HIPAA Privacy & Security Training for Clinicians
Introduction

• As a clinician at Duke Medicine, you have direct access to patients and patient information and a legal and ethical obligation to protect patient privacy
• This privacy module describes the Privacy & Security Rules and outlines your privacy and security responsibilities under the Rules
Objectives

At the end of this presentation, you should be able to:

– Describe how the Privacy and Security Rules affect your work at Duke Medicine
– Demonstrate how you may use and disclose Protected Health Information (PHI)
– Illustrate how to protect patients’ health information verbally, electronically, and on paper
– Identify how to report privacy and security concerns
– Explain the penalties for privacy and security violations
BASICS OF HIPAA PRIVACY & SECURITY RULES
Health Insurance Portability and Accountability Act (HIPAA)

The Privacy Rule:
- Protects an individual’s health care information known as PHI
- Identifies permitted uses and disclosures of PHI
- Gives patients control over their health information (Patients’ Rights)

The Security Rule:
- Protects an individual’s health care information that is maintained or transmitted electronically
- Defines administrative, physical, and technical safeguards for electronic PHI (ePHI)
- Requires corrective action of workforce members who fail to comply with security policies and procedures
Basics of the Privacy Rule: PHI

What is PHI?

- Information that identifies a person who is living or deceased
- Past, present, or future health information
- Health information that is electronic, in paper form, or spoken in conversation such as lab reports, conversations among clinicians, medical images, medical records
Basics of the Privacy Rule: PHI Identifiers

- PHI includes the following identifiers. To de-identify PHI, all of the 18 identifiers must be removed:

(A) Names;
(B) All geographic subdivisions smaller than a State, except the initial three digits of a zip code for all such geographic units containing 20,000 or more people
(C) All elements of dates (except year) for dates directly related to the individual, except ages (unless over 89)
(D) Telephone numbers;
(E) Fax numbers;
(F) Electronic mail addresses;
(G) Social security numbers;
(H) Medical record numbers;
(I) Health plan beneficiary numbers;
(J) Account numbers;
(K) Certificate/license numbers;
(L) Vehicle identifiers and serial numbers, including license plate numbers;
(M) Device identifiers and serial numbers;
(N) Web Universal Resource Locators (URLs);
(O) Internet Protocol (IP) address numbers;
(P) Biometric identifiers, including finger and voice prints;
(Q) Full face photographic images and any comparable images;
(R) Any other unique identifying number, characteristic, or code, except as permitted for re-identification purposes provided certain conditions are met.
Basics of the Privacy Rule: De-identification

– Removal of name is not de-identification
– Think . . . Could the patient identify himself or herself? Could the patient’s family members or friends identify the patient?
  • See policy “De-Identified Protected Health Information”
Basics of the Privacy Rule: De-identification

- If creating a case report, clinicians must de-identify the patient identifiers or have an executed authorization from the patient
  - e.g. if writing an article and you include a patient’s demographic information and the patient’s diagnosis, an authorization is necessary
  - Aggregate of conditions so it is de-identified and an individual patient or case is not discussed
SHARING PHI: TO WHOM AND HOW MUCH?
Sharing PHI

• The Privacy Rule states that PHI should only be used* and disclosed**
  – For treatment
    • e.g. providing clinical care, appointment reminders, discharge planning
  – For payment of health care services
    • e.g. Billing insurance companies, collecting payments from patients, pre-certification of services, and billing clinical trials sponsors
  – For healthcare operations
    • e.g. training, medical auditing, credentialing, case management, etc.
  – As authorized in writing by the patient
    • e.g. copy of patient’s medical record to the patient or other individual designated by the patient, sharing PHI with media
  – For other circumstances described in the Privacy Rule
    • e.g. law enforcement, public health, FDA adverse event reporting, etc.

* Use means sharing health information within Duke Medicine
** Disclosure means sharing health information with others or entities outside of Duke Medicine
How much PHI may be shared?

Minimum Necessary

• Unless disclosing PHI for treatment purposes, you must only access and share the minimum necessary—the minimum amount of information you need to accomplish the task or to do your job

• If you receive a request to share PHI and are unsure whether to release, you should contact your supervisor

• See the Policy Applying the Minimum Necessary Standard for Using, Disclosing, and Requesting Protected Health Information
• You are a nurse at DUH. Often family members call and ask you about a patient in your unit. May you share patient information with the family? If so, how much information can be shared?
Sharing PHI: Questions and examples

• The Privacy Rule permits disclosures to family and friends who are involved in the patient’s care if, using professional judgment, the clinician determines it is in the patient’s best interest to share the information. As the clinician, you must:
  – only disclose the PHI necessary to make a decision regarding the patient’s care
  – only discloses the PHI that is directly relevant to the person’s involvement in the patient’s care
  – only share the information the person needs to know to care for the patient
• Discuss with your manager if your unit uses a passcode/password which limits the PHI disclosed to only those who know the passcode—clinicians must still follow the minimum necessary rules and use professional judgment
Sharing PHI: Questions and Examples

• What does professional judgment mean as it relates to sharing PHI with family and friends involved in the patient’s care?
  – Professional judgment is judgment made by the clinician based upon facts and circumstances including the patient’s health and health care needs
  • If patient is present and has the capacity to make healthcare decisions, the clinician may discuss the patient’s health information with a family member, friend, or other person if the patient agrees or, when given the opportunity, does not object.
  • If the patient instructs not to tell his or her family about his or her condition, the clinician should not discuss the patient’s condition or treatment in front of family
Sharing PHI: Questions and Examples

• What are examples of using professional judgment and sharing PHI with family and friends involved in the patient’s care?
  – Sharing information with a patient’s adult daughter who accompanies her mom to the appointment when the daughter calls with questions about her mom’s medication. You should verify the daughter’s identity and may share information specifically related to that visit and the mother’s medication for that visit
  – Discussing a patient’s home care instructions with a patient’s neighbor who provides daily care to the patient
  – Discussing a patient’s medication with the patient’s adult son who accompanies the patient to the exam room
Sharing PHI: Questions and Examples

• May we share patient information with the media or publications on a certain condition or treatment?
  – If contacted by the media regarding patients, you should contact Duke Medicine Communications or Marketing and Creative Services to ensure patients have executed an authorization permitting the disclosure of their PHI. See policy Photographing/Videotaping/Audiotaping of Patients.”
Sharing PHI: Questions and Examples

• May we share PHI with vendors? How much information may be shared?
  – PHI may be shared with vendors if they are Business Associates, and we have a Business Associate Agreement with the vendor

• A business associate (BA) is a person or organization who is not part of Duke’s workforce but, in performing services on behalf of Duke, needs PHI to complete the responsibilities. Examples of BAs:
  – An accounting firm who in providing services to DUHS has access to PHI
  – A consultant who reviews medical records
  – An outside transcriptionist company that provides transcription services
Sharing PHI: Questions and Examples

– Prior to sharing any PHI with a vendor, staff must ensure an executed Business Associate Agreement (BAA) —a contract that describes the expectations and obligations of a BA in protecting the privacy and security of PHI entrusted to them.
  • A BAA must be executed prior to exchange of any PHI, e.g., sharing PHI to evaluate the vendor's services prior to execution of the service contract
  • A BAA should be implemented by following the Business Associate Policy and template located at http://staff.dukehealth.org
  • If a prospective business associate requests changes, please consult with Office of Counsel
Sharing PHI with Vendors

• Examples of vendors for when a BAA would be needed:
  – Device Manufacturer vendor who provides maintenance to a medical device
  – A representative assists OR staff video tape a procedure
  – A representative trains staff on a piece of new equipment
Sharing PHI: Questions and Examples

• A patient asks for a copy of her record. Can you provide her with a copy of her medical record?
  – Yes. Patients should contact Health Information Management/Medical Records (http://him.duhs.duke.edu/modules/flash_articles/) and complete an authorization form to obtain a copy of their medical records. Patients generally have the right to receive a copy of their medical record.
  – With an executed authorization, patients may designate other individuals to have a copy of their clinical information.
Sharing PHI: Questions and Examples

• May we share patient information with police?
  – The Privacy Rule permits certain disclosures to law enforcement. You should contact your manager who will work with Duke Police (DUPD) if contacted by outside law enforcement about sharing PHI. If you receive a written request, forward to Health Information Management.
Sharing PHI: DUPD

• If DUPD asks for a patient’s H&P, wants to interview staff or a patient, contact Risk Management—DUPD may interview patient with the patient’s authorization. Risk Management will work with DUHS Compliance to obtain permission

• If DUPD ask for blood test results for alcohol testing, forward to Health Information Management

• If SBI asks for pharmacy information, contact Risk Management—SBI must provide a request in writing and are limited to prescription records
Sharing PHI: Documentation

- Patients have the right to request an accounting of certain disclosures of their health information
- Accounting of Disclosures excludes uses or disclosures made for payment, treatment, and healthcare operations and disclosures the patient has specifically authorized
- Duke must document certain disclosures including but not limited to:
  - disclosures to public health agencies as required by law without authorization (e.g. STD reporting)
  - disclosures to the FDA for adverse event reporting
  - disclosures for research performed with an IRB waiver of need for authorization
  - disclosures to law enforcement
  - disclosures for administrative procedures without authorization from the patient
  - disclosures required by law (including legally required disclosures to workers compensation)
Sharing PHI: Documentation

• If a disclosure is not for payment, treatment, healthcare operations, or a disclosure for which the patient has specifically authorized, the disclosure must be documented in the disclosure log.
  – If such a disclosure is made, it is your responsibility to ensure the disclosure is included in the disclosure log
    • See the Right to an Accounting of Disclosures of Protected Health Information policy
  – To obtain access to the disclosure log, contact Health Information Management
    • Duke University Hospital, 919-668-5280
    • Durham Regional Hospital, 919-470-5172
    • Duke Raleigh Hospital, 919-954-3150
  – All written patient requests for an accounting of disclosures should be forwarded to the DUHS Privacy Officer
Privacy Video: Coworker Privacy

• Now, let’s see a video . . .
• http://staff.dukehealth.org/TechEd/Coworker_privacy.html
Privacy Video: Coworker Privacy

• In the video what should Jane have done?
  – Jane followed the proper policies and procedures in contacting the hospital information desk for information about her coworker, Karen. However, when she did not receive any information, she should have stopped. When Jane accessed Karen’s medical record without authorization and then disclosed the information to Bill, she did so for personal use and not to perform her job responsibilities.
  – Jane should not have looked up any information in Karen’s medical record, and Bill should not have suggested Jane do so.
  – Individuals can only access systems that are related to their job responsibilities—checking on a coworker is not job related.
Sharing PHI: Unauthorized Access

• **Unauthorized Access** is the access/disclosure of information that an employee does not have a responsibility to access or share (e.g. accessing PHI for personal reasons with no authorization). The following examples are not allowed:
  – Disclosing the hospitalization of a neighbor and the diagnosis
  – Looking at an ex-spouse’s record for a custody hearing
  – Looking at a spouse’s medical record without written authorization

• Staff cannot access information on adult children, friends, **patients**, staff, acquaintances, etc. **unless involved in their care or have written authorization from the individual***
  – Authorization form available from Health Information Management/Medical Records

*For payment and treatment purposes, staff may access their own electronic medical record.
PROTECTING PATIENT INFORMATION
Protecting Health Information

Protecting *spoken* health information means we should:

- Direct visitors and callers to the information desk
- Speak softly in semi-private rooms
- Close doors or curtains when talking about treatments or doing procedures
- NOT talk about a patient’s care in public areas like the waiting room, cafeteria, city buses, Duke buses
- Knock first and ask to enter a patient’s room
- Ask a patient’s permission before speaking about the patient’s condition in front of visitors
- Use *professional judgment* when making decisions about sharing PHI with friends and family when a patient is incapacitated or otherwise unable to give authorization for sharing information with friends and family
Protecting Health Information

To protect health information on paper we must:

– NOT leave papers unattended on printers, copiers, fax machines, etc.
– Use a cover sheet when faxing PHI; check to make sure you have the correct fax number
– Keep health information away from public view
– Shred information no longer needed (NOT place in trash) following the Retention, Preservation and Destruction of Records Policy
– Find the owner of “lost” papers found in restrooms, lobbies, etc.
– Secure medical records—lock
– Not print spreadsheets and then take them home
– Not remove papers containing PHI from campus
  • Ask your supervisor before removing confidential information off campus
Protecting Health Information

Protecting electronic health information means we should:

- Keep computer screens pointed away from the public
- Log off or secure your computer workstation when leaving
- Create strong passwords. See the Information Security Standard: Passwords
- NEVER share passwords even with technical support people and assistants
- Report viruses, computer errors, and security violations
- Follow the Electronic Communications Policy
- Not store sensitive electronic information (SEI) on mobile devices unless it is encrypted. Store SEI on DHTS-supported shared and personal network drives accessing through VPIN.
- Keep portable devices in a safe and secure place--locked
- Properly dispose of mobile devices that are no longer needed following the Information Security Standards on Media Control
Protecting Health Information: E-mails

- Use DHTS-supported e-mail when sending work related e-mails
- De-identify the PHI in the e-mail as much as possible
- Click the “Sensitive Electronic Information” box when sending e-mails containing PHI outside of Duke Medicine
  - Include (Secure) as the first word in the subject line for webmail (i.e. iNotes) which does not have an SEI button
- Send the e-mail only to those who have a “need to know” the information
- Check to make sure you have the correct e-mail address (name and position)
- E-mails should not be automatically forwarded outside Duke Medicine
- Do not put PHI in the subject line of e-mails
How do I securely email SEI in Lotus Notes?

Click the “Sensitive Electronic Information” box in Lotus Notes when sending emails containing PHI. When using this method, you should click the “Sensitive Electronic Information” check box for every outgoing message you want sent securely.

Or you should type (Secure) as the first word in the subject line—should be used for iNotes, Macintosh clients, and smartphones which do not have the SEI box.
How do I securely email SEI in Outlook?

Press the “Sensitive Electronic Information” button before you press the Send button to send the email securely. This will insert the [Send Secure] tag at the beginning of the Subject line.

When using this method, you should click the “Sensitive Electronic Information” check box for every outgoing message you want sent securely.

Outlook Web Access (OWA) and Macintosh clients should include the work (secure) in parentheses as the first word in the subject line.
Securely Storing SEI

• Use DHTS-supported shared and personal (unique to you) network drives
  – These drives can be accessed through PIN, VPN, or VPIN on your desktop
  – These drives are secure and backed up nightly
  – For questions on accessing such drives, contact your System Administrator

• Don’t store PHI on your personal computer/device
Protecting Health Information: Social Networking

• On **personal social media sites** (Facebook, MySpace, Twitter, etc.) and professional association list serves/Web sites, **you should not:**
  – Post or discuss Duke patients or any PHI (even if de-identified)
  – Discuss your day at work including events that happened on the unit or department
  – Participate in any online conversation involving patients or patient information
  – Take or post any pictures (including on cell phones) of patients, patient’s body parts, patient images, etc. **even if the family or patient agreed and the pictures do not identify the patient**
  – Blog details about your clinical activities
  – “Friend” patients on social media sites (e.g. Facebook, MySpace, Twitter)
To protect patient privacy, you **should**:

- Use internal communication tools (Lotus Notes, Outlook, Duke Wikis and blogs inside the Duke Medicine firewall)
  - Generally, no PHI should be shared on Duke Wikis or blogs
- Contact Marketing & Creative Services for [tips and guidelines if developing a Duke social networking site](#)
  - The posting of any PHI including pictures requires the patient’s written authorization and approval by the Privacy Office
Examples of Possible Privacy and Security Violations

Is this situation a privacy breach?

• On his personal Facebook page, Tom Smith, RN has the following information posted on her wall and in her profile:
  • Occupation: Nurse with Life Flight
  • Status: “Tough day today: one of my patients died in route to the hospital”
  • Picture posted with the message “Great stab wound pictures, Tom!”
Examples of Possible Privacy and Security Violations

Yes! By sharing where he works and the events that happened while working, Tom has violated the privacy rights of the patient who died as well as the rights of the patient’s whose picture he posted on his Site. Such pictures and discussions should not occur on an individual’s personal social media page.

Individuals should not discuss clinical activities on their personal social networking and post pictures of patients even if de-identified.
Examples of Privacy and Security Violations

Is this situation a breach?
A medical assistant posts a picture of patient in which she is checking the patient’s vitals. Picture contains the caption “Mackenzie, my favorite patient, on her 10th birthday.” Other staff members write the following comments:

“I can’t believe how much she has grown. That’s a great picture.”
“Wish all my BMT patients were as good as Mackenzie”
“Wish all my patients’ PARENTS were as good as Mackenzie’s parents”
Yes! In this example the medical assistant who posted the picture and identified the child as a patient at Duke would face corrective action as well as the other staff members who commented. The medical assistant should not have posted the picture and the staff should not have commented.
North Carolina Identity Theft Protection Act

- Requires Duke Medicine to implement procedures to protect against unauthorized access of an individual’s personal information, specifically social security numbers (SSN)
- Duke Medicine does not use SSN as an individual’s primary identification number
  - Staff should follow policy “Protecting the Confidentiality of Social Security Numbers”
  - If staff desires to create a database or implement a system or screens within a system that captures or includes social security numbers, staff must obtain approval from the Compliance Office (668-2573) and/or the Duke Medicine Chief Information Officer (668-0518)
- Staff are required to report any suspected inappropriate access of SSN to the Compliance Office 668-2573 or the Duke Medicine Integrity Line 1-800-826-8109
Protecting Health Information: Breaches

• Duke Medicine has obligations to report a breach of patient information
  – A breach is, generally, an impermissible use or disclosure under the Privacy Rule of unsecured PHI which compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.
  – A breach is permitting an unauthorized person to have access to PHI
  – A breach of secured (encrypted) PHI (e.g. PHI stored on an encrypted laptop) is not a breach as defined by HITECH
Protecting Health Information: Breaches

• Upon allegation of a breach of unsecured PHI, the Privacy Office will perform a risk assessment to determine if the unauthorized use, access, or disclosure “poses a significant risk of financial, reputational, or other harm to the individual”
  – If risk exists, Duke has reporting responsibilities to the patient and the Department of Health and Human Services
    • Breach must be reported within 60 days of discovery of breach
Staff Responsibilities

• You have a duty to report any allegation of a breach including reporting unauthorized access
  – Report any allegation to the Compliance Office at 668-2573 or 1-800-826-8109
    • Examples include: misdirected e-mails, letters, or faxes containing PHI
    • Any loss of unencrypted laptops storing PHI must be reported to Duke Police and Risk Management
    • If you have questions on if the allegation should be reported, REPORT IT!
Individual Rights

• Restrictions on disclosures of PHI
  – Duke Medicine must agree to a patient’s requested restriction if the disclosure is to a health plan (insurance company) for purposes of payment or operations, and
  – The PHI relates to a service for which the patient has paid out of pocket in full
    • e.g. patient pays out of pocket for cosmetic surgery
  – PRMO is leading initiative to develop means to flag records/accounts and restrict disclosures
    • If staff is asked to restrict, they should contact their manager to work with the PRMO
Business Associates (BA) and Business Associate Agreements (BAA)

- All BAAs are required to be updated to address the new HITECH security requirements
  - All contract renewals are required to have a new BAA found attached to the Business Associate Policy
REPORTING BREACHES AND CORRECTIVE ACTION
Reporting Breaches

If you become aware of a Privacy or Security violation or an alleged breach, you should notify any of the following:

- Your manager or supervisor
- Your facility privacy or security director or officer
- Your compliance office
  - DUHS Compliance Office 668-2573
  - SOM Compliance Office 684-2144
  - PDC Compliance Office 668-5161
- The Integrity Line (1-800-826-8109)
Integrity Line

• If you wish to make an anonymous report or feel uncomfortable calling the Compliance Office directly, you can call the Integrity Line

1-800-826-8109

• An outside company handles all hotline calls
• All hotline calls are confidential and thoroughly investigated by the compliance office
• You do not have to give your name
What happens to me when I report a Privacy Concern?

Non-Retaliation/Non-Retribution Policy

• If you report a concern in “good faith,”* no retaliation or retribution may be taken against you even if the investigation determines that a problem does not exist.

• Supervisors will be disciplined for any attempts to punish or retaliate against anyone acting in good faith in reporting a compliance violation.

*Good faith means that the person reporting the problem truly believes that a problem exists.
Violating HIPAA Privacy or Security Rules

- You and Duke may receive severe penalties for HIPAA Privacy or Security Rule violations.
  - There are civil and criminal penalties
- If you do not protect an individual’s health information, you may face corrective action under Duke’s work rules.
  - Duke Medicine penalties for HIPAA Privacy or Security Rule violations depend on the level of violation
  - Corrective action includes up to and including termination of employment
  - See the Breach of Protected Health Information/Patient Privacy Policy
Summary: Privacy and Security Rules and Responsibilities

- Use and disclose PHI only as related to your job responsibilities
- Take appropriate safeguards to protect patient privacy
- Report privacy and security concerns

- For questions, contact DUHS Compliance 668-2573 or compliance@mc.duke.edu