

HIPAA SECURITY, PRIVACY, AND THE NATIONAL PROVIDER IDENTIFIER

Frederick Britten

Fort Hays State University

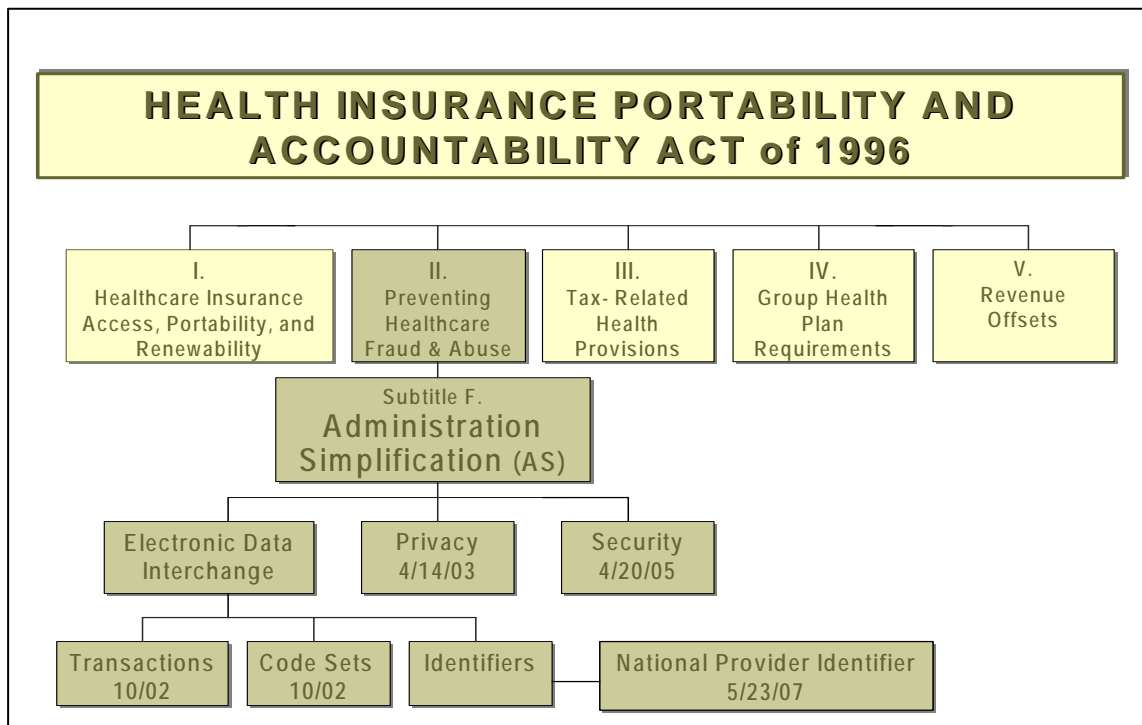
Carol Ann Raymond

The University of Georgia

Outline

- HIPAA Review
- Enforcement Update
- National Provider Identifier
- Security Rule
- Compliance Process
- Handouts and Resources

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT of 1996



HIPAA Legislation - Key Provisions

I	Healthcare Insurance Access, Portability, and Renewability	Improves the portability of insurance when changing job by limiting preexisting condition exclusions
II	Preventing Health Care Fraud and Abuse Subtitle F: Administration Simplification	<ul style="list-style-type: none"> Establishes health care fraud and abuse programs Establishes regulations for electronic data, privacy, security
III	Tax-Related Health Provisions	<ul style="list-style-type: none"> Allows employees to set up medical savings accounts exempted from taxation Provides for long-term care provisions
IV	Enforcement of Group Health Care Requirements	<ul style="list-style-type: none"> Specifies coverage for preexisting conditions and continuation of coverage
V	Revenue Offsets	<ul style="list-style-type: none"> Relates to company-owned life insurance plan deductions Revises provisions concerning loss of US citizenship for income tax purposes

Who Must Comply?

- **Covered Entities (CE)**
 - **Healthcare providers** who transmit any health information in electronic form
 - Insurance claims, eligibility, etc.
 - Health plans
 - Clearinghouses
- **Business Associates**
 - Services provided on behalf of the covered entity, involving the use or disclosure of protected health information (PHI)
 - Must sign agreement to comply with HIPAA
 - Consultants, accreditation agencies, vendors, etc.

HIPAA Enforcement

- **Administration Simplification Violations:**
 - **Civil Penalties (Health and Human Services)**
 - Up to \$100/per violation, up to \$25,000 per calendar year for identical violations

- **Criminal Penalties (Department of Justice)**
 - Knowing misuse of PHI: up to \$50,000 and/or up to one year imprisonment
 - “Under false pretences”: up to \$100,000 and/or up to five years imprisonment
 - Personal gain/malicious harm: up to \$250,000 and/or up to 10 years imprisonment

Civil Penalties

- HIPAA Administration Simplification: Enforcement; Final Rule (45 CFR Parts 160 and 164)
 - Published February 16, 2006
 - Effective March 16, 2006
- Covers enforcement process
 - Primarily complaint-driven
 - May also be by compliance review
- **Over 16,000 privacy complaints filed as of 10-31-05**

Civil Penalties

- CE is liable for a violation by workforce members acting within the scope of the agency
 - Includes employees, students, volunteers
 - Training programs and students included in HIPAA Privacy Rule under healthcare operations
- May not be imposed if failure to comply was
 - Due to reasonable cause and
 - Not due to willful neglect and
 - Is corrected within a certain time

National Provider Identifier

- A NEW identifier known as the NPI.
- Unique health identifier for health care providers.
- Designed to improve the efficiency and effectiveness of the health care system and is a part of the HIPAA legislation.

NPI Overview

- Compliance Date: May 23, 2007

- Providers and health plans must use only NPI to identify providers in standard EDI transactions.
- NPIs can also be used on paper transactions
- 10 positions (9 plus the check-digit)
- All numeric
- Only a number. NO IMBEDDED INTELLIGENCE

- Who can have an NPI?
 - Any health care provider. If EDI exists, there must be a NPI.
 - Health care providers are individuals (human) and organizations (non-human)
 - Entities, such as billing services, do not qualify as a provider and will not be able to obtain an NPI.
 - Numbers will be assigned for LIFE.

- An NPI will not:
 - Guarantee reimbursement by health plans
 - Enroll providers in health plans
 - Make providers covered entities
 - Require providers to conduct electronic transactions

National Provider Identifier System

- Information about **individuals** will include:
 - Required: name, gender, mailing address, location address, taxonomy codes, date of birth, state/country of birth, contact person's name/telephone
 - Situational: License number(s)/State(s). Required for certain taxonomy codes
 - Optional: SSN/ITIN, name prefix/suffix, other name(s), credential(s), other identifiers

- Information about **organizations** will include:
 - Required: Name, mailing address, location address, telephone number, taxonomy code, authorized official's name/telephone, contact person's name/telephone.
 - Situational: EIN (if provider has one), License number required for certain taxonomy codes
 - Optional: other names/identifiers

How is an NPI obtained?

- Provider completes application form to apply for an NPI.
 - Can file electronically or on paper
 - Application is processed by NPS
 - Data Editing
 - Data Validation
 - Duplicate application detection

- Provider receives notification of NPI

Provider Requirements

- May begin applying for NPIs on May 23, 2005
- Must begin using by May 23, 2007
- Must notify NPS enumerator within 30 days of any changes to the application
- Must disclose NPI when requested
- Require business associates to use NPI
- There is NO REQUIREMENT for providers who do not use electronic transactions

Benefits of the NPI

- No longer necessary to use different identifiers for different health plans, contracts, locations.
- Each organization determines how many NPIs they will need
- Will need the information if providers are going to get paid.
- Health plans must use the NPIs
- It will replace other identifiers such as UPIN, BCBS, Medicaid, CHAMPUS, etc.
- Same NPI for all health plans

Implications

- Talk to your payers to see when they will be ready to accept NPIs. DO NOT USE THEM UNTIL THEY ARE READY.
- See: <http://cms.hhs.gov/providers/npj> for the Medicare schedule
- Allow for time to insure NPI is setup is accurate and timely reimbursement

Ways to Apply for NPI

- Web-based application
 - <https://nppes.cms.hhs.gov>
 - Mail
 - Obtain a copy at <http://www.cms/hhs.gov/forms/cms10114.pdf>
 - Call: 1-800-465-3203 or TTY 1-800-692-2326 or
 - E-mail: customerservice@npienumerator.com
 - Mail to: NPI Enumerator, PO Box 6059, Fargo, ND 58108-6059

Privacy Rule

- Limits the availability and use of Protected Health Information (PHI)
 - Electronic, paper, and oral information
- Requires administrative, physical, & technical safeguards
- Enforced by Office of Civil Rights (OCR)

Security Rule

- Limits access to PHI in electronic format (E PHI)
 - ePHI that is created, received, maintained, or transmitted

- Requires administrative, physical, & technical safeguards
 - More specific than in Privacy Rule
- Enforced by Center for Medicare & Medicaid Services (CMS)
 - Office of HIPAA Standards (OHS)
- Covers all electronic PHI (E PHI), whether it is being stored or transmitted
- Requires implementation of appropriate administrative, technical, and physical safeguards for E PHI
- Is technology neutral - what to do, not how
- Is scalable and flexible - takes into account:
 - Size, complexity and capabilities of the entity
 - Technical infrastructure, hardware, and software security capabilities
 - Costs of security measures
 - Probability and criticality of potential risks

Security Standards: General Rules

160.306(a)

- (1) Must ensure the **confidentiality, integrity, and availability** of E PHI
 - **Confidentiality** – Information is available or disclosed only to authorized persons
 - **Integrity** – Information is not altered or destroyed in an unauthorized manner
 - **Availability** – Information can be accessed by an authorized person
- (2) Must protect against any **reasonably** anticipated threats or hazards to the security or integrity of E PHI
- (3) Must protect against any **reasonably** anticipated uses or disclosures that are not permitted by privacy rules
- (4) Must ensure compliance with workforce

Specifications

- **Required**
 - Standard must be implemented as stated
- **Addressable (not optional)**
 - Assess whether each specification is reasonable and appropriate for its environment to protect E PHI.
 - If reasonable and appropriate - Implement as stated
 - If not reasonable and appropriate,
 - Document rationale and implement an equivalent alternative measure, if reasonable and appropriate

Safeguard Categories

- **Administrative Safeguards** 45 CFR164.308

- Actions, policies, and procedures to protect EPHI and to manage the conduct of the workforce
- **Physical Safeguards** 45 CFR 164.310
 - Physical measures, policies and procedures to protect electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion
- **Technical Safeguards** 45 CFR 164.312
 - Automated processes to protect data and control access

Compliance Process

- Privacy and Security Committee
 - Develop Review Schedule
 - Assign Compliance Responsibilities
 - Reviews, Audits, Updates, Training
 - Complete Compliance Processes
 - Maintain Records

Administrative Safeguards

- Risk Analysis (R)
 - Identify threats, vulnerabilities, security controls
- Risk Management (R)
 - Identify, control, minimize, or eliminate security risks
- Workforce Security (A)
 - Authorization and supervision, clearance, termination
- Security Awareness and Training
 - Initial (all new students, employees, volunteers)
 - Maintain records for 6 years
- Security Reminders (A)
 - Periodic security updates
 - Maintain documentation of updates
- Protection from Malicious Software (A)
 - Guard against, detect, report malicious software
 - Viruses, worms, spy ware
 - Pornographic computer files
- Log-in Monitoring (A)
 - Monitor Log-in attempts
- Password Management (A)
 - Procedures to create, change, safeguard passwords
 - No sharing or posting, change on regular basis, terminate with employee

- Strong passwords

Evaluation (R)

- Perform a periodic technical and non-technical evaluation
 - Review and maintain reasonable and appropriate security measures
 - Complete periodic evaluations in response to environmental or operational changes
 - Annually or every two years

Tools

- Risk assessment forms
- Security Access Log (UGA)
- Protected Information (PI) User Inventory (UGA)
- Privacy and Security Site Review (UGA)
- Training Program

Physical Safeguards

- Facility Security (A)
 - Locked doors, keys, signs
 - Visitor escorts in areas with PHI/EPHI
 - Personnel badges, visitor identification badges
 - Workforce awareness of strangers or unusual activity
- Access Control and Validation (A)
 - Control and validate access based on job function

Physical Safeguards

- Workstation Use (R)
 - Restrict access to authorized users
 - Identify all workstations that access ePHI
 - On-site and off-campus controls
 - Proper use of workstation
 - Secure / confidential placement
 - Screensavers
 - Log in and off (whenever leave workstation/auto log-off)
 - Virus protection software
 - Use and update regularly
- Workstation Security (R)
 - Restrict access to authorized users
 - Identify all workstations that access EPHI
 - Desktop, Laptop (type data, physical security)
 - Personal Digital Assistants (PDAs)
- Device and Media Controls
 - Disposal (R)
 - Overwrite, degauss, destroy

- Electronic Media Re-use (R)
 - Overwrite, degauss, destroy
- Accountability (A)
 - Who has data / where
- Data Backup and Storage (A)

Tools

- NIST Guidelines for Media Sanitization (800-88)
- Security Access Log (UGA)
- Protected Information (PI) User Inventory (UGA)
- Security Site Review (UGA)
- Training Program

Technical Safeguards

- Access Control
 - Unique User Identification (R)
 - Unique login names for each user
 - Identify and track users
 - No group user IDs permitted
 - Automatic Logoff (A)
 - Unattended terminals
- Audit Controls (R)
 - User activity in information systems with EPHI
 - Who has read, accessed, or changed a file
 - Notification of abnormal conditions
 - Intrusion detection, firewalls
- Integrity (A)
 - EPHI not altered or destroyed in unauthorized manner
- Person or Entity Authentication (R)
 - Verify that a person or entity seeking access to EPHI is the one claimed
 - Password protection, keys, biometrics

Tools

- Audits
- Security Access Log (UGA)
- Protected Information (PI) User Inventory (UGA)
- Security Site Review (UGA)
- Training Program

Infusion into the Curriculum

- Information about HIPAA Privacy, Security, and the NPI should be incorporated into the existing academic curriculum of programs.

- Suggested courses where it might fit:
 - Professional Issues
 - Clinical Topics
 - Professional Practices in SLP and Audiology
 - Special Seminar

- More and more externships are requiring students to have this information before they begin.

References

- **HIPAA Final Enforcement Rule**
 - <http://www.hhs.gov/ocr/hipaa/FinalEnforcementRule06.pdf>
- **HIPAA Security Rule**
 - <http://www.cms.hhs.gov/SecurityStandard/>
 - <http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>
- **National Institute of Standards and Technology (2006, February).** *NIST Special Publication 800-88. Draft Guidelines for Media Sanitization.* US Department of Commerce. Retrieved January 21, 2006, from <http://csrc.nist.gov/publications/nistpubs/index.html>

Resources

- **ASHA Information**
 - <http://www.asha.org/about/legislation-advocacy/federal/hipaa>
- **CMS/OHS HIPAA Information**
 - <http://www.cms.hhs.gov/HIPAAGenInfo/>
 - Email questions to CMS askhipaa@cms.hhs.gov
 - CMS HIPAA Hotline 1-866-282-0659, TTY 877-326-1166
- **HIPAA Privacy Rule (Office for Civil Rights)**
 - <http://www.hhs.gov/ocr/hipaa/finalreg.html>
 - OCR Guidance (significant aspects of the Privacy Rule):
 - <http://www.hhs.gov/ocr/hipaa/privacy.html>
- **Medicaid and Medicare**
 - <http://www.cms.hhs.gov/HIPAAGenInfo/>
- **Microsoft. Strong passwords: How to create and use them.**
 - <http://www.microsoft.com/athome/security/privacy/password.msp>
- **National Provider Identification**
 - <http://www.cms.hhs.gov/NationalProvIdentStand>
 - <http://www.cms.hhs.gov/NationalProvIdentStand/Downloads/NPIFactSheet012606.pdf>
- **Phoenix Health Systems** <http://www.hipaadvisory.com/>
- **Policies**
 - **CAL HIPAA** <http://www.calhipaa.com>
- **Security Series (6 HHS Papers)**
 - <http://www.cms.hhs.gov/EducationMaterials/Downloads/Basics.pdf>
- **Transactions and Code Sets**

- <http://www.cms.hhs.gov/TransactionCodeSetsStands/>
- **UGA College of Education Security**
 - <http://www.coe.uga.edu/security/>
- **UGA /USG HIPAA**
 - <http://www.infosec.uga.edu/policymanagement/hipaa.php>
 - <http://www.usg.edu/legal/hipaa/policies.phtml>

Resources – Handouts

- Disclosure Log (FHSU)
- Privacy and Security Site Review (UGA)
- Protected Information User Inventory (UGA)
- Security Access Log (UGA)
- Security Policy (FHSU)

For more information, contact:

Fred Britten
Professor/Director of Audiology
Fort Hays State University
103G Albertson, Hays, Kansas 67601
785.628.4451
fbritten@fhsu.edu

Carol Ann Raymond
Director, UGA Speech and Hearing Clinic
The University of Georgia
528 Aderhold Hall, Athens, GA 30602
706.542.4559
raymond1@uga.edu