The HIPAA Privacy Rule: Guidelines for Health Care Providers

Key Terms and Acronyms

- **Privacy**: the right of an individual to keep his/her individual health information from being disclosed
- **Use:** with response to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an an entity that maintains such information
- **Disclose:** release or divulgence of information by an entity to person or organizations outside that entity

Key Terms and Acronyms

- **Authorization**: the mechanism for obtaining consent from a patient for the use and disclosure of health information for a purpose that is not treatment, payment or health care operations.
- **Minimum necessary**: when using any PHI, an entity must generally make reasonable efforts to limit itself to “the minimum necessary to accomplish the intended purpose of the use, disclosure, or request”
- **Covered Entity:** defined as health plan; health care clearinghouses; health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards

Purpose of Privacy Rule

- Protect and enhance the rights of healthcare consumers by providing them access to their protect health information (PHI) and controlling inappropriate use of their PHI

PHI include any of the following:

- Name
- All elements of dates, except year, and all ages over 89 or elements indicative of such age *
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographs and any comparable images
- Any other unique, identifying number

* Data elements that are allowed in a Limited Data Set

Use of Limited Data Sets (LDS)

- LDS: a class of PHI that excludes 16 of the 18 identifiers.
  - Can be used for research, public health or health care operations, as long as the recipient of the data signs a Data Use Agreement with the university
  - May not be used to re-identify or contact an individual
  - “Minimum necessary” standard applies
  - Accounting of Disclosures of PHI does not apply when a LDS is disclosed as allowed by law

What patient information must we protect?

- Includes, but is not limited to:
  - Medical records
  - Diagnoses
  - X-rays, photos and Images
  - Prescriptions
  - Lab work and other test results, billing records
  - Claim data
  - Referral authorizations,
  - Explanation of benefits
  - Clinical research records of patient care must also be protected
  - PHI about individuals who have been deceased less than 50 years

Access to PHI

- Based on “need to know” and “minimum necessary” principles
- Must track disclosures of PHI
- Policies/procedures and training of staff
- Individuals needing access to PHI include those individuals:
  - Providing health care
  - Performing payment or billing activities
    - Can only provide information on a specific visit
  - Participating in health care operations

“Minimum Necessary” Standard

- You are permitted to access and use only the minimum patient information necessary to do your own job.
  - Healthcare provider may need to access entire health record to obtain and develop a comprehensive medical history
  - A billing clerk may only need to access a given office visit in order to correctly submit a claim for payment

Patient Privacy Rights

Patients have a right to:

- Receive our “Notice of Privacy Practices”
  - Required to sign form acknowledging receipt
  - Form is scanned into health record
- Access and request a copy of their health record
- Request amendments/addendums
- Request restrictions on use and/or disclosure within limits of the law
- Request an accounting of disclosures
- File a complaint if privacy rights may have been violated

Notice of Privacy Practices

- Serves as the main communication to patients
- Educates patients on:
  - Their rights related to their PHI
  - Your responsibilities for protecting their PHI
  - How you may use and disclose their PHI
- Directs patients where to go for questions and concerns regarding their PHI

HITECH and HIPAA

Health Information Technology for Economic and Clinical Health (HITECH) Act and the HIPAA privacy and security standards.

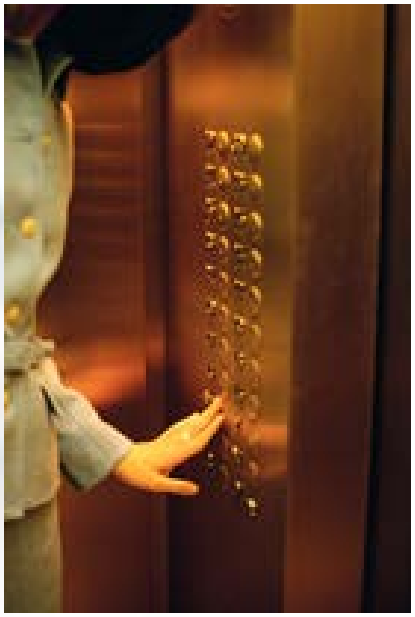
- Breach notification requirements
- Fine and penalty increases for privacy violations
- Patient right to request electronic copies of the electronic health care record
- Patient right to restrict disclosure to health plans for services self-paid in full (“self-pay restriction”)
- Mandates that Business Associates are directly liable for compliance with HIPAA provisions

What is not covered under HIPAA/PHI?

- Employment records of the employer
- Family Educational Rights and Privacy Act (FERPA) records

- Preemption of state law:
  - Privacy Rule overrides any other state law *unless* that state law provides more protection for the consumer

Privacy Breach Examples



- Users not logging out of computer systems, allowing others to access their computer or system
- Talking in public areas such as an elevator, talking too loudly, talking to the wrong person
- Lost/stolen or improperly disposed paper documents, films, notebooks, medication bottles
- Lost/stolen unencrypted laptops, tablets, cell phones, media devices (video and audio recordings)
- Lost/stolen unencrypted zip disks, CDs, flash drives, memory sticks
- Hacking of unprotected computer systems
- Email or faxes sent to the wrong address, wrong person, or wrong number
- Leaving PHI in a voicemail

Patient Authorization

An Authorization for Use or Disclosure Form ***must*** be completed.

If *any* of the required elements are not completed on the authorization form, the authorization is *INVALID* and you *may not* act on the request!

Treatment, Payment, & Healthcare Operations (TPO)

Examples of permitted disclosures for TPO include:

- Providing medical treatment and services
- Coordinating continuing care needs and services
- Obtaining payment for services

Health Care Operations

- Activities that support health care operations include:
  - Quality Assurance & performance improvement
  - Medical staff peer review
  - Auditing and monitoring
  - Compliance reviews

Payment for Services

- Activities that are intended to obtain payment for healthcare services include:
  - Insurance verification
  - Eligibility
  - Billing & collections
- Activities to obtain payment generally do not require a patient authorization
- The bill the patient would receive is also HIPAA protected

Patient Pays Cash for the Visit

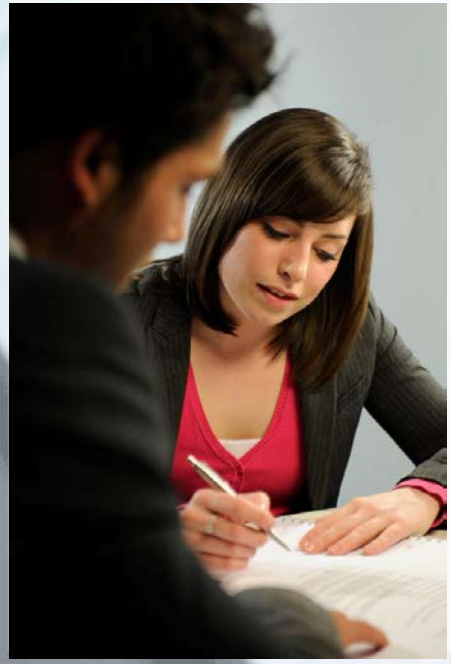
- HIPAA/HITECH now allows the following:
  - When a patient pays cash for a visit and does *not* want their insurance company billed for the service, the healthcare provider cannot share information about the visit or the treatment given with the patient's health plan, or other requesting entity without the expressed written permission of the patient for that specific visit.

Disclosure of PHI

Disclosure occurs when:

- PHI is communicated outside of the facility's health care network
- Data in an electronic claim is submitted for payment
- Authorization for use and disclosure form must be signed by the patient/legally authorized individual, dated and have a time limit of the authorization.

Disclosures within TPO that Require Patient Authorization



- Drug and alcohol abuse treatment
- HIV and AIDS test results
- Mental/behavioral health

Disclosures Mandated or Permitted by Law

- Disclosures that are mandated or permitted by State or Federal law, or by certain government agencies, ***do not*** require patient authorization

- Examples include:
  - Organ and tissue donation
  - Public health activities
  - Health oversight agencies
  - Coroners, medical examiners, and mortuaries
  - Military commands
  - Workers compensation
  - Correctional facilities
  - Law enforcement
  - Serious threat to health & safety

Permitted Disclosures to Law Enforcement

- Responding to a court order, subpoena, or similar process
- Identifying or locating a suspect, witness, or missing person
- Reporting about crime victims

Disclosures that *Must* be Accounted For

- Disclosures to law enforcement
- Abuse, assault, neglect
- Judicial and administrative proceedings
- Public Health activities
- Data collected in preparation for research
- Agency health oversight activities
- Organ and tissue donation
- Coroner

Disclosures that *do not* need to be Accounted for

- TPO
- PHI given to the patient or their representative
- Where an authorization has been obtained
- Uses/disclosures to HCP involved in patient's care and where authorized
- National security or intelligence

Requests for release of PHI

- Respond to requests when necessary to ensure patient safety, treatment, and continuity of care
- Clinical staff may disclose PHI to individuals directly involved in the patient's care, as long as the patient identifies the individuals who may be provided such information

Requests for release of PHI (cont.'d)

- Written authorization from the patient (or the patient's legally authorized representative) is required to disclose or access PHI for uses other than treatment, payment, or healthcare operations.
- Special authorization is required to access any information pertaining to drug and alcohol abuse, mental health diagnosis or treatment (psychotherapy record), HIV/AIDS test results, and genetic testing.

Handling Requests for release of PHI

- Validate the identity and authority of the requestor
- Check photo ID for in-person requests and/or pick-up of PHI
- Ensure that the appropriate request for release of PHI is in the health record and is duly signed and dated
- Validate phone requests by call back to the requestor
- Document how disclosure of the information was made, e.g., US mail, encrypted email, hand delivered.

What should be documented in the health record related to release of PHI?

- Date of disclosure
- Name of entity or person receiving the information
- Brief description of PHI disclosed
- Brief purpose of the disclosure
- Legible signature of person providing the information

Documentation for Permitted and Mandated Disclosures

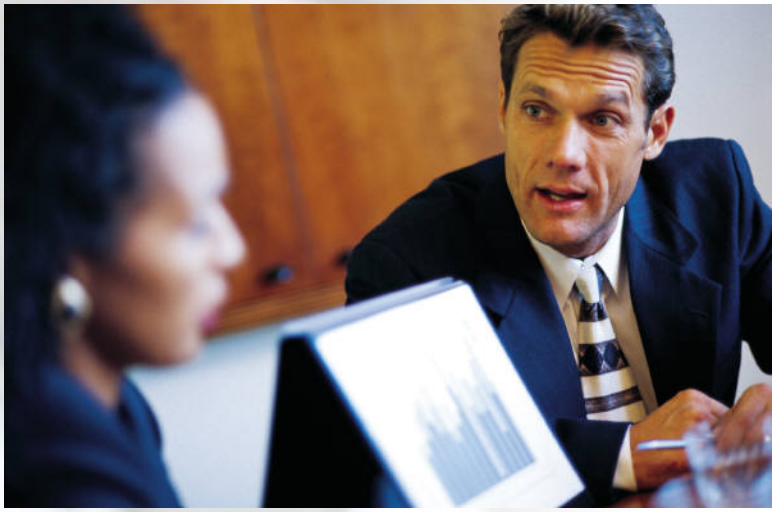
- Certain disclosures of PHI must be documented for purpose of accounting disclosures
- Disclosures may be documented:
  - In the clinical record
  - On a mandated reporting form, i.e., abuse report or Confidential morbidity report to Public Health
  - On a PHI Disclosure Documentation form

Patient Requests for Restrictions on Uses and Disclosure of PHI

- Requests must be in writing
- Request for alternative forms of communication, e.g., mail to PO Box and not a street address, do not leave voice messages
- Requests will be evaluated on an individual basis
- Refer requests to a Director or the University Compliance Office
- Accommodating requests is based on the information system’s capabilities to restrict information

Disclosures Requiring Patient Authorization before PHI can be released

- *Research
- Marketing
- Fundraising



*Unless IRB approves Waiver of patient authorization

PHI for Research purposes

- Researchers may obtain, create, use, and disclose individually identifiable health information if they obtain the appropriate authorizations and approvals for research, which include both of the following:
  - IRB approval for research
  - Patient authorization for release of medical information for research purposes, and/or a IRB approved Waiver of Authorization

HIPAA Mandates related to the Protection of PHI in Research

- Systems and processes be in place to protect the confidentiality and privacy of patient information.
- All principle investigators (PI) are responsible for all aspects of their research study, including adherence to HIPAA regulations for the protection of privacy and confidentiality of identifiable PHI.
- PIs must take appropriate steps, including the usage and storage of research data in a manner that ensures physical and electronic security (e.g., data encryption).
- Data Use Agreements or Business Associate Agreements may be required to allow for sharing data with parties external to the university.

Requirements for Security of PHI

- University Faculty, Staff and Students are responsible for utilizing appropriate and applicable security controls to protect all PHI information resources under the university's control, such as:
  - Safeguarding PHI from accidental or intentional disclosure to unauthorized persons
  - Safeguarding PHI from accidental or intentional alteration, destruction, or loss
  - Safeguarding computers from viruses and malware
  - Taking precautions that will minimize the potential for theft, destruction, or any type of loss
  - Administrative: contingency plans, e.g., disaster recovery
  - Physical: Access control
  - Technical: Authentication
  - Network: Data transmission security

Requirements for Security of PHI (cont.'d)

- Protecting workstations from unauthorized access and theft (e.g., via password authenticated access and physical lockdown) to ensure that ePHI is accessed, used, and/or disclosed ***only*** by authorized persons

- Protecting other electronic assets and portable media (e.g., USB thumb drives, external hard drives, CD-ROM/DVD disks, floppy disks, magnetic tapes, videotapes, SD memory cards, and all other forms of removable media or electronic storage devices) from unauthorized access and theft, to ensure that ePHI contained within is accessed, used, and/or disclosed ***only*** by authorized persons

  - Passwords must be used when accessing desktops/laptops/tablets/cell phones
  - Do not include any ePHI in the subject line, e.g., patient name
  - Do not send attachments containing ePHI without encryption

Patient Requests for Alternative Information

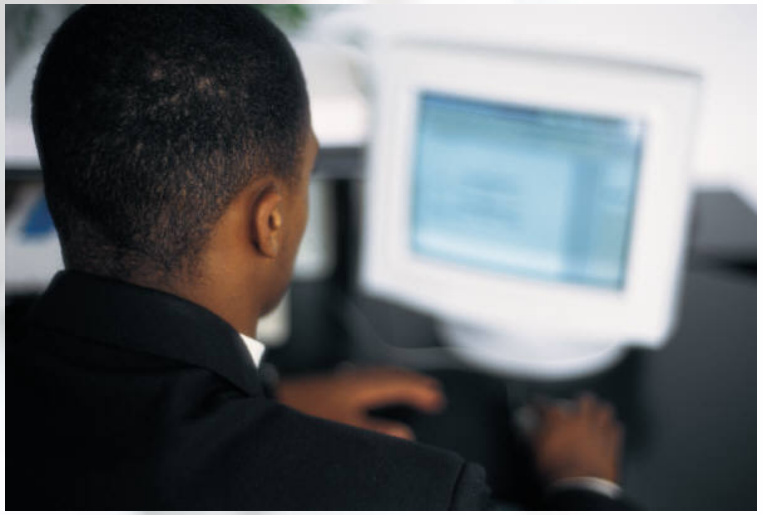
- Patients may request that communications about medical matters be made in a certain way or to a certain location
- Reasonable requests should be accommodated

Patient Requests to Inspect or Obtain a Copy of their PHI

- Provide the patient with an “Authorization for Use and Disclosure of Health Information” form
- The Center’s Director is responsible for:
  - Reviewing request with HCP
  - If appropriate, providing information and copies of information to the patient upon request

Patient Requests to Amend their Health Record

- Patients must submit the request in writing to the designated office named on the Notice of Privacy Practices
- Director reviews records with HCP

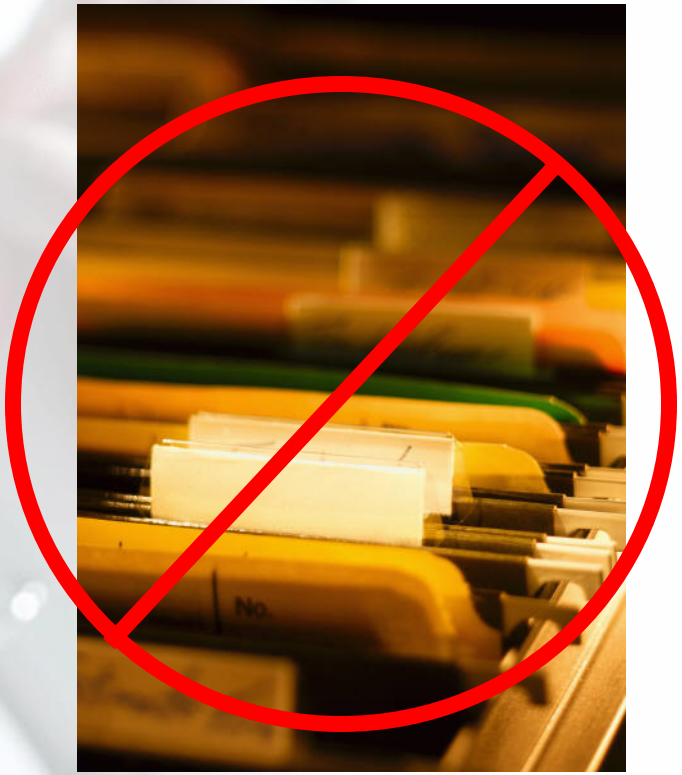


Amendment Requests

- We cannot change the record if:
  - It was not created by one of our HCP
  - Records are confidential and aren't available for inspection
  - Not part of the set of records designated as covered by HIPAA
  - Record is accurate and complete
- Policy requires response to patient within 10 working days of request, 20 days if records not on site

Denying Patient Requests to View their Health Information

- Patient access may be denied in certain instances
- Consult with Center's Director or the University's Compliance Office



Emailing PHI

- Requires written permission from the patient or legally authorized guardian/individual.
- Even with consent, records should be sent via encrypted email to ensure only those with permission to access the records receive them.

Email Regarding Patients

- Never send ***un***encrypted information over the internet that you would not place on a billboard.
- You cannot control how a message you generate is forwarded or shared once it is sent!

Faxing Health Information

- Faxing of PHI is another key privacy consideration
- Consider faxing PHI when the information is:
  - Urgently needed for patient care or to obtain payment
  - Authorized by the patient or his/her legal representative

Guidelines for Faxing PHI

- Locate fax machines in secure locations
- Secure incoming faxes
- Verify the accuracy of fax numbers before sending outgoing faxes
- Use a fax cover sheet for all transmissions
- Pre-program frequently called numbers
- Notify others of any fax number changes

Handling Misdirected Faxes

- Obtain the correct fax number ***and*** immediately transmit a request to the unintended recipient requesting that the material be destroyed immediately and obtain a written attestation that the recipient destroyed all copies and did not use/disclose the information.
- Follow Center procedures:
  - Complete online Incident Report
  - Contact University Compliance Office

Social Media Use

- Do not share any patient information acquired through your work at WesternU, even if the information is public or on some form of social media site
- Information obtained from your patient/provider relationship is **confidential**
- Posting PHI without authorization is a violation of the patient's **right to privacy** and confidentiality
- Even if you *think* you've de-identified the information, it still might **be identifiable to others**
- NOTE: De-identification of PHI requires removal of all 18 PHI identifiers, which includes "*Any other unique identifying number, code, or characteristic*" (e.g., photo of a wound; description of a patient's condition)

Social Media Points to remember

- **Do not provide information regarding patients through any social media outlet:** eliminates risk of violating HIPAA. You just never know if the patient you cared for earlier today liked you so much that they started following your tweets.
- **Do not respond to healthcare questions posed on social media**. The small favor you think you are doing for a friend may come back to bite you in the form of a malpractice suit or an unlicensed-practice-of-medicine allegation if the friend lives in one state and you in another.
- **Keep your personal social media accounts separate from your business social media accounts**: substantially reduces risk of your patients and co-workers being able to see *that* picture of you in college posted by your old roommate.
- **Regularly check your social media accounts**. Viruses, hackers, and imposters pose a risk that you are unknowingly emitting an unfavorable image of yourself.
- **Retain strong privacy settings:** helps maintain separation of personal and business social media outlets.

Remember, social media poses additional risks to healthcare providers. By appropriately managing these risks, healthcare providers can enjoy the benefits of social media and avoid the pitfalls.

Patient Complaints

- Patients complaints or concerns regarding information practices should be addressed through existing channels
  - Center Director
  - Clinical Dean
  - University Compliance Office
- Patients may also file a written complaint and request an investigation with the state Department of Health and Human Services (DHHS)
- The PCC’s Notice of Privacy Practices provides information on where the patient can send the complaint

Your Responsibilities

- Control access to PHI
- Use and disclose only the information necessary to meet the need
- Obtain authorizations for disclosures
- Be aware of penalties for privacy/security breaches
- Report breaches to Compliance Office

Reporting Violations

- If it is discovered that HIPAA/HITECH protected information was inappropriately accessed or complaints are received related to HIPAA/HITECH, this should be immediately reported to the compliance office for investigation.

Consequence of Violating HIPAA

Oral, paper, or electronically

Civil Code 56.36/ Health & Safety Code 130200

- **Mandates the confidentiality of medical information**:
  - Implement appropriate administrative, technical and physical safeguards to protect the privacy of a patient's medical information, and implement reasonable safeguards to prevent unauthorized access, use, or disclosure.
- **Individual Fines / Penalties:**
  - $2,500 – $25,000 per violation
  - $250,000 – maximum penalty
- Potential misdemeanor, if economic loss or personal injury
  - **Potential for civil action by consumer with statutory damages ($1000) in addition to actual damages**
  - **CDPH may notify licensing board for further investigation/ discipline of individual providers.**

Health & Safety Code 1280.15

- **Mandates prevention of unlawful or unauthorized access to, use of, or disclosure of patient medical information**
- **Reporting obligations:**
  - Incident of unlawful access, use, or disclosure of a patient's medical information must be reported within 5 days of detection of the breach to CDPH and the affected patient(s) / legal representative.
- **Institutional Fines for failure to prevent or report:**
  - $25,000 – initial violation (per pt.)
  - $17,500 – subsequent occurrence
  - $250,000 – maximum penalty
  - $100 / day for late reporting
    - **Criteria considered by CDPH included in the determination of amount of the fine.**
    - **CDPH may refer violation to licensing boards**

California Medical Information Act (CMIA)

- Applies to individuals as well as institutions
- Unauthorized access includes
  - inappropriate review or viewing of patient health information without a direct need for diagnosis, treatment or other lawful use
- Healthcare facilities are required to report incidents of unauthorized access, use, or disclosure of PHI to the California Department of Public Health, and to the affected patient within **5 business days** after breach detection
- When you suspect or know of a breach you must report it to the University Compliance Office **immediately** at extension 3871
- **An online Incident Report must also be completed**

Cal. Civ. Code §§ 56-56.37

Other laws and regulations on HIPAA

- **Other Federal Laws**
  - Medicare Conditions of Participation promoting patient rights including privacy
  - Federal Trade Commission protection of consumer privacy
  - FERPA protection of student education records
  - HHS and multiple agencies' protection of information
- **Other California State Laws**
  - Confidentiality of Medical Information Act (CMIA)
  - Title XXII protections of patient records
  - Information Practice Act
  - Breach notifications
  - Lanterman-Petris-Short (LPS) protection of mental health records
- **University Policies and Procedures**

Remember….

H

HIPAA compliance is everyone's job.

I

Bending rules could mean you are breaking the law.

P

Protect PHI as if it were your own.

A

Always take the most conservative approach.

A

Ask for permission—with an Authorization—not for forgiveness.

Imagine that it's your PHI, and do the right thing!