

# HIPAA Training

# What is HIPAA?

HIPAA (*Health Insurance Portability and Accountability Act*) is a federal law passed in 1996 and updated in 2013

HIPAA was expanded and strengthened by the HITECH Act (*Health Information Technology for Economic and Clinical Health*) in 2009

HIPAA and HITECH establish requirements for the privacy and security of *Protected Health Information (PHI)* and *electronic Protected Health Information (ePHI)*

# Privacy vs. Security

## Privacy Rule

- Establishes an individual's right to privacy of all Protected Health Information (PHI)

## Security Rule

- Additional requirements for safeguarding electronic Protected Health Information (e-PHI)

# Who Must Follow HIPAA Rules?

## Covered Entity

- Health plans
- Health care clearinghouses
- Healthcare providers and their staff

## Business Associate

- Parties that perform services involving PHI in support of the covered entity
  - Examples: IPAs, MSOs, certain vendors

# What is PHI?

## Protected Health Information (PHI):

- Identifies (or can be used to identify) a patient, living or deceased
- Relates to past, present, or future health conditions, treatments, or payment
- Is transmitted or maintained in any form (electronic, paper, or oral representation)

# Examples of PHI

Name

Address  
(street, city, zip,  
county, etc.)

Medicare ID  
Number

Any Date  
(birth, death,  
admit, discharge)

Telephone & Fax  
Numbers

E-mail Address

Social Security  
Number

Medical Records

Member ID  
Number

# Permitted Uses & Disclosures

PHI **MAY** be used or disclosed for:

- Treatment of the patient
- Payment of healthcare bills
- Business operations
- Disclosures required by law
- Public health & other governmental reporting

# Other Uses & Disclosures

**Subpoenas related to claims and medical records** should be referred to PDT Claims staff, who will engage PDT's third party liability recovery vendor.

**All other law enforcement requests, court orders, and subpoenas** should be immediately referred to the PDT CEO or Vice President of Finance.

**For any other uses and disclosures** of PHI outside of what is permitted or required by law, signed authorization from the patient (or patient's representative) is required.



# Minimum Necessary

PHI must not be used or disclosed in excess of the **minimum necessary** amount needed to meet regulatory or contractual requirements.

- Only access the **minimum necessary** amount of PHI needed to carry out your job duties.
  - Avoid viewing PHI out of curiosity or entertainment
  - Avoid accessing PHI of friends or family
- Information provided to external parties must also be restricted to the **minimum necessary** amount needed to carry out their duties.

# Individual Rights

Individuals have the right to...	How to uphold:
...copy, access, or grant access to PHI	<p>The request is required to be in writing.</p> <p>Request forms are available at P:\PDT Compliance.</p> <p>Requests are reviewed by the PDT Compliance Officer.</p>
...request an amendment to PHI	
...restrict the use or disclosure of PHI	
...request an accounting of disclosures	
...request alternative communication methods (also known as confidential communication)	<p>Update the <i>Member Alternate Contact Information</i> and <i>HIPAA Restriction Flag</i> in MedMC.</p>
...file a complaint about privacy violations	<p>Complaints of suspected or confirmed privacy violations should be referred to the PDT Compliance Officer.</p>

# Protecting PHI: DOs & DON'Ts

## To protect PHI, always:

- Use a fax cover sheet with a Confidentiality Statement
- Limit faxing to when information is urgently needed
- Send faxes from a secure (not public) fax machine
- Quickly remove faxes and copies from common areas
- Ensure PHI is locked away when not in use
- Turn PHI over on your desk for short periods away
- Dispose of PHI in a shredder bin (or shredder)
- Limit visitors and ensure facilities remain locked
- Discuss PHI in private areas using hushed tones

# Protecting PHI: DOs & DON'Ts

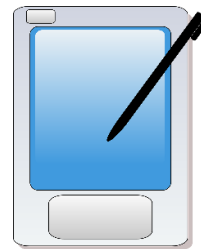
## To protect PHI, **never**:

- Fax information pertaining to:
  - Drug/alcohol dependency
  - Mental or psychological illness
  - Sexually-Transmitted Disease (STD)
  - HIV status
- Dispose of PHI in the trash
- Allow unauthorized visitors into areas containing PHI
- Remove PHI from PDT work locations
- Leave PHI on your desk during long periods away

# What is ePHI?

## Electronic Protected Health Information (ePHI):

- Identifies (or can be used to identify) a patient, living or deceased
- Relates to past, present, or future health conditions, treatments, or payment
- Is transmitted or maintained in **electronic** form



# Protecting ePHI: DOs & DON'Ts

## To protect ePHI, always:

- Add “PHI” to the subject line of an email containing ePHI
- Add “ZSECURE” to the email subject line to encrypt emails sent outside of PDT-managed email domains
  - *N/A for emails sent within PDT-managed domains*
- Lock your screen before leaving your workstation
- Report signs of compromise to IS immediately:
  - Slowness or freezing; missing data
  - Windows opening by themselves
  - Password is changed or account is locked
  - Settings have changed; unusual toolbars appear

# Protecting ePHI: DOs & DON'Ts

## To protect ePHI, never:

- Include patient information in the email subject line
- Click a link or download a file from a suspicious email
- Store PHI on smart phones or removable media (USB)
- Send PHI from your personal email address (Gmail, etc.)
- Share PHI in recorded Zoom meetings or on Monday.com
- Install software or applications without IS support
- Grant system access to external parties unless the request is in writing and was independently verified

# Protecting ePHI: Passwords

- Change default passwords immediately
- Use a unique password for each system or application
- Passwords must not be a dictionary word
- Passwords must not be stored in a readable format
- Avoid inserting passwords into email, text, or IM

Never use anyone else's login and password, or let someone else use yours. *You are responsible for what occurs while you are logged in.*



# Security Incidents

Security Incidents are defined by HIPAA as the *attempted* or *successful* unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**Phishing attacks** can be reported using the Phish Alert Button (PAB) in your Outlook toolbar.

**All other security incidents** must be immediately reported to the PDT Compliance Officer, or to your manager.

# Breaches

Breaches are defined by HIPAA as the impermissible acquisition, access, use, or disclosure of PHI with some probability that the PHI has been compromised.

**Potential breaches** must be immediately reported to the PDT Compliance Officer, or to your manager:

- PHI sent unsecured, unencrypted, or in the email subject line
- PHI sent to the wrong recipient, or sent by the wrong method
- Electronic device containing PHI is lost or stolen
- PHI is used or disclosed beyond the minimum necessary
- PHI is found in common areas or in the trash

# Reporting HIPAA Concerns

Issues and concerns related to HIPAA must be reported without delay to your manager or to the PDT Compliance Officer :

**Karen Palmer, CHC**  
**(562) 860-8771 x114**  
**Fax: (760) 631-7629**

[compliance@pdtrust.com](mailto:compliance@pdtrust.com)

Reporting is confidential, and reporting methods are available 24/7. Reports can be made anonymously. *There will be no retaliation for reporting in good faith.*

# Disciplinary Actions

Level & Definition of Violation	Action	Example
Accidental and/or due to lack of proper education	<ul style="list-style-type: none"> <li>• Re-training and re-evaluation</li> <li>• Oral warning with documented discussions of policy, procedures, and requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Improper disposal of PHI</li> <li>• Improper protection of PHI (leaving records on counters, leaving documents in inappropriate areas).</li> <li>• Not properly verifying individuals</li> <li>• Not following PDT policies</li> </ul>
Purposeful violation of privacy, or an unacceptable number of previous violations	<ul style="list-style-type: none"> <li>• Re-training and re-evaluation</li> <li>• Written warning with discussion of policy, procedures, and requirements</li> </ul>	<ul style="list-style-type: none"> <li>• Accessing or using PHI without have a legitimate need</li> <li>• Not forwarding appropriate information or requests to the Compliance Officer for processing</li> </ul>
Purposeful violation of privacy policy with associated potential for patient harm	<ul style="list-style-type: none"> <li>• Termination of employment or contract</li> </ul>	<ul style="list-style-type: none"> <li>• Unauthorized disclosure of PHI</li> <li>• Sale of PHI to any source</li> <li>• Any use or disclosure that could result in patient harm</li> <li>• <b>Failure to report incidents, breaches, or FWA</b></li> </ul>

# Civil Penalties

\$100 - \$50,000 per violation

- Unaware of the violation despite reasonable due diligence

\$1,000 - \$50,000 per violation

- Aware (or should have been aware) of the violation by exercising reasonable due diligence

\$10,000 - \$50,000 per violation

- Willful neglect of HIPAA Rules, and
- Violation corrected within 30 days of discovery

\$50,000 per violation

- Willful neglect of HIPAA Rules, but
- No effort made to correct the violation within 30 days of discovery

# Criminal Penalties



**Deliberately obtaining or disclosing PHI without authorization**

- Up to 1 year in jail
- \$50,000 fine

**Obtaining PHI under false pretenses**

- Up to 5 years in jail
- \$50,000 fine

**Obtaining PHI for personal gain or with malicious intent**

- Up to 10 years in jail
- \$250,000 fine

# Privacy/Security P&P

PDT maintains detailed policies and procedures to ensure patient privacy, information security, and ongoing HIPAA compliance.

Policies, procedures, and other resources are available on the PDT desktop, or by request to the PDT Compliance Officer:

**Karen Palmer, CHC**  
**(562) 860-8771 x114**  
**Fax: (760) 631-7629**  
**[compliance@pdtrust.com](mailto:compliance@pdtrust.com)**