



# HIPAA Privacy Training

# What is HIPAA?

**HIPAA** is the Health Insurance Portability and Accountability Act of 1996. One of the provisions under HIPAA is the regulation of health information privacy.

This presentation gives guidance for handling Protected Health Information (PHI) as addressed under the HIPAA Privacy Rule and the HIPAA Security Rule

# Who Must Comply?

Entities that must follow the HIPAA privacy and security rules are called *covered entities*. An employer is not a covered entity based on being an employer alone.

- An employer must comply if the employer sponsors an Employment Retirement Income Security Act (ERISA) group health plan.
- The group health plan is the covered entity, but the employer needs to comply with the HIPAA regulations as the plan sponsor and administrator.

# Other Restrictions on Use of Employee Health Information

- Be cautious – other laws may also restrict use of employee health (or other) information:
  - State privacy laws
  - FMLA
  - Americans With Disability Act (ADA)
  - Genetic Information Non-discrimination Act (GINA)
  - Mental Health Privacy Acts
  - State electronic disclosure acts (Social Security Numbers)

# What is the HIPAA Privacy Rule?

The HIPAA privacy rule gives an individual rights over how their health information may be used or disclosed and protects the unauthorized disclosure of *protected health information* (PHI).

It sets rules on who can view and receive participants' health information whether it is in an electronic, written or oral form. "Responsible employees" who have access to and/or handle PHI must comply with these rules.

The U.S. Department of Health and Human Services enforces the HIPAA privacy rule (<http://www.hhs.gov>).

# Definition of Responsible Employee

- An FRA employee whose duties:
- Require that the employee have access to PHI to perform administrative functions on behalf of the health plan
- Make it likely that he or she will receive or have access to PHI on behalf of the Health Plan

Any other FRA employee, not so designated, who creates, discloses, or receives PHI on behalf of the Health Plan is treated as a Responsible Employee under the Policy, even though his or her duties do not (or are not expected to) include creating, disclosing, or receiving PHI.

# What is Protected Health Information (PHI)?

PHI:

- Relates to the past, present or future physical or mental health condition of an individual, provision of health care to an individual, or payment for such health care
- Identifies or can be used to identify an individual (e.g. name, address, birth date, Social Security number, account number).
- Is in the possession of or has been created by *covered entities*.

# What is PHI? (continued)

PHI may be included in:

- Health care claims or encounter information.
- Health care payment and remittance advice.
- Coordination of benefits.
- Health care claim status.
- Enrollment or disenrollment in a health plan.
- Eligibility for a health plan.
- Health plan premium payments.
- Referral certification and authorization.

# Minimum Necessary Rule

- The Privacy Rule requires that we take reasonable steps to limit the use or disclosure of, and request for, protected health information to the ***minimum necessary*** to accomplish the intended purpose.

The minimum necessary standard applies in three circumstances:

1. When using PHI internally;
2. When disclosing PHI to an external party in response to a request (except for treatment-related disclosures)
3. When requesting PHI from another covered entity.

## Minimum Necessary Rule (continued)

- A Responsible Employee who engages in a transaction involving PHI is responsible for confirming that the transaction satisfies the minimum necessary requirement.
- In addition to limiting the PHI used or disclosed, a Responsible Employee must take steps to ensure that only the person needing the PHI for the intended purpose receives it.
- If a responsible Employee is the recipient of PHI, he or she should process, copy or record such PHI without disclosing it to others

# Determining Minimum Necessary

Criteria to consider when determining whether a proposed transaction involving PHI complies with the minimum necessary requirement:

- Is it necessary for payment or health care operations?
- Can the intended purpose be served adequately if fewer people were permitted access to the PHI?
- Can the intended purpose be served adequately if less PHI is used or disclosed?
- Does the method for transmitting the PHI reasonably ensure that it is received only by the intended recipient?

# Permitted Uses and Disclosures

No authorization is needed from the employee for:

- Payment activities
- Health care operations activities
- To the individual
- For workers' compensation purposes
- For certain public policy reasons

# Disclosures for Payment and Health Care Operations

## Health Care Operations

- General administration and design
- Quality assessment
- Obtaining legal and other services
- Plan audits
- Risk underwriting

## Payment

- Enrollment
- Assist employee with claim
- Determining eligibility and coverage
- Billing and claims management
- Pre-authorization (TPA)
- Utilization management
- Medical necessity (TPA)

# Authorization

- A proper authorization must:
  - Authorize you to disclose specific information
  - Be signed and dated
  - Include an expiration date or event
  - Still be valid (not revoked)
- Keep a copy of the authorization in the participant's benefit file for 6 years

# Privacy Physical Safeguards

Steps to take to safeguard physical PHI:

- Limit visitor access to facilities containing PHI/ePHI
- Do not let visitors travel unescorted through facilities
- Store PHI in a secure location (locked file cabinet or office)
- Never take materials containing PHI from the work site
- Remove physical PHI you may be using from view if another person enters your workspace
- Be mindful of who is copied on correspondence containing PHI that is sent via mail

## Physical PHI (continued)

- Take reasonable steps to ensure that incoming faxes and print jobs containing PHI are retrieved and viewed only by the Responsible Employee who is the intended recipient
- Print materials containing PHI to a secure printer requiring a badge swipe
- Before sending a fax that contains PHI, verify that the person receiving the fax is someone whom you are required, permitted, or authorized to disclose the PHI
- Destroy unneeded material

# Electronic Security

ePHI refers to PHI in electronic form, such as e-mail, databases and computer files containing PHI

## Steps to safeguard ePHI:

- Access to PHI in electronic form is restricted to Responsible Employees who need the access for their job duties
- Make sure that PHI displayed on your monitor is viewable only by you
- Prior to leaving your work area for a significant amount of time, close the window containing PHI and lock your computer (all computers or devices containing ePHI should have automatic time-out enabled)
- Watch “Reply All”
- Mobile devices used to access ePHI should be password protected

# Electronic Transmissions of PHI

A Responsible Employee who performs Electronic Transmissions as part of his or her job functions, may engage in such a transaction if the following conditions are met:

- PHI may be disclosed to a Business Associate (BA) or a Subcontractor and the BA may be allowed to create, receive, maintain or transmit PHI on behalf of the Health Plan, provided that there is a Business Associate Agreement in place.
- The Responsible Employee has received reasonable assurances that the intended recipient has appropriate control of and access to the computer(s) receiving the electronic transmission.

# Electronic Transmissions of PHI (continued)

Whenever possible an Electronic Transmission of PHI must meet the following criteria:

- When using open networks (*i.e.*, the internet or dial-in lines), the PHI should be encrypted before sending in order to avoid interception by parties other than the intended recipient
- For non-open networks, either access control (password protection) or encryption should be used to prevent parties other than the intended recipient from intercepting messages.

# E-mail Containing PHI

- All e-mail to an Individual should be sent to the e-mail account on record with the Health Plan or to the e-mail address specifically provided by the Individual.
- The Responsible Employee must take reasonable steps to verify the identity of the recipient before sending communications via e-mail.
- On outgoing e-mail that includes PHI, the Responsible Employee may not routinely copy other persons to whom an Individual directed his or her e-mail (whether as “cc” or directly). The Responsible Employee first must consider whether such persons copied on the original e-mail are authorized to receive the PHI

## E-mail Containing PHI (continued)

- A Responsible Employee must advise third parties to send e-mail containing PHI to a business e-mail account accessible only by the Responsible Employee (and such other Responsible Employees and Business Associate employees with a legitimate need to use or access such PHI in the performance of Health Plan functions).

# Verbal Communication of PHI

## Security for telephonic and other verbal communication of PHI

- Take reasonable steps to ensure that persons who do not have a legitimate need to know the content of the conversation do not overhear telephone and other verbal conversations in which PHI is discussed.
- Before engaging in a conversation in which you disclose PHI, take reasonable steps to verify that the other party on the line or present is a person to whom you are required, permitted or authorized to disclose PHI.
- When leaving a recorded message containing PHI, take reasonable steps to verify that the intended recipient is a person to whom you are required, permitted or authorized to disclose PHI and that the intended recipient has sole access to the answering machine.

# FRA HIPAA Privacy Policy

To comply with HIPAA, FRA must maintain a HIPAA Privacy Policy which addresses:

- The job functions at Fermilab that have reason to handle or access PHI
- The safeguards and practices for handling, transmitting and storing PHI
- How we ensure that all who handle PHI understand the safeguards and approved practices, and the consequences of not following the policy
- The sanctions that will be applied to those who violate the policy
- Designation of a Privacy Officer (Kay Van Vreede)

# Complaints and Policy Violations

- Complaints
  - To Benefits Department/Privacy Officer or Health and Human Services
  - Privacy Officer investigates
- Report Policy Violations
  - Promptly notify Privacy Officer (immediately upon discovery)
  - Mitigate harmful impact (may include notifying individual)
  - Cooperate with investigation
  - Prevent recurrence
- No retaliation or intimidation for complaints or reporting violations
- Privacy Officer
  - Must correct violation ASAP but no later than within 30 days
  - Must take immediate steps to mitigate any harm caused by violation

# Privacy Notice

- Automatically provide a copy to new participants at enrollment
- Current participants have been given a privacy notice
- Provide a copy to anyone upon request
- Provide notice of notice every 3 years
- Provide an updated notice if material changes

# Individual Rights Under HIPAA

- Right to inspect/copy PHI
- Right to request amendment to PHI
- Right to request restrictions on disclosure
  - Health plan is not required to comply with request
- Right to request confidential communications
- Accounting of disclosures
- Direct these requests to the Privacy Officer

# HIPAA Security Rule – Electronic PHI

Applies to all covered entities and their Business Associates that work with and transmit ePHI

Focuses on:

- Confidentiality – data or information is not made available to unauthorized persons or processes
- Integrity – data or information has not been altered or destroyed in an unauthorized manner
- Availability – data or information is accessible and useable upon demand only by an authorized person

# FRA HIPAA Security Policy

- Covered entities must create HIPAA Security Policies and Procedures
- Our HIPAA Security Policy addresses what electronic PHI we handle, and identifies the administrative, physical and technical safeguards we have in place to ensure security of this information
- Designates a Security Officer (currently Irwin Gaines)

# Difference between Secure and Unsecure PHI

- Unsecured PHI is PHI that is unencrypted
  - Must encrypt/destroy unsecured PHI to render it secured
- Secured PHI is:
  - Unusable
  - Unreadable or
  - Indecipherable to unauthorized individuals.
- Paper PHI:
  - Avoid printing EPHI when possible
  - Will be unsecured unless shredded or destroyed in a similar fashion
  - Shred documents in shredders
  - Encryption will render it secured
  - When possible – encrypt!

# HIPAA Security Rule Requirements

- Computers used for storing and transmitting ePHI must have protection from malicious software
- All FRA computers must have enabled virus scanning software that regularly updates such computers with security patches and virus signatures
- In the event a virus is detected, the Information Technology Department is immediately notified and the virus is immediately quarantined. Any infected hardware is manually isolated

# HIPAA Security Rule Requirements (continued)

- Log-in attempts must be monitored and discrepancies reported
- The Service Desk serves as the primary way to monitor log-in attempts. The Information Technology help desk will report discrepancies to the Laboratory Benefits Manager.
- Each system used must have safeguards for password management. Do not share your password with anyone.

# HIPAA Security Rule Requirements (continued)

- Employees with access to ePHI are required to sign a confidentiality agreement and acknowledge policies and procedures upon hire.
- Reminders of these policies and procedures should be sent to all Responsible Employees on a periodic basis to promote security awareness
- A Responsible Employee must complete security awareness training as soon as practicable after becoming a Responsible Employee and shall complete periodic training thereafter

# Security Incident Response and Reporting

- Security Incidents
  - Attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in the Plan's information system
- Examples
  - Someone uses your workstation with your password and without authorization
  - Viruses
  - Theft of workstation

REPORT ALL SECURITY INCIDENTS TO YOUR HIPAA SECURITY OR PRIVACY OFFICER

# Enforcing the HIPAA Security Policy

- The Security Official shall first investigate any violation of these Policies and Procedures and document the investigation efforts and findings.
- An investigation must include a meeting with the employee alleged to have violated these Policies and Procedures.
- Investigations of a violation of these Policies and Procedures will otherwise be handled in accordance with FRA's policies.
- Any sanctions imposed against an employee must be commensurate with the violation of these Policies and Procedures.

# Enforcing the HIPAA Security Policy (continued)

- Sanctions may include warnings, suspension or other disciplinary action, including termination of employment.
- The Security Official shall make the final determination of the appropriate sanction, taking into account any prior violations of these Policies and Procedures by the employee, the severity of the violation, length of service and the responsibility held by the employee.
- The sanction procedures and provisions of the Fermilab Policy on Computing and the Director's Policy on computing shall apply
- Employees must be informed of policies concerning sanctions for inappropriate access, use and disclosure of EPHI.

# Civil Enforcement

- HHS received over 87,000 complaints of HIPAA violations
- Office of Civil Rights has resolved 95% through
  - 21,000 via enforcement
  - 9,800 found no violation
  - 51,000 were not eligible for enforcement
- Most common issues (in order):
  - Impermissible uses and disclosures of PHI
  - Lack of safeguards for PHI
  - Uses and disclosures of more than minimum necessary PHI
  - Lack of administrative safeguards of electronic PHI

# End of Training Materials

**Please request the on line test through the TRAIN Database**