PHYSICIANS DATA TRUST

HIPAA Training

PHYSICIANS DATA TRUST

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)

PHYSICIANS DATATRUST

Privacy Rule vs. Security Rule

Privacy Rule

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

Security Rule

- Requirements for safeguarding **electronic** Protected Health Information (e-PHI)

PHYSICIANS DATATRUST

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

PHYSICIANS DATATRUST

What is PHI?

Protected Health Information (PHI):

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

PHYSICIANS DATATRUST

Examples of PHI

Name	Address (street, city, zip, county, etc.)	Medicare ID / Member ID Number
Any Date (birth, death, admit, discharge)	Telephone & Fax Numbers	E-mail Address
Social Security Number	Medical Records / Referral Records	Encounter Data / Claims Data

PHYSICIANS DATA TRUST

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

PHYSICIANS DATATRUST

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.

PHYSICIANS DATATRUST

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.

PHYSICIANS DATATRUST

Individual Rights

Individuals have the right to…	How to uphold:
…copy, access, or grant access to PHI	The request is required to be in writing. Request forms are available at P:\PDT Compliance. Requests are reviewed by the PDT Compliance Officer.
…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)	Update the *Member Alternate Contact Information* and *HIPAA Restriction Flag* in MedMC.
…file a complaint about privacy violations, PDT's privacy/security practices, etc.	Complaints of this nature should be referred to the PDT Compliance Officer.

PHYSICIANS DATA TRUST

Working with PHI

DO:

- Ensure PHI is in locked storage for long periods away
- Turn PHI over on your desk for short periods away
- Quickly remove copies from common areas
- Dispose of PHI in a shredder bin (or shredder)
- Discuss PHI in private areas using hushed tones
- Confirm identity before disclosing PHI

DON'T:

- Allow unauthorized visitors into work areas
- Dispose of PHI in the trash
- Remove PHI from PDT work locations

PHYSICIANS DATA TRUST

Faxing PHI

DO:

- Limit faxing to when information is urgently needed
- Use a fax cover sheet with a Confidentiality Statement
- Send faxes from a secure (not public) fax machine
- Quickly remove faxes from common areas

DON'T:

- Fax information pertaining to:
  - Drug/alcohol dependency
  - Mental or psychological illness
  - Sexually-Transmitted Disease (STD)
  - HIV status

PHYSICIANS DATA TRUST

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




PHYSICIANS DATA TRUST

System Security

DO:

- Report signs of compromise to IS immediately:
  - Slowness or freezing; missing data
  - Windows opening by themselves; unusual toolbars appear
  - Password or settings have changed or account is locked

DON'T:

- Click a link or download a file from a suspicious email
- Install software or applications without IS support
- Grant system access to external parties, unless the request is in writing and was independently verified

PHYSICIANS DATATRUST

Passwords

DO:

- Change default passwords immediately
- Use a unique password for each system or application
- Use Microsoft Edge as a password manager
- Lock your screen before leaving your workstation

DON'T:

- Insert passwords into email, text, or IM
- Use dictionary words as passwords
- Store passwords in a readable format
- Use anyone else's account or let someone else use your account

PHYSICIANS DATA TRUST

Secure Storage

DO:

- Store PHI within the PDT desktop

DON'T:

- Store PHI outside of the PDT desktop (Google Drive, etc)
- Store PHI on smart phones or removable media (USB)
- Store PHI on Monday.com
- Share PHI in recorded Zoom meetings
- Upload PHI to Zoom

PHYSICIANS DATATRUST

Emailing ePHI

DO:

- Add “PHI” to the subject line to let the recipient know that the email message contains PHI
- Add “ZSECURE” to the subject line to encrypt emails
  - N/A for email addresses ending in @pdtrust.com, @stvincentipa.com, and @seasidemedicalgroup.net

DON’T:

- Include any patient information in the subject line
- Send PHI from your personal email address (Gmail, etc.)

PHYSICIANS DATATRUST

Security Incidents

Security Incidents are *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.

- Please let the security team know if you clicked any links or downloaded any attachments.

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

PHYSICIANS DATATRUST

Impermissible Use or Disclosure

Member privacy violations:

- Security incidents in which ePHI was exposed
- Saving ePHI to Monday, Zoom, or cloud storage
- Sending ePHI via text or personal email
- Accessing PHI beyond the minimum necessary
- Providing PHI to the wrong party in any form
  - Physical, mail, fax, email, SFTP, oral, etc.
  - Stolen records; stolen check detail

All instances of impermissible use or disclosure must be immediately reported to the PDT Compliance Officer, or to your manager.

PHYSICIANS DATA TRUST

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.

- *Each violation is assessed for PHI compromise*
- *Not all security incidents are breaches*
- *Not all impermissible uses/disclosures are breaches*

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

PHYSICIANS DATATRUST

Additional Risks

Other vulnerabilities:

- ePHI emailed to the correct party without encryption
- ePHI emailed to the correct party in the subject line
- Electronic device used for PDT business is lost or stolen
- PHI left unsecured, in common areas, or in the trash
- Interacting with a suspicious email message
- PDT, IPA, or provider website vulnerabilities
- **Noncompliance with PDT Privacy/Security policies**
- **Failure to report privacy and security concerns**

PHYSICIANS DATATRUST

Disciplinary Actions

Level & Definition of Violation	Action	Example
Accidental and/or due to lack of proper education	• Re-training and re-evaluation • Oral warning with documented discussions of policy, procedures, and requirements	• Improper disposal of PHI • Improper protection of PHI (leaving records on counters, leaving documents in inappropriate areas). • Not properly verifying individuals • Not following PDT policies
Purposeful violation of privacy, or an unacceptable number of previous violations	• Re-training and re-evaluation • Written warning with discussion of policy, procedures, and requirements	• Accessing or using PHI without have a legitimate need • Not forwarding appropriate information or requests to the Compliance Officer for processing
Purposeful violation of privacy policy with associated potential for patient harm	• Termination of employment or contract	• Unauthorized disclosure of PHI • Sale of PHI to any source • Any use or disclosure that could result in patient harm • **Failure to report incidents, breaches, or FWA**

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

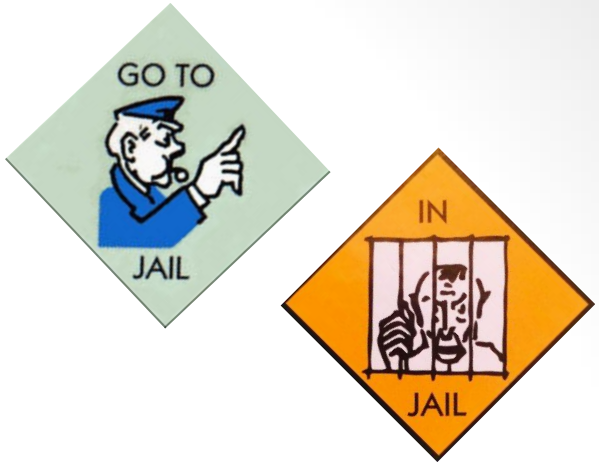
- Willful neglect of HIPAA Rules, and
- Violation corrected within 30 days of discovery

$50,000 per violation

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

PHYSICIANS DATATRUST

Criminal Penalties



Deliberately obtaining or disclosing PHI without authorization	Obtaining PHI under false pretenses	Obtaining PHI for personal gain or with malicious intent
• Up to 1 year in jail • $50,000 fine	• Up to 5 years in jail • $50,000 fine	• Up to 10 years in jail • $250,000 fine

PHYSICIANS DATATRUST

Reporting HIPAA Concerns

Issues and concerns related to privacy and/or security 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

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.*

PHYSICIANS DATATRUST

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

PHYSICIANS DATATRUST