



**DUKE UNIVERSITY
DUKE UNIVERSITY HEALTH SYSTEM**

Office of Internal Audits



Overview of HIPAA Privacy/Security

December 12, 2007

Presenters:

Valla Wilson, Internal Audit Director, Duke Medicine

Rosemary Herhold, IT Audit Senior, Duke University/Duke Medicine



AGENDA



- Overview of HIPAA Regulations
- HIPAA Privacy Rule Overview
- Key Contacts
- Duke Policies/Sanctions
- General Responsibilities
- HIPAA Security



WHAT DOES HIPAA STAND FOR?



Health

Insurance

Portability and

Accountability

Act



HIPAA OVERVIEW



- There are three components to HIPAA:
 - Standards for the Privacy of Individually Identifiable Health Information (Privacy Rule)
 - Standards for Electronic Security
 - Standards for Electronic Transactions and Code Sets
- This presentation will focus on the **HIPAA Privacy Rules and Standards for Electronic Security – The “Security Rule”**



WORKFORCE



- *Whether or not the covered entity pays them, a covered entity's workforce consists of:*
 - its employees (physicians, faculty, staff)
 - its volunteers
 - its trainees
 - other people under the direct control of the covered entity
 - Student interns
 - Contractors
 - Temporary employees



HIPAA PRIVACY

Standards for the Privacy of Health



PRIVACY STANDARDS FOR THE PRIVACY OF HEALTH



- Provides definitions
- Places limits on use and disclosure
- Specifies patients' rights
- Requires policies and procedures and systems such as:
 - Selecting a Privacy Officer
 - Providing training for the workforces
 - Setting sanctions for violations



WHERE IS HIPAA DATA?



- Health care entities
- Human resources
- Business associates
- Persons working from home
- Research
- Students



Health information means any information that:

- is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse
- relates to the past, present or future physical or mental health of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual
- includes:
 - medical records
 - claims information
 - payment information
 - almost all information related to a person's health care



PROTECTED HEALTH INFORMATION (PHI)



- PHI is any health information that could identify an individual patient, including
 - NAME, ADDRESS, or PHONE number
 - HEALTH INSURANCE number
 - SOCIAL SECURITY number
- Protected health information is all individually identifiable health information transmitted or maintained by a covered entity
- PHI is health information that is:
 - transmitted by electronic media
 - maintained in any electronic media
 - transmitted or maintained in any other form or medium
- PHI includes health information contained in a covered entity's records maintained in its health care capacity, but does not include employment records maintained by a covered entity in its capacity as an employer.



PATIENT IDENTIFIERS



Identifies?

- Medical Symptoms/Condition
- Patient's Name
- Street Address
- City/Town
- State
- Last TWO Digits of Zip code
- Year of Birth
- Social Security Number
- First THREE Digits of Zip Code
- Year of Admission
- Photograph
- Age, under 50
- Phone/Fax Number
- Year of Discharge
- Email, URL, IP address
- Date of Admission, Service
- Birthdate
- Drivers License

Doesn't Identify?



PATIENT IDENTIFIERS

Identifies

- Patient's Name
- Street Address
- City/Town
- Last TWO Digits of Zip code
- Social Security Number
- Photograph
- Phone/Fax Number
- Email, URL, IP address
- Date of Admission, Service
- Date of Birth
- Drivers License

Doesn't Identify

- Medical Symptoms/Condition
- State
- Age, under 50
- Year of Admission
- First THREE Digits of Zip Code
- Year of Discharge
- Year of Birth



HIPAA gives patients rights to:

- access, inspect and copy PHI
- request amendment of PHI
- receive accounting of disclosures
- request restrictions on disclosures
- have communications of PHI made at alternative locations or by alternative means



DISCLOSURE



- Disclosure is:
 - releasing, transferring, providing access to or divulging Individually Identifiable Health Information (IIHI) in any manner, to anyone outside the entity that maintains the IIHI
- IIHI is any part of health information that:
 - is created or received by a health care provider, health plan, employer, or health care clearinghouse
 - relates to the past, present or future
 - physical or mental health or condition of an individual
 - provision of care to an individual
 - payment for the provision of health care to an individual
 - identifies the individual (or there is a reason to believe that the information can be used to identify the individual)



An accounting of disclosures includes:

- the date of each disclosure
- who received the PHI
- if known, the addresses
- a brief description of the PHI disclosed
- a brief statement of the purpose of the disclosure



EXCEPTIONS TO THE RIGHT FOR AN ACCOUNTING FOR DISCLOSURES



A patient does not have the right to an accounting if the disclosures were:

- For treatment, payment, or health care operations based on a patient's signed authorization,
- incidental, or
- part of a limited data set



Health care operations include any of the following activities of the covered entity or organized health care arrangement:

- conducting quality assessment and improvement activities
- reviewing the competence or qualifications of healthcare professionals, evaluating plan performance, training of non-healthcare professionals, accreditation, certification, licensing or credentialing activities
- conducting or arranging for medical review, legal services, and auditing functions (including fraud and abuse detection and compliance programs)
- business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity
- business management and general administrative activities of the entity



WHAT IS A BUSINESS ASSOCIATE?

- Business associates are companies or people that provide services to a provider. A business associate might also perform, or assist with the performance of, some activity the provider needs done.
- PHI may be disclosed to business associates without patient authorization if there is a HIPAA-compliant, written contract
- Employees are not considered business associates and do not need written BA contracts
- Exceptions:

The business associate standard does not apply to disclosures:

- for treatment purposes
- to a plan sponsor by a group health plan
- between a public benefits program health plan and another agency for a government program



MINIMUM NECESSARY INFORMATION

- **Minimum necessary information** = the minimum amount needed to do the task required
- The Minimum Necessary standard does not apply to:
 - Uses and disclosures required by law
 - Disclosures made to the individual or as a result of the authorization of the individual
 - Disclosures to or requests by a health care provider for treatment purposes
 - Uses or disclosures that are required for compliance with the regulations that implement the other Administrative Simplification provisions of HIPAA
- Covered entities must limit requests to other covered entities for PHI to what is reasonably necessary for the use or disclosure intended
- Covered entities are responsible for developing policies and procedures that define the "minimum necessary" PHI that is needed for the tasks they routinely perform.



DE-IDENTIFIED INFORMATION

- Health information is considered **de-identified** when it does not identify an individual, and the covered entity has no reasonable basis to believe that the information can be used to identify an individual
- De-identify when:
 - Disclosure is not for treatment, payment or health care operations
 - None of the exceptions apply for getting authorization
 - Authorization either can't be obtained or there is a reason not to obtain it
- The Privacy Rule provides two possible ways for health information to be de-identified:
 - by applying generally accepted statistical and scientific principles and methods
 - by removing a list of identifiers from the health information



USE AND DISCLOSURE FOR RESEARCH

- HIPAA authorization requirements apply to research uses and disclosures of PHI
- May deny research related treatment if subject refuses signing an authorization for the research
- May *not* deny treatment that is unrelated research if the patient refuses signing an authorization
- Research authorization may be combined with an informed consent to participate in the research study, another authorization, or any other legal permission related to the research
- No blanket authorizations to cover future, unspecified research are allowed
- Each use or disclosure of PHI for research purposes requires authorization



IRB AUTHORIZATION WAIVERS

- IRB or Privacy Board may waive authorization requirement
- 3 criteria for waiver:
 - no more than minimal risk to the privacy of the individual;
 - can not reasonably be conducted without the waiver; and
 - can not reasonably be conducted without access to the PHI
- For waiver approval there must be:
 - plan to protect identifiers from improper use or disclosure;
 - plan to destroy identifiers at earliest opportunity; and
 - written assurance that PHI will not be used or disclosed to a third party



RESEARCH SUBJECTS RIGHTS

- An accounting of disclosures is required when a patient requests it for research disclosures obtained under one of the following circumstances:
 - an IRB or Privacy Board waiver of authorization; or
 - one of the two research exceptions to the authorization requirements applies; or
 - review is preparatory to research; or
 - research is on decedents
- Accounting only needs to include:
 - A name
 - All research protocols or activities under which the individual's PHI may have been disclosed
 - A brief description of the type of PHI disclosed
 - The date or time period in which disclosure might have occurred
 - The name and contact information of the researcher receiving the disclosure
- No accounting is required for disclosures contained in a limited data set



RESEARCH SUBJECT RECRUITMENT

- Recruitment is classified as "research" in the Privacy Rule
- Development or use of research databases falls within the definition of "research"
- Authorization or waiver is required to disclose PHI in a database to sponsors for subject recruitment
- Authorization or waiver is not required to disclose PHI contained in a limited data set
- Limitations on the use of PHI by a recipient of a limited data set for subject recruitment:
 - the PHI may not be used to contact subjects
 - telephone numbers, internet provider addresses, and email addresses are not part of a limited data set and may not be collected from prospective subjects by interactive websites advertising clinical trials



Resources Available to Help You When You Have A HIPAA Compliance Question or Concern or Need to Inquire About Training

- Colleen Shannon , DUHS Chief Compliance Officer/HIPAA Privacy Officer: 668-2573
- The Duke Health Enterprise Privacy Hotline: 800-688-1867
- DUHS Corporate Compliance Department Main Number : 668-2573
- The Compliance Hotline: 800-826-8109
- Tina Tyson, School of Medicine Chief Compliance Officer: 668-0679
- SOM HIPAA Compliance questions: 684-1883
- Joan Podleski, Duke University Institutional Ethics and Compliance Director: 613-7627



Confidentiality Policy includes sanctions for violations

Three levels of Sanctions for violations:

- Level 1 – Carelessness – reveals confidential information without a legitimate need to know reason.
 - Corrective action: Ranges from First offense - counseling to Fourth Offense - Termination
- Level 2 – Intentional and unauthorized accessing of confidential information – accesses for other than authorized purposes
 - Corrective action: First offense – Final written warning with a two-week unpaid suspension and Second offense - Termination
- Level 3 – Intentional and unauthorized disclosure of confidential information – accesses and discloses information without required authorization.
 - Corrective action: Termination



OUR RESPONSIBILITIES FOR HIPAA PRIVACY COMPLIANCE



- Responsibilities for protection
 - Only access and share information on a “job related need to know” basis.
- Covering information and discarding documents properly
- Not taking PHI home and limiting access
- Be careful not to share information concerning patients or research subjects to others
- Always remember that we show that we “care” by respecting privacy rights. This applies to:
 - Employees as patients
 - Family members
 - Church family
 - Neighbors
 - Local celebrities/people in the news



OUR RESPONSIBILITIES FOR HIPAA PRIVACY COMPLIANCE *Continued*



- Identifying those who may have access to PHI and will need HIPAA Training
- Report when you are aware of anyone disclosing information inappropriately
- Become familiar with HIPAA Privacy policies
- Make an inquiry to authority person when you have questions or concerns



DUKE UNIVERSITY
DUKE UNIVERSITY HEALTH SYSTEM



Office of Internal Audits

HIPAA Security Rule

An Introduction



Agenda

- What is the Security Rule?
- Do the Privacy Rule and the Security Rule Overlap?
- How is HIPAA compliance documented in Duke Medicine?



Security Rule Structure

- Three safeguards and two requirements
- Eighteen standards
- Forty-one implementation specifications



- What is the difference between “required” and “addressable” implementation specifications?



Administrative Safeguards



- Comprise $\frac{1}{2}$ of the security rule
- Managing the conduct of employees with ePHI
- Assessing the risks and managing risk through controls
- Documented policies and procedures are required.



Administrative Safeguards Standards



- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts and Other Arrangements



Physical Safeguards



- Controlling physical access to ePHI stored on hardware and media
- ePHI stored on workstations, in facilities, and on a flash drive
- Physical safeguards require documented policies and procedures.



Physical Safeguards Standards



- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls



Technical Safeguards

- Focus of the technical safeguards is protecting ePHI through use of technology.
- Documented policies and procedures are required.



- Access Controls
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security



Security Rule Structure

- Three safeguards and two requirements
- Eighteen standards
- Forty-one implementation specifications



Business Associate Contracts



- Responsibility does not end because there is a contract.
- Covered entities should be careful with whom they contract.
- Depending upon circumstances, covered entities are required to notify the Secretary of Health and Human Services if their business associate does not maintain the requirements of the Security Rule.



- Any changes to these policies must be documented.
- All documentation must be kept on file for 6 years.
- All policies and procedures implemented to safeguard ePHI must be documented.



Privacy and Security Rule Overlap

- The Privacy Rule and Security Rule are part of the same federal act.
- Privacy Rule: “.....a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”
- Ongoing training is required in both rules.
- It makes sense that people charged with governance in Privacy and Security communicate and coordinate with each other.



Information System Operations Plan (ISOP)



- ISOP tool is part of Duke Health's governance process.
- Continually updated and improved.
- Used to document HIPAA compliance for information systems.

HEALTH SYSTEM Information Security Office

www.iso.duke.edu

Plan Sum Help

Goal: Select a method to satisfy each requirement for a given system by clicking on the corresponding M link. The methods r system should be blank when done.

Requirement Filter:

	Print	All	Management				Operational						AC			
			CA	PL	RA	SA	AT	CM	CP	IR	MA	MP		PE	PS	SI
%	Methods Remaining	49	1	1	1	1	2	4	5	1		1	2	2	3	8
ail	Certification Remaining	49	1	1	1	1	2	4	5	1		1	2	2	3	8

	Method	Certification
cedures that establish the rules for granting and modifying access ...		
o information and resources unless authorized ...		
ion procedures ...		
ill be attributable to an individual (user accounts) ...		
f changes to access rights (adds, changes, and deletes) ...		
he login attacks- Automatically disable account ...		
an one account with administrator authority ...		
at an unattended, logged-in system is vulnerable to unauthorized use ...		
	Total: 8	



Thank you for listening.



Questions???



- Presenters' Contact Information:

Valla.Wilson@duke.edu

Rosemary.Herhold@duke.edu

- Sign In Sheet
- CPE Certificates