PHYSICIANS DATATRUST

HIPAA Training

PHYSICIANS DATATRUST

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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Who Must Follow HIPAA Rules?

Covered Entity

- Health plans
- Healthcare clearinghouses
- Healthcare providers and staff

Business Associate

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

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

What is ePHI?

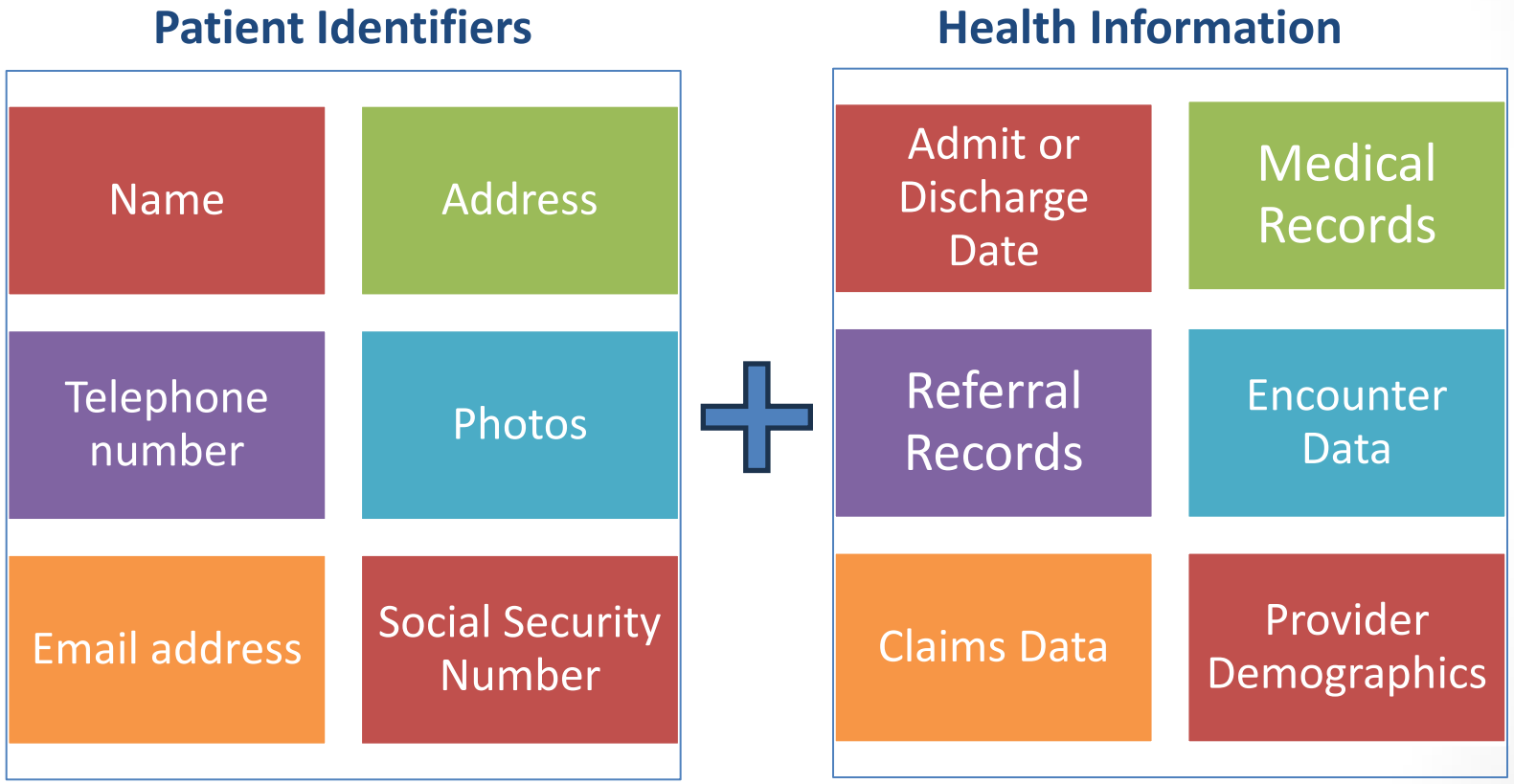
Electronic Protected Health Information (ePHI):

- PHI transmitted or maintained in electronic form

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Examples of PHI



Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

Minimum Necessary

PHI must not be used in excess of the **minimum necessary** amount needed to carry out your duties.

- Avoid viewing PHI out of curiosity or entertainment
- Avoid accessing PHI of friends or family

PHI must not be disclosed in excess of the **minimum necessary** amount needed for an external party to carry out their duties.

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Other Uses & Disclosures

Subpoenas related to claims and medical records should be referred to PDT Claims, 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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Impermissible Disclosures

Impermissible disclosures must be immediately reported to PDT Compliance, or to your manager.

- Accessing or sharing PHI beyond the minimum necessary
- Disclosing PHI to the wrong party in any form
  - Physical, mail, fax, email, SFTP, oral, etc.
  - Stolen physical PHI, e.g. check detail
- Security incidents in which ePHI was exposed

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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) or the INKY "Phish" button.

- Please advise if you clicked any links or attachments.

All other security incidents must be immediately reported to PDT Compliance, PDT IS/IT, or to your manager.

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

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.

- Not all instances are considered breaches
- Each instance is evaluated for PHI compromise

Confirmed breaches are reported to the affected individuals, the health plan, and the Department of Health and Human Services. Sometimes, reporting to law enforcement or the media is required.

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Disciplinary Actions

Level & Definition of Violation	Example	Action
Accidental and/or due to lack of proper education	• 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	• Re-training/education • Oral warning with documented discussions of policy, procedures, and requirements
Purposeful violation of privacy standards, or an unacceptable number of previous violations	• Accessing or using PHI without have a legitimate need • Not forwarding appropriate information or requests to the Compliance Officer for processing	• Re-training/education • Written warning with discussion of policy, procedures, and requirements
Purposeful violation of privacy standards with potential for patient harm	• Unauthorized disclosure of PHI • Sale of PHI to any source • Any use or disclosure that could result in patient harm • **Failure to report privacy and security concerns**	• Termination of employment or contract

Physicians Data Trust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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, and/or
- No effort made to correct the violation within 30 days of discovery

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

HIPAA in the News

- Snooping in Medical Records Leads to $240k Settlement
- $350k Settlement for PHI Disclosure on an Unsecured Server
- Health System Pays $1.04 Million for Stolen Laptop Breach
- Improper PHI disposal $300,640 settlement

PHYSICIANS DATA TRUST

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

Faxing PHI

DO:

- Limit faxing to when information is urgently needed
- Use a fax cover sheet with a Confidentiality Statement
- 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 DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

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
- Report immediately if your phone or laptop is lost or stolen

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 DATA TRUST

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

Emailing PHI

DO:

- Add “zsecure” to the subject line to encrypt emails
  - N/A for @pdtrust.com email addresses
  - N/A when the email does not include PHI

DON’T:

- Include patient information in the subject line

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST

Reporting HIPAA Concerns

Issues and concerns related to privacy and/or security must be reported without delay to your manager or to PDT Compliance:

Karen Palmer, CHC, CHPC
(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, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

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 PDT Compliance:

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

Physicians DataTrust, Inc. proprietary material. Consent for use of this material must be obtained prior to use. Inappropriate use of this material is prohibited

PHYSICIANS DATATRUST