

HIPAA Privacy & Security Review

Betsy Porter, NYSUT Member Benefits Trust

1-800-626-8101, ext. 1247

May 2, 2008

Health Insurance Portability & Accountability Act of 1996

- **Portability** - 1996
- **EDI*** - October 2003
- **Privacy*** - April 2003/2004
- **Security*** - April 2005/2006

* Administrative Simplification
portion of HIPAA

What does Administrative Simplification mean?

- Standardizing transmission of health-related data
- Protecting personal medical information

Who does HIPAA apply to?

“Covered entities”

- Doctors
- Hospitals
- Insurance Companies
- Pharmacies
- Group Health Plans
- Third Party Administrators (TPAs)
(must comply but not a covered entity)

**Where do benefit
funds fit in?**

Under HIPAA:

Benefit Funds offering certain types of benefits are considered “**Group Health Plans.**”

Benefit Funds are considered “**Covered Entities.**”

HIPAA Covered Benefits

YES if:

- Medical and Health Insurance
- Dental
- Vision
- Hearing
- Catastrophe MM
- Long Term Care
- Prescription Drug
- IRS Sec 125
- Medical Reimbursements

NO if:

- Long or Short Term Disability
- Life Insurance
- AD&D
- Legal Service Plans
- Financial Counseling Programs

HIPAA Exceptions

- Group Health Plan with < 50 participants and is self-administered - Exempt from Administrative Simplification provisions
- Group Health Plans providing benefits solely through an insurance contract with a provider AND create/receive no PHI (just summary info.) - Not required to perform certain HIPAA tasks

Privacy Review

HIPAA Privacy Rule

The purpose of the Privacy Rule is to set national standards for the protection of health information. It requires Covered Entities to implement standards to protect and guard against the misuse of individually identifiable health information.

Privacy Review

Privacy rules apply to these areas:

- Treatment
- Payment
- Healthcare operations

Privacy Review

Treatment:

- The provision, coordination or management of health care and related services by one or more health care providers.
- Coordination of management of health care by a health care provider and a third party.
- Consultation or referrals between one health care provider and another.

Privacy Review

Payment:

Activities undertaken by a health plan or provider to obtain or provide reimbursement or premiums for the provision of health care.

- Determinations of eligibility or coverage
- Billing, claims management, collections
- Medical necessity reviews, utilization reviews

Privacy Review

Health Care Operations:

Certain services or activities necessary to carry out the covered functions of the covered entity related to treatment or payment.

- Auditing claims
- Resolution of internal plan grievances
- Legal services

Privacy Review

PHI – Protected Health Information

Information communicated by a covered entity orally, on paper or by electronic means that individually identifies and relates to an individual's (participant's, dependent's or retiree's) medical condition, provision of medical care, enrollment, premium payment, health status or treatment.

Privacy Review

Examples of PHI:

Personal information: Name, address, phone, fax, e-mail, social security number, etc.

Dates: Birth, death, eligibility, hospital admission and discharge, etc.

Records: Medical treatment, claims and payments for members and dependents, eligibility backup, etc.

Privacy Review

PHI General Rule:

Covered entities may not use or disclose Protected Health Information (PHI) without the participant's written authorization for purposes not related to treatment, payment, or health care operations.

Privacy Review

Minimum Necessary:

Benefit Funds must make reasonable efforts to limit using PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

De-Identification:

Funds may disclose PHI that has been de-identified. Funds will use de-identified information whenever possible.

Privacy Compliance To-Do List

- ___ Contact Member Benefits for materials & legal counsel for guidance
- ___ Reference HIPAA in Plan Documents
- ___ Reference HIPAA in contracts with providers and business associates (such as TPAs)
- ___ Certifications to Insurance Carriers & Group Health Plan (from Local Association)
- ___ Name Privacy Official
- ___ Issue Privacy Notice
- ___ Trustee & Staff Training
- ___ Create a Privacy Manual containing policies and procedures

Privacy Compliance

Reference HIPAA in Plan Documents

Acknowledge HIPAA compliance in
Declaration of Trust, Summary Plan
Description or Benefits Booklet

Privacy Compliance

Reference HIPAA in contracts with providers and business associates (such as TPAs)

- Benefit Fund and benefit/service provider acknowledge HIPAA compliance
- Business Associate Agreements

Privacy Compliance

Certifications to Insurance Carrier & Group Health Plan

Acknowledgement of HIPAA compliance from plan sponsor (Local Association) to insurance providers and group health plan (i.e., Benefit Fund)

Privacy Compliance

Name Privacy Official

- Administers Fund's Privacy Policies & Procedures
- Handles complaints & questions
- Document Official's name & contact info. in Privacy Notice
- Can be same as Security Official

Privacy Compliance

Issue Privacy Notice

- Notice provides Fund's acknowledgement of Privacy compliance, explains how Fund uses PHI & describes participants' privacy rights
- Provide to each participant
- Remember to provide to NEW participants
- Send reminder of Privacy Notice availability every 3 years – 4/2007 for small Funds

Privacy Compliance

Trustee & Staff Training

- Training presented by you
- Training on YOUR Fund's compliance measures and Policies & Procedures
- Document attendance on Training Certification form
- Remember to train new trustees/staff

Privacy Compliance

Create a Privacy Manual containing Policies and Procedures

- Includes:
 - Identity verification procedures
 - Administrative, Technical & Physical Safeguards you establish to protect PHI
 - Procedures related to authorizations and individual rights
 - Record retention policies
- Separate from HIPAA Security manual

**Any Privacy
Questions?**

Electronic Data Interchange (EDI)

- Standardization of electronically transmitted transactions involving health records
- Expensive & unrealistic for small Benefit Funds to do themselves
- Your business associates (e.g., TPAs) can handle for you
- Ensure Business Associate Agreements reflect their compliance with EDI

Security Review

HIPAA Security Rule

The purpose of the Security rule is to provide national standards for reasonable and appropriate administrative, physical and technical safeguards to protect CIA – the Confidentiality, Integrity and Availability of **electronic PHI**.

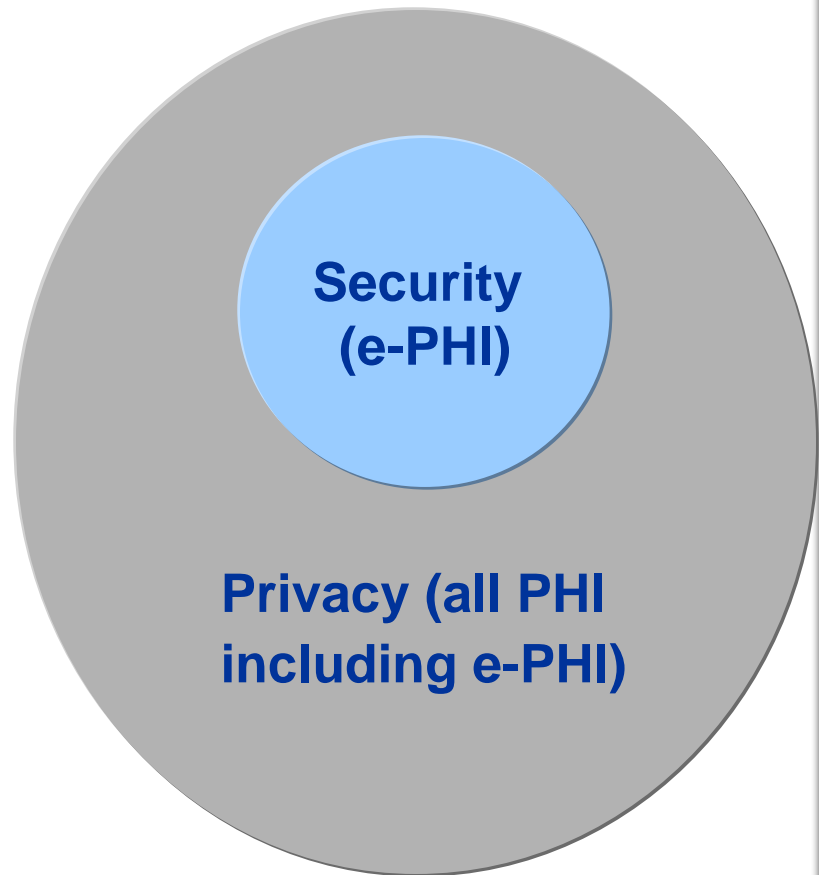
Security Review

Protection of CIA

- **Confidentiality** – Only the right people see the data
- **Integrity** – The information is what it is supposed to be; it hasn't changed
- **Availability** – The right people can see it when needed

Security Review

**HIPAA Security
rules require the
protection of
Electronic
Protected Health
Information (e-PHI)**



Security Review

What is Electronic PHI?

YES, if PHI is created, maintained or transmitted via:

- **CD or Disk**
- **E-Mail**
- **Internet**
- **Magnetic Tape**
- **Stored on a computer**
- **Private Network**
- **Leased Lines and Dial-up (Telephone lines)**

NO, if PHI is created, maintained or transmitted via:

- **Paper transactions**
- **Paper to paper faxes**
- **Person to person telephone**
- **Video Conferencing**
- **Voice Mail messages**

Security Review

The Risks are Real – Computers face:

- Unauthorized disclosure and theft of individuals' data
- Web site penetration
- Unauthorized data access
- Viruses or worms
- Human error
- <http://media.trendmicro.com/product/general/malware.html>

Security Review

Security Scope

Must implement basic safeguards to protect e-PHI from unauthorized access, alteration, deletion and transmission.

Security Review

Basic Protections

- Acceptable use policy
- Firewalls
- Virus scanning software
- Secure transfer of data
- Physical security of IT equipment
- E-mail encryption

Security Compliance To-Do List

- Contact Member Benefits for materials & legal counsel for guidance
- Conduct risk analysis & assessment
- Correct deficiencies identified during the analysis
- Create Security Policies & Procedures Manual
- Create a Business Continuity Plan
- Reference HIPAA Security in Plan Documents and in contracts with providers & Business Associates (e.g., TPAs)
- Name Security Official
- Trustee & Staff security awareness training

Security Compliance

Get familiar with the HIPAA Security Standards

- HHS web site has great series of papers called HIPAA Security Series (really!)
- Standards are required or addressable

Security Compliance

Conduct Risk Analysis & Assessment

- Refer to HIPAA Security Series #6: Basics of Risk Analysis & Risk Management
- Focus is to identify Assets (systems and infrastructure that contain or transport e-PHI); Threats (forces that could endanger assets); Vulnerabilities (weaknesses in current system)
- Document everything
- Correct deficiencies detected

Security Compliance

Create Security Policies & Procedures Manual

- Provides for documentation of your Fund's specific policies & procedures related to security of e-PHI
- Separate from HIPAA Privacy P&P manual

Security Compliance

Create a Business Continuity Plan

- Plan documented in Policies & Procedures Manual
- Emergency contact information
- Data retrieval procedures
- Alternate operations
- Resumption of business

Security Compliance

Reference HIPAA Security in Plan Documents and in contracts with providers & Business Associates (e.g., TPAs)

- Acknowledge HIPAA compliance in Declaration of Trust, Summary Plan Description or Benefits Booklet
- Benefit Fund and benefit/service provider acknowledge HIPAA compliance
- Business Associate Agreements

Security Compliance

Name Security Official

- Person most familiar with IT operations and procedures
- Can be same as Privacy Official
- Document official's name in Policies & Procedures

Security Compliance

Trustee & Staff security awareness training

- Training presented by YOU
- Training on YOUR fund's Security compliance measures and Policies & Procedures
- Document attendance via "Training Certification" form
- Remember to train new trustees/staff

**Any Security
Questions?**

Why comply?

- HIPAA Privacy & Security are federal regulations
- If audited, would be asked to prove compliance
- If complaint received by HHS, you'll be investigated
- Penalties exist for non-compliance

Noncompliance

Sanctions:

A Benefit Fund trustee or employee responsible for handling PHI will be sanctioned for violating HIPAA Privacy and/or Security policies and procedures.

The Privacy/Security Official will determine if the violation occurred, determine the severity and effect of violation and the sanction to be imposed.

Noncompliance

Sanctions:

Sanctions will include disciplinary action, up to and including dismissal from employment or removal from the Benefit Fund Board of Trustees (Regulations don't provide specific guidelines).

Civil Penalties:

\$100 per incident, up to \$25,000 per person, per year, per standard (HHS will assess).

Noncompliance

Criminal Penalties:

Criminal penalties will be imposed for covered entities that knowingly and improperly disclose or obtain information under false pretenses. These are enforced by the US Department of Justice.

Noncompliance

Criminal Penalties:

- Up to \$50,000 and one year in prison for obtaining and disclosing PHI.
- Up to \$100,000 and five years in prison for obtaining PHI under false pretenses.
- Up to \$250,000 and ten years in prison for obtaining and disclosing PHI with the intent to sell, transfer, or use it for commercial advantage, personal gain or malicious harm.

Helpful Web Sites

- **Health & Human Services Office of Civil Rights -**
www.hhs.gov/ocr/hipaa/
- **Centers for Medicaid & Medicare Services -**
www.cms.hhs.gov/hipaa/hipaa2

Questions?

Contact Member Benefits Trust at

1-800-626-8101

Betsy Porter: ext.1247 or
bporter@nysutmail.org

Laura Calhoun: ext. 1302 or
lcalhoun@nysutmail.org