

Technical Safeguards

- Automated technical processes used to protect data and control access to data.



Ch.1: Introduction to HIPAA

Ch. 2: Privacy Rule

Ch. 3: Security Rule

Ch. 4: How to Identify and Report a HIPAA Violation

Ch. 5: Consequences of Non-Compliance

Security Rule Standards

Administrative Safeguards

- Security Management Process
- Risk Analysis
- Sanctions
- IT Activity Review
- Security Officer
- Workforce Security
- Information Access Management
- Security Training
- Security Incident Process
- Contingency Plan
- Evaluation
- Business Associate Contracts

Physical Safeguards

- Facility Access Control
- Workstation Use
- Workstation Security
- Device & Media Control

Technical Safeguards

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security



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.

Administrative Safeguards to take note of include:

- ✓ Be aware of documented Policies and Procedures
 - The *MHRB HIPAA Policy and Procedures* are in place to safeguard ePHI.
- ✓ Ensure you've completed the HIPAA and Information Security Awareness Training
 - HIPAA Training is conducted annually and is required of all Metro employees that may have access to PHI or ePHI.
 - Training is a prerequisite for access to systems containing ePHI.
 - Remind co-workers of the importance of HIPAA and the policies and procedures supporting appropriate conduct.

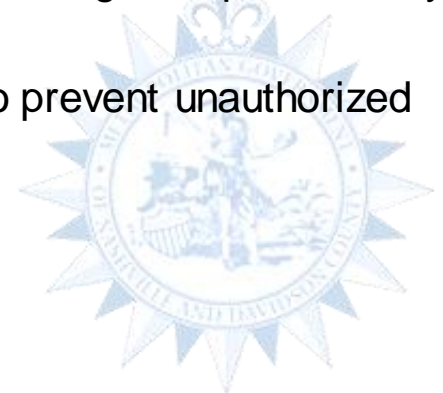


Physical Safeguards

Physical Safeguards protect Metro from unwanted physical access to areas where PHI is housed and stored.

Physical Safeguards to take note of:

- ✓ Ensure spaces and areas that contain PHI are locked and secure.
- ✓ File and store any hard copy PHI in locked file cabinets when not in use.
- ✓ Properly dispose of PHI via a shredder or secure shred bins - do NOT throw PHI in trash bins.
- ✓ Secure disposal of storage devices (e.g., USB flash drives, external hard drives, etc.)
- ✓ Do not allow others to borrow your identification badge or use their badges to permit entry for visitors.
- ✓ When stepping away from your computers, lock your computers to prevent unauthorized individuals from accessing or viewing PHI.

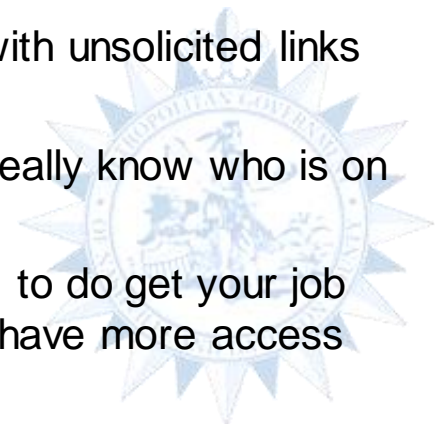


Technical Safeguards

Technical Safeguards protect Metro from unwanted access to its electronic PHI (ePHI)

Technical Safeguards to take note of:

- ✓ Do not share your ID and passwords to applications or systems containing PHI. This can allow unauthorized users to manipulate records under your account.
- ✓ Ensure to manually lock your computer; your auto logoff is your backup and not your primary method of ensuring your computer logs out!
- ✓ Always use the most secure means of transmitting information, to non-Metro parties.
- ✓ For example: using an SFTP instead of FTP, using encryption methods to send emails, including password protected files when necessary.
- ✓ Be very suspicious of emails from known or unknown senders with unsolicited links or attachments.
- ✓ Do not use email as a primary means to share PHI. You never really know who is on the other end of that email.
- ✓ Be proactive and honest about what information you really need to do get your job done. Let your managers or your IT team know if you think you have more access than you need.



Daily Activity Safeguards with HIPAA

FAX

- Use a Fax Cover Sheet with a confidentiality statement.
- Ensure Fax Cover Sheet does not include PHI.
- Double check 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.

MAIL

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

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 a "need-to-know" basis.
- Use "reply all" with caution.

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.



Complex Passwords

All Metro employees must use **Complex Passwords** that are at least 8 characters and include letters, digits, and punctuation.

Below are some helpful tips to help you create a strong password:

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!
Abcab	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!

Internet Usage

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:

- Accessing and using social media on Metro computers.
- Opening suspicious attachments or links within an email.
- Using the “reply all” function when unnecessary.

Additional Guidance

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

If any of your devices have PHI then YOU MUST notify ITS.



Ch.1: Introduction to HIPAA

Ch. 2: Privacy Rule

Ch. 3: Security Rule

Ch. 4: How to Identify and Report a HIPAA Violation

Ch. 5: Consequences of Non-Compliance

Ransomware

Ransomware is a type of software created for the malicious purpose of limiting access to systems or information, usually via encryption, until the attacker is paid a determined sum of money.

Money is often paid through a type of crypto-currency to prevent tracking of the criminals. Crypto-currency, like Bitcoin, is not backed by a central bank and is generated through the use of complex algorithms.

Ransomware can be delivered to your system by:

- **Phishing attacks:** a fraudulent email looking to be coming from an official source.
- **Drive-by Download:** a compromised website or software will automatically download without user consent.
- **Software:** downloading software for free off an unknown or unlicensed site may contain malware.
- **Social engineering:** prior infected computers may use email contacts to spread the infection further.

A ransomware attack may look like:





Chapter 4: How to Identify and Report a HIPAA Violation

What is the Difference between a BREACH and an INCIDENT?

An **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.



Security Incident Examples

The following events may lead to a breach of ePHI:

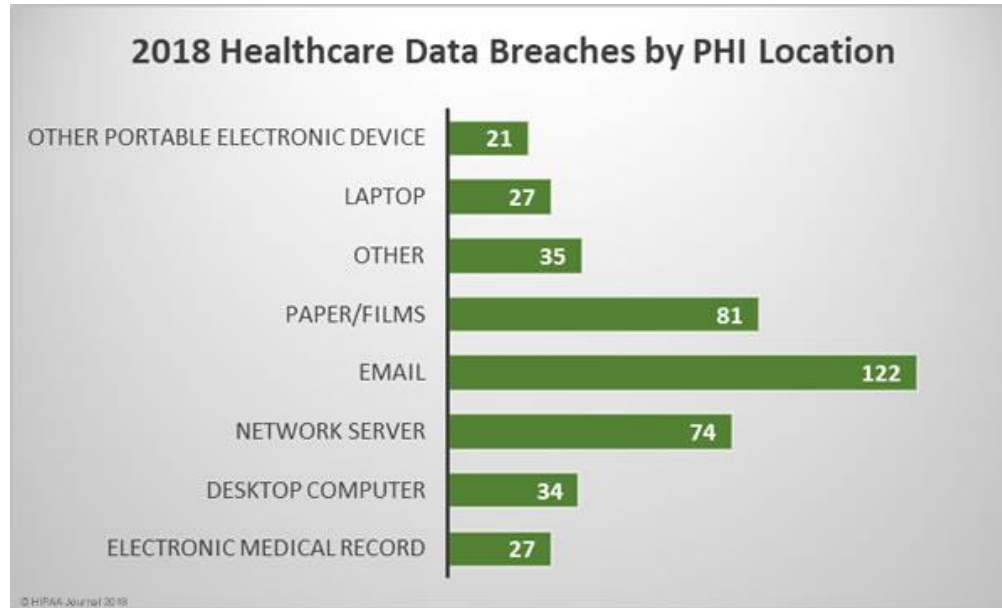
- Improper disposal
- Loss
- Theft
- Unauthorized access/disclosure
- Hacking/IT incident

The most common locations of breached PHI:

- Email
- Paper/films
- Network server
- Desktop computer
- Laptop
- EMR
- Portable electronic device



Security Incident Examples



Source: <https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/>

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 HIPAA Security or Privacy Officer
2. Report anonymously to the HIPAA Compliance Office



Reporting to the Security and Privacy Officer

Metro Business Associate	Designated Security Officer
Metro Information Technology Services	John Griffey, Chief Information Security Officer
Metro Covered Entities	Designated Privacy Officer
Metro Public Health Department	Tonya Foreman, Director, Medical/Vital Records
Metro Human Resources Department	Justin Stack, Human Resources Benefits Manager
Nashville Fire Department	Joaquin Toon, Assistant Chief, Quality Improvement Commander
Metro Public Schools – Benefits Department	David Hines, Director of Health Benefits

IMMEDIATELY REPORT

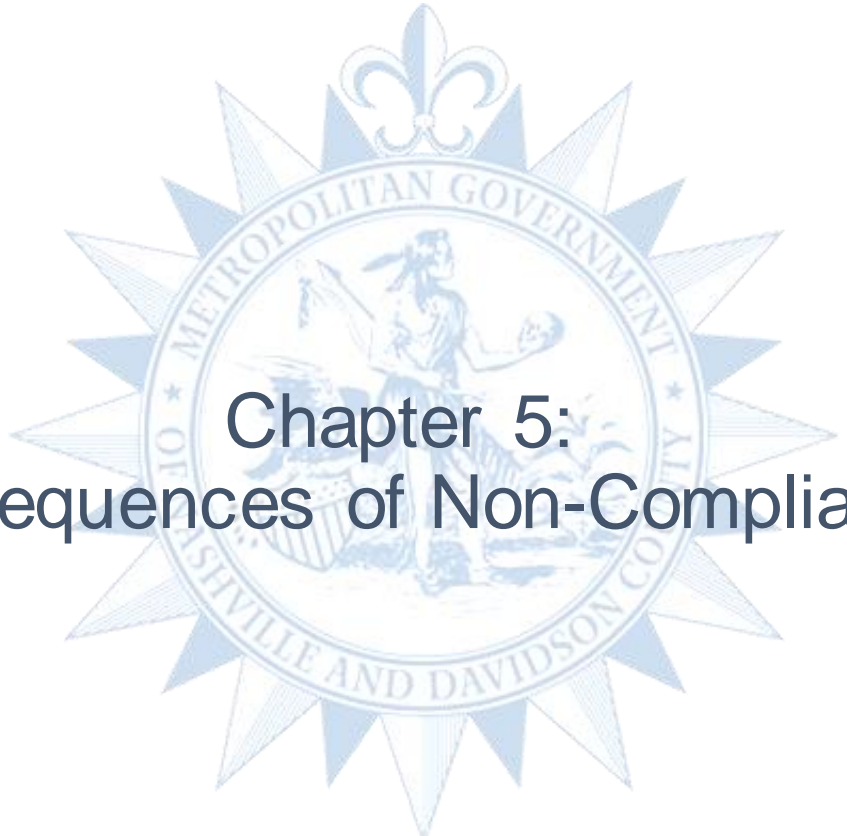
HIPAA Compliance Office

HIPAAComplianceOffice@Nashville.gov

(615) 880–1700

Employees will not face any consequences for reporting incidents.



The seal of the Metropolitan Government of Nashville and Davidson County, Tennessee, is centered in the background. It features a central figure holding a scale and a sword, surrounded by a circular border with the text "METROPOLITAN GOVERNMENT" and "NASHVILLE AND DAVIDSON COUNTY, TENNESSEE". The seal is topped with a fleur-de-lis and surrounded by a sunburst pattern.

Chapter 5: 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, Legal Actions = Direct Financial Loss

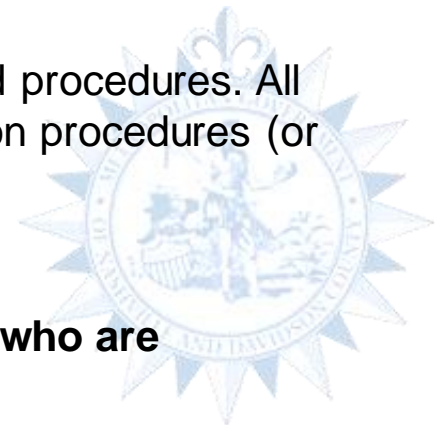
Indirect Financial Loss and Reputational Damage = Loss of Public Trust

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).

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



Consequences of Non-Compliance

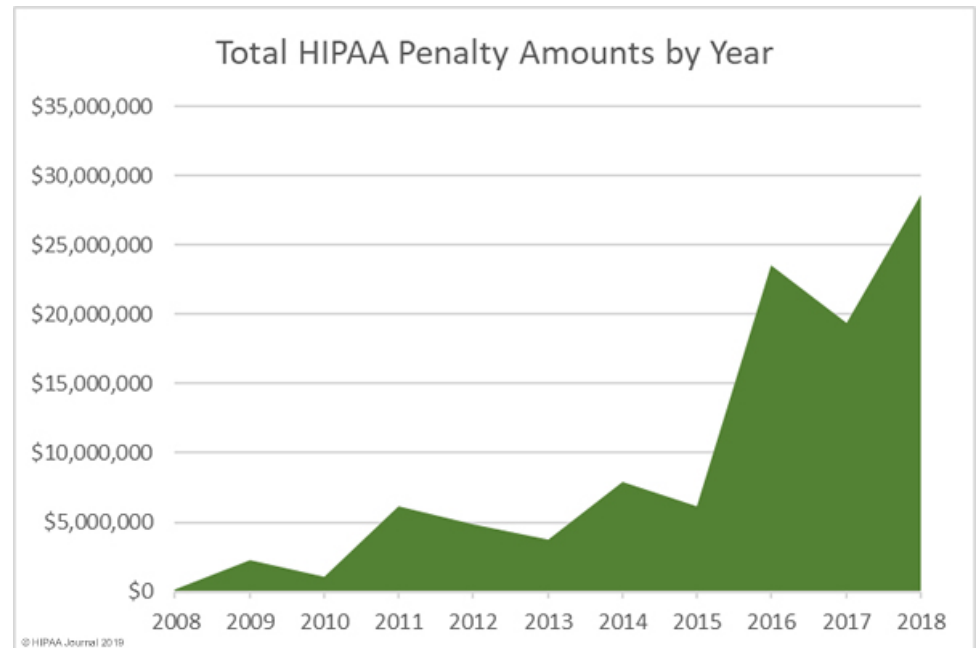
A privacy related incident, or data breach, may result in various adverse actions, including:

Direct Financial Loss

- Civil Penalties
 - Up to \$1.5 million per year per violation
- Criminal Penalties
 - Up to \$250k, imprisonment of up to 10 years, or both
- Lawsuits
 - Invasion of privacy/negligence

Indirect Financial Loss

- Reputational Damage – avoid the “Wall of Shame”
- Loss of Public Trust



Source: <https://www.hipaajournal.com/summary-2018-hipaa-fines-and-settlements/>



Why is Compliance Important?

- It's the law. HIPAA non-compliance continues to result in significant monetary fines and even jail time.
 - Data breach notification requirements are now much stricter.
 - State Attorney General can bring civil actions on behalf of their citizens.
 - The number of mandatory independent audits are greatly increasing.
- Patients, Plan Participants, and stakeholders trust to protect their information.



Federal and State Enforcement Actions

HHS (Federal) Civil Penalties

Violation Category - Section 160.404	Penalty Range for Each Violation	All Such Violations of an Identical Provision in a Calendar Year
(A) Reasonable Diligence (Did Not Know)	\$112 - \$55,910	\$1,677,299
(B) Reasonable Cause	\$1,118 - \$55,910	\$1,677,299
(C)(i) Willful Neglect – Corrected	\$11,182 - \$55,910	\$1,677,299
(C)(ii) Willful Neglect – Not Corrected	\$55,910	\$1,677,299

DOJ Criminal Penalties

Violation Category	Penalty Range for Each Violation
Knowingly obtaining PHI	Up to \$50,000 and one (1) year in prison
Committed under false pretenses	Up to \$100,000 and five (5) years in prison
Committed with the intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm	Up to \$250,000 and ten (10) years in prison



HIPAA Data Breach Costs

Outside of imposed fines from OCR and AG's Offices, what does a Breach cost?

- Costs incurred in breach:
 - ✓ \$ to engage expert consultants
 - ✓ \$ for implementation of security improvements
 - ✓ \$ for operational changes (e.g., update websites, customer service workflow, new systems)
 - ✓ \$ for breach notification letters by first class post (\$0.49) = 1 letter cost Anthem ~\$40M in postage alone
 - ✓ \$ to provide credit protection to breach impacted victims
 - ✓ \$ for class action lawsuits (~\$1,000 per victim)
 - ✓ \$ for lost business



Questions & Answers

