



HIPAA Privacy and Security Rules: What's Important to Know to Protect Your Patients, Yourself, and Your Institution

Debra Duncan, BSBA
ECU HIPAA Privacy Specialist
Compliance Administrative Specialist
The Brody School of Medicine



Overview

- Background and General Information
- Use and Disclosure of Protected Health Information
- Patients Rights under HIPAA
- HIPAA and Research
- ECU HIPAA Privacy Violation Levels and Sanctions
- Penalties under HIPAA
- 2009 American Recovery and Reinvestment Act
- HI-TECH Act
- ECU Security Rule Basics



Background and General Information

- Health Insurance Portability and Accountability Act – HIPAA
 - How did privacy and security rules result from a law relating to health insurance portability?
 - HIPAA implemented insurance portability rules and “administrative simplification rules”
 - Administrative simplification rules: Uniform transactions related to health information
 - Congress felt that additional privacy and security protections were necessary once transmission of health claims and other health information became uniform and electronic



Background and General Information (Cont'd)

- HIPAA Privacy rules
- In general, were effective April 14, 2003
- Federal law which established a minimum level of privacy protections related to “protected health information” (PHI)
- Prior to HIPAA privacy rules, state law governed confidentiality of patient information
- State laws that are “more stringent” than HIPAA will “preempt” or override HIPAA privacy rules



Background and General Information (Cont'd)

- **HIPAA Security Rules**
 - In general, were effective April 14, 2005
- **Ensure confidentiality, integrity, and availability of “electronic” PHI**
- **Provide for rules related to technical, physical, and administrative safeguards for ePHI (e.g., use of computer workstations, software, encryption standards, etc.**



Background and General Information (Cont'd)

- What is Protected Health Information?
 - Information that is created or received by the covered entity;
 - Relates to past, present or future physical or mental health or condition of the individual, or related to payment for health care; and
 - Identifies the individual or provides a reasonable basis to be used to identify the individual
- Can be in any form: Verbal, written or electronic



Background and General Information (Cont'd)

- PHI is very broad: Includes all personal demographic and health information related to patients in any form
- Examples of PHI:
 - Name, address, birth date, social security number, driver's license number, telephone number
 - Billing records, appointment information, research information
 - Medical records, diagnostic reports, lab results, prescriptions, etc.



Background and General Information (Cont'd)

■ Notice of Privacy Practices (NPP)

- ECU is required to provide each patient with its Notice of Privacy Practices
- Written acknowledgement required except in emergency situations, but should be obtained as soon as possible
- Explains how the institution may use and disclose PHI and discusses the patient's rights under HIPAA
- Patient must receive a copy
- Notice posted in English and Spanish on the ECU HIPAA website at <http://www.ecu.edu/cs-dhs/hipaa/index.cfm>



Background and General Information (Cont'd)

■ Training

- All workforce members must receive annual HIPAA Training to protect the privacy and security of individually identifiable health information.
- Healthcare computer system administrators must attend additional training due to the HIPAA Security Rule regulations; contact your manager for details. Visit Computer Safety and Security on the ITCS website at www.ecu.edu/cs-itcs for more information and new security alerts



Use and Disclosure of PHI

- General Rule: HIPAA authorization required for any use or disclosure of PHI
- Broad exception for “treatment, payment or health care operations”
- “Treatment”
 - Providing information to other providers involved in the care of the patient (e.g., other nurses, doctors, lab personnel, etc.)
 - Does NOT allow for disclosure of psychotherapy notes and other types of sensitive conditions (i.e., HIV status); separate consent required to release that type of information



Use and Disclosure of PHI (Cont'd)

- “Payment”
 - Submission of claims for services to third party payors
 - Collection activities
- “Health care operations”
 - Using and disclosing PHI for quality assurance reviews, internal auditing, peer review, outside lawyers, accountants, etc.



Use and Disclosure of PHI (Cont'd)

- “Business associate agreement” necessary for outside entities or individuals who are performing services on behalf of ECU or who are performing auditing, legal, or consulting services for ECU
 - Holds the outside entity or individual to the same requirements as ECU



Use and Disclosure of PHI (Cont'd)

- Other Examples of Exceptions to the Authorization Requirement
 - Law enforcement purposes
 - Judicial and administrative proceedings (per court order or subpoena)
 - Health oversight agencies (e.g., HHS)
 - Certain public health activities (e.g., CDC, public health departments, tracking of FDA recalls, reporting of adverse events during research)



Use and Disclosure of PHI (Cont'd)

Providers should obtain a general consent to use and disclose PHI prior to providing services.

- A copy shall be retained in the patient's medical record.
- A new form should be initiated and signed annually.



Use and Disclosure of PHI (Cont'd)

- A HIPAA authorization is a special type of authorization; not the same as the general consent for treatment
- Must be in writing and include specified elements; patient must receive a copy and the patient is permitted to revoke authorization at any time in writing



Use and Disclosure of PHI (Cont'd)

- Typical uses of a HIPAA authorization
 - Research at a covered entity
 - Patient's request to release PHI to an outside entity or individual
 - Release of employment-related examination information
 - Psychotherapy notes and other sensitive conditions
 - Certain fundraising or marketing activities (that are not exempt from the authorization requirement)



Use and Disclosure of PHI (Cont'd)

- Disclosure of PHI to Patient's Family and Others Involved in Care
 - May disclose PHI directly relevant to such person's involvement in the care
 - May disclose PHI to notify a family member, a personal representative or others involved in the patient's care of the patient's location, general condition, or death.
- If the patient is present you must first:
 - Obtain the patient's agreement to involve family members or others
 - Provide the patient with the opportunity to object; or
 - "Reasonably infer from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure"



Use and Disclosure of PHI (Cont'd)

- Disclosure of PHI to Patient's Family and Others Involved in Care: If patient is not present or otherwise incapacitated
 - Provider or covered entity may, “in the exercise of professional judgment,” determine whether the disclosure is in the best interests of the individual, and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's care
 - Covered entity may use professional judgment and its experience with common practice to make “reasonable inferences” on the patient's best interest in allowing a person to act on behalf of the individual to pick-up prescriptions, medical supplies, X-rays, etc.



Use and Disclosure of PHI (Cont'd)

■ “Minimum Necessary” Rule

- In general, the amount and types of PHI used or disclosed is restricted to the minimum amount of PHI necessary to satisfy the request.
- “Reasonable efforts” must be taken to not disclose more than the minimum amount of PHI necessary to accomplish the intended purpose.
- For example, disclosures to employers (pursuant to a valid HIPAA authorization), family members, etc.
- Does not apply in disclosures for treatment purposes to other providers or for release of PHI to patient pursuant to their own authorization.



Use and Disclosure of PHI (Cont'd)

■ Incidental Disclosures

- Those types of disclosures are not protected under HIPAA
- Disclosures that occur even after proper safeguards have been taken
- Examples: Waiting room sign-in sheets, calling out patient names in waiting room, shared hospital rooms, teaching rounds



Use and Disclosure of PHI (Cont'd)

- With review and approval, information can be used if individually identifiable parts have been removed.
 - Names
 - Address info smaller than 'State'
 - All date info except year
 - Phone, fax, e-mail, website address
 - Numbers – SSN, MRN, insurance, account #, licenses, vehicle ID, device ID
 - Fingerprints, full face photos



Use and Disclosure of PHI (Cont'd)

■ Commonsense Safeguards

- Be aware (and beware) of your surroundings
- Do not discuss patient information in hallways, elevators, restaurants, or other public places where others may overhear your conversation
- Faxes: Verify fax numbers prior to sending PHI and ask if someone will be waiting for the information (especially if you do not know location of fax machine)
- Computer screens: To the extent possible, turn away from visitors, etc.; always lock computer when leaving workstation if you are viewing PHI



Use and Disclosure of PHI (Cont'd)

- Commonsense Safeguards (cont'd)
 - Do not ever share your EMR password with anyone for any purpose
 - Do not access any medical record or other PHI unless you have a legitimate business or patient care purpose
 - For example, never access a medical record or other PHI to learn of a friend's condition, birth date, status of newly delivered baby, etc.



Use and Disclosure of PHI (Cont'd)

■ Contacting Patients

- Make every effort to speak to patient directly
- Never leave voice messages containing information regarding condition, test results, etc.
- If you must leave a message, leave your name, ECU Physicians, and your phone number only. Do not state the reason for the call.



Use and Disclosure of PHI (Cont'd)

- Verification of Identity of Individual Requesting PHI
 - Reasonable efforts must be made to verify identity of caller or individual requesting PHI
 - Reasonable questions include knowing certain personal information regarding patient, such as DOB, maiden name, etc. (not easy to find information such as telephone number, address, etc.)



Patient Rights under HIPAA

- Right to Request Amendment to Medical Record
 - Patient may request a change to the medical record
 - Provider is not required to amend; however, must notify patient regarding decision
 - Typically happens with sensitive types of conditions: Obesity, mental illness conditions, etc.



Patient Rights under HIPAA (cont'd)

■ Right to Access PHI

- Patient may inspect and copy PHI stored in the designated record set (DRS)
- Request must be in writing using approved form
- Request forms are maintained in patient's DRS
- May deny access in certain circumstances
- ECU employees are not permitted to access PHI without first going through HIS/S (treated same as other patients)



Patient Rights under HIPAA (cont'd)

- Patients can Request a Summary of Disclosures of their ECU-maintained PHI which has been made during the past six years
 - Patients are permitted to request a listing showing to whom their PHI has been released
 - Does not include disclosures made for treatment, payment, or health care operations; disclosures made pursuant to patient's own authorization or disclosures prior to April 14, 2003 (effective date of rule)
 - Does not include disclosures made for national security or intelligence purposes, or law enforcement purposes



Patient Rights under HIPAA (cont'd)

- Right to Confidential and Alternative Communications
 - Patient has the right to request the method whereby they will be contacted (e.g., what telephone number, location, etc.)
 - Any requests to communicate PHI by alternate means must be submitted in writing using the ECU Request for Alternate Communication Form



Patient Rights under HIPAA (cont'd)

- Right to Further Restrict Disclosure of PHI
 - Patient may request that their PHI not be disclosed in a certain manner, even if it is permitted under HIPAA
 - ECU may accept or decline request
 - Common requests include no disclosure for fundraising purposes (institutions are otherwise permitted to use minimal PHI for fundraising purposes), no disclosure to certain government agencies, or certain family members
 - Requests must be made in writing using ECU's Request for Restriction on the Use and Disclosure of PHI Form



Patient Rights under HIPAA (cont'd)

- Right to Complain about Privacy and Security Practices
 - Any individual may file a complaint regarding suspicion of a potential privacy violation
 - Individuals may file privacy complaints with:
 - ECU Privacy Officer 744-5200
 - BSOM Compliance Hotline (866) 515-4587
 - The United States Office for Civil Rights
 - No intimidation or retaliatory actions taken against any individual making a complaint



Research and HIPAA

- HIPAA has specific rules related to how PHI is used and disclosed for research purposes.
 - Study subjects must sign HIPAA authorization in addition to general research consent (See UMCIRB website)
 - HIPAA authorization can be “waived” by the Institutional Review Board for certain types of research activities (typically involving review of PHI for purposes of creating historical database of identifying trends in treatment, etc.)



Research and HIPAA (Cont'd)

- Investigators must follow certain procedures to access PHI for purposes of determining potentially eligible study subjects or for developing research protocols
- If you will perform research, you should study ECU's policies regarding HIPAA and research located on the UMCIRB website at <http://www.ecu.edu/irb/>



ECU HIPAA Privacy Violation Levels & Sanctions

- “A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart...” [164.530 (e) (1)]
 - Specific internal sanctions are outlined in East Carolina University Privacy Policy #0002.



ECU HIPAA Privacy Violation Levels & Sanctions (Cont'd)

■ Violation Level 1

- Failure to demonstrate appropriate care
- Examples:
 - Failing to log off a computer
 - Leaving PHI in a non-secure location
 - Inappropriate hallway conversation



ECU HIPAA Privacy Violation Levels & Sanctions (Cont'd)

■ Violation Level 2

- Intentional or unintentional exposure of PHI internally
- Unauthorized access to PHI
- Repeated Level 1 violations
- Examples:
 - Providing passwords to unauthorized users
 - Accessing PHI for which you have no responsibility



ECU HIPAA Privacy Violation Levels & Sanctions (Cont'd)

- Violation Level 3
 - Intentional or unintentional exposure of PHI internally or externally
 - Repeated Level 2 violations
 - Examples:
 - Sharing PHI with unauthorized individuals
 - Failing to perform necessary actions to prevent disclosure



ECU HIPAA Privacy Violation Levels & Sanctions (Cont'd)

- Violation Level 4
 - Intentional abuse of PHI
 - Examples:
 - Large scale disclosure
 - Use for personal gain
 - Destroying PHI



ECU HIPAA Privacy Violation Levels & Sanctions (Cont'd)

■ Sanctions

- Violations can result in local sanctions ranging from documented counseling, in accordance with ECU's disciplinary policies, up to and including dismissal.
- Other Federal sanctions may result including fines and/or imprisonment.



Penalties under HIPAA

- Civil Penalties

- \$100 per violation up to an annual limit of \$25,000 per individual

- Criminal Penalties

- \$50,000 to \$250,000 monetary penalties
- Prison time – 1 to 10 years, depending on situation

- Damage to reputation, career



Penalties under HIPAA

■ Privacy Rule Enforcement Highlights from OCR

- Since April, 2003, HHS has received over 29,944 HIPAA privacy complaints
- 75% have been resolved through:
 - Investigation and enforcement (5,066)
 - Investigation and finding no violation (2,484)
 - Closure of cases not eligible for enforcement (16,184)



Penalties under HIPAA

- OCR Most Frequent Compliance Issues (in order of frequency)
 - Impermissible use and disclosure of PHI
 - Lack of safeguards of PHI
 - Lack of patient access to PHI
 - Violation of “minimum necessary” rule
 - Lack of or invalid HIPAA authorization
- OCR referred 411 cases to the Department of Justice for criminal investigation



American Recovery & Reinvestment Act

- American Recovery and Investment Act of 2009, Pub. L. No. 111-5 (2009) (“ARRA” or the “Act”) signed into law February 17, 2009
- Privacy subtitle under ARRA drastically modifies certain provisions under HIPAA
- Variable effective dates



Key Changes under 2009 ARRA

- Security Breach Notification Requirements
 - Providers and vendors of “personal health records” (PHRs)
- Heightened Enforcement
 - Increased penalties (tiered system)
 - New requirements for auditing by HHS
 - Penalties extend to business associates
 - New entities authorized to enforce violations
- Major Changes for Business Associates
 - Direct liability under HIPAA
- Increased Restrictions on Use and Disclosure of PHI
- Additional Rights for Patients



Security Breach Notification Requirements

- First federal notification law
- For breach of any “unsecured PHI,” the covered entity is required to notify within 60 days each individual whose PHI has been accessed, acquired or disclosed as a result of such breach.
- In addition, must notify HHS of such breach within 60 days
- Annual disclosure requirement to HHS regarding notifications
- If breach involves 500 or more individuals, notice to HHS must be immediate; “prominent” local media must also be notified.
- Excludes certain inadvertent or unintentional disclosures



Heightened Enforcement Under 2009 ARRA

- Effective immediately
- Four new tiers of CMPs:
 - Range from \$100 to \$50K for each violation
 - \$25K to \$1.5 million for similar violations within a calendar year
 - Tiers based on level of culpability, knowledge, etc.
- Authorizes state attorneys general to bring a civil action in federal district court against individuals who violate the HIPAA rules.
- GAO is tasked with recommending a methodology to HHS to allow harmed individuals to receive a percentage of any CMP or monetary settlement.
- Requires periodic audits of covered entities and business associates for compliance.



Business Associates under 2009 ARRA

- Applies HIPAA security provisions to business associates in the same manner as they apply to covered entities.
- Directly liable for penalties (for both security and privacy violations).
- Expands entities that will be subject to BA requirements (any entity that provides data transmission of PHI to us or our business associates)



Increased Restrictions on Use and Disclosure of PHI/2009 ARRA

- New definition of “minimum necessary”
 - Currently it’s at the discretion of the provider
- Under new law, whenever possible we must use or disclose PHI in the form of a “limited data set” which has certain identifiers removed (e.g., names, addresses, SSN, etc.).
- Except for limited purposes, cannot receive any remuneration in exchange for an individual’s PHI, unless there is an authorization.
- Additional restrictions on communications regarding products or services where we receive compensation for such communication.



Additional Patient Rights under 2009 ARRA

- For entities that use an EMR, must allow patients copies of PHI in electronic format
- At some point will allow patients right to request an accounting for disclosures involving treatment, payment, and health care operations (as it stands, we would be subject to this on 1/1/14 to monitor such disclosures since 1/1/11).
- Cannot disclose PHI to health plan if patient paid in full “out of pocket”
- Clear opportunity to opt-out of fundraising communications



Healthcare Workforce Acceptable Use Policy

- This policy informs ECU Health Care Components and ECU workforce members of their responsibilities to protect the confidentiality, integrity and availability of EPHI. Non-compliance with this policy can lead to the application of the health care components' and/or ECU's sanctions policies.
 - You must take precautions to protect the confidentiality, integrity and availability of EPHI for which you have access. These precautions require that you:
 - Do not share your account or your password. All activities associated with your assigned user account are your responsibility.
 - Report any suspicious activity involving your account or other systems with access to EPHI.
 - Do not circumvent or otherwise bypass existing security measures. For example, do not disable anti-virus or firewall software.



Storing EPHI on Workstations

- Please do not store EPHI on your workstation.
Secure alternative: Piratedrive.
- Get approval by department head prior to storing EPHI on workstation
- Department manager must inventory and document EPHI stored on workstations at least annually.
Also, security safeguards for protecting the EPHI must be documented
- If storing EPHI on a portable device (laptop or PDA), the data must be encrypted to protect it from unauthorized disclosure if the device is lost or stolen.



EPHI and Portable Device Security

- Devices must have a power on password.
- Label device with contact information.
- Devices storing, accessing or transmitting sensitive or confidential data must use AES standard encryption for all data that is stored on the device.
- EPHI shall remain on the device only as long as necessary.
- Bluetooth infrared shall be disabled with connected; network connection must be achieved via ECU's network.
- Device must be powered to log-off or power down after 15 minutes of inactivity.



EPHI and Portable Device Security (Cont'd)

- Devices must be capable of using antivirus; must have an antivirus installed and updated to most recent definitions.
- The device must not be shared among others.
- Before transfer of ownership, the device must be securely wiped of all EPHI.
- The device must implement a device reset with the data erasure after 5 consecutive failed attempts.
- Portable devices must be physically secured; user must take steps to prevent the loss of theft of the device.
- Any loss, theft, or suspected unauthorized use of the device must be reported to the ECU Police immediately.



E-mail and Wireless Networking

- **E-mail and EPHI:** Do not send EPHI over e-mail unless (a) you send the email from your account on the university's enterprise e-mail system to another account on the enterprise e-mail system or (b) you send e-mail to locations outside of the enterprise e-mail system and you have taken appropriate safeguards to prevent unauthorized access to the enclosed EPHI.
- **Wireless Networking and EPHI:** Do not access or send EPHI over a wireless network, unless the data is encrypted prior to transmission. Two possible encryption alternatives: Citrix & Virtual Private Network (VPN). Data sent over a wireless network can be captured by unauthorized persons in nearby buildings, parking lots, and streets.
- *Contact the ITCS Security Department: Prior to purchasing any computing system that will store or transmit EPHI in order to ensure that the appropriate measures are in place at the beginning.*



ECU Security Reminders

- Use strong passwords (www.signup.ecu.edu)
- Backup critical files to other media and store offsite
- Lock your computer (Ctrl-Alt-Del) when not in use
- Guard your display from unauthorized eyes
- Don't install personal or unauthorized software
- Be cautious! Don't release information to unauthorized visitors or phone callers
- Use common sense and don't share your password
- Lock sensitive doors, drawers, cabinets, and secure software
- Update anti-virus definitions; allow daily automated updates



ECU HIPAA Policies

- Complete HIPAA Privacy and Security Policies are available at the following website: www.ecu.edu/hipaa



Questions?

For questions regarding privacy policies or procedures, contact the ECU HIPAA Privacy Officer: Micki Jernigan, JD, MPH, 744-5200, or jerniganm@ecu.edu or Debra Duncan, 744-5200, duncande@ecu.edu.

For questions regarding security policies or procedures, contact the ECU HIPAA Security Officer: Margaret Umphrey, 328-9000, or stree term@ecu.edu

For questions and requests regarding PHI disclosures
contact:

[Health Information System/Services](#)
Medical Pavillion, 1800 West 5th Street
744-3761 or 744-5478