



University of California
San Francisco

advancing health worldwide™

Advanced HIPAA PHI Management

Target Audience: Individuals with responsibilities for management of Protected Health Information (PHI) including disclosure, accounting and responding to requests for patient information.

Copyright 2008 The Regents of the University of
California

All Rights Reserved

The Regents of the University of California accepts no liability for any use of this presentation or reliance placed on it, as it is making no representation or warranty, express or implied, as to the accuracy, reliability, or completeness of the presentation.

Objectives

- **Become familiar with:**
 - HIPAA Privacy Laws: New patient rights
 - Management of Protected Health Information (PHI)
 - Minimum Necessary Standard (MNS)
 - Designated Records Set (DRS)
 - Uses & Disclosures (U&D)
 - Restrictions
 - Authorizations and special exceptions
 - Accounting for disclosures
 - Security considerations

What is HIPAA?

- HIPAA (Health Insurance Portability and Accountability Act) is a Federal Law that specifies Administrative Simplification provisions that...
 - Protect the privacy of patient information
 - Provide for electronic and physical security of health and patient medical information
 - Simplify billing and other transactions

All health care providers, health plans and health care clearinghouses are required to comply with HIPAA privacy regulations by April 14, 2003.

Key HIPAA Terms & Definitions - 1

PHI...Protected Health Information

- Information about past, present or future medical or mental health or condition; created / received by a provider in the course of treatment/evaluation; individually identifiable; in ANY medium – written, oral or electronic
- Excludes: Employment data and research data; however, these items are subject to other privacy laws and must be treated confidentially.

Key HIPAA Terms & Definitions - 2

TPO...Treatment, Payment & Operations

- HIPAA allows UC to create, use and share a patient's protected health information (PHI) for treatment, payment and healthcare operations, such as:
 - Treatment of the patient, including appointment reminders
 - Payment of healthcare bills (e.g., claim submission, authorizations and payment posting)
 - Health care operations and business operations, including teaching and medical staff quality activities

Key HIPAA Terms & Definitions - 3

DRS...Designated Record Set

- **Includes:**
 - Medical records or other information used for decision making in the treatment/evaluation of a patient.
 - Medical billing and payment information
- **Excludes:**
 - Operational information, such as clinic schedules, procedure logs, peer review information, business information, rough drafts.
 - Research records which are not part of the medical / treatment record

Key HIPAA Terms & Definitions – 4

MNS...Minimum Necessary Standard

The minimum information needed to do one's job

- Staff access to information must be based on the job duties / roles, e.g., “need to know”
- Exercise reasonable efforts not to use or disclose more than the minimum amount of information needed to accomplish an intended purpose
- MNS does not apply to provider requests for information relating to treatment/evaluation

Key HIPAA Terms & Definitions – 5

U&D...Uses & Disclosures

- Use... is the sharing, employment, application, utilization, examination, or analysis of protected health information (PHI) within the covered health care component that maintains the PHI.
- Disclosure... is the release, transfer, provision of, access to, or divulging in any manner PHI outside the covered health care component that maintains the PHI.

Key HIPAA Terms & Definitions – 6

BAA...Business Associate Agreement

- A business associate:
 - Performs a function involving protected health information (PHI), i.e., collection agencies, external auditors or consultants
 - On behalf of the University of California/UCSF
 - Requires HIPAA contract language called “Business Associate Agreements” (BAAs) to protect PHI.
- A business associate must maintain the same level of privacy of PHI as UCSF and must report confidentiality incidents to UCSF.

Key HIPAA Terms & Definitions - 7

OCR...Office of Civil Rights

- Enforcement by the Health & Human Services (HHS) Office of Civil Rights (OCR)
 - Minimum fine of \$100 per Infraction with Maximum of \$25K for Multiple Violations of Identical Violation
 - Wrongful Disclosure Penalties Range from \$50K - \$250K per Incident and Jail Terms from 1-10 Years
- Be Aware: Individual and/or organization fines/penalties including sanctions for disclosures and/or scrutiny for breaches will be enforced.

Key HIPAA Terms & Definitions - 8

PR...Personal Representatives

- Federal Law: Under HIPAA, patients can choose a “surrogate decision-maker” who is referred to as the individual’s “personal representative.”
- The patient is required to notify us either in writing or verbally of their personal representative.
- California Law: Pre-empts or supercedes HIPAA in determining who is a personal representative.
 - Examples of Exceptions: Suspected abuse or neglect of children, elders or dependent adults reporting requirements

Key HIPAA Terms & Definitions - 8

PR...Personal Representatives - Minors

- Parent, guardian or other person acting in loco parentis usually has:
 - Authority to make healthcare decisions about an un-emancipated minor
 - Right to obtain access to PHI about a minor child
 - Personal representative agrees to confidentiality between the minor and provider
- Exceptions: When is a parent NOT a minor's personal representative?
 - When California Law does not require consent of parent / personal representative, e.g.,: reporting child abuse
 - The minor consents to the health care, e.g.,: reproductive and/or substance abuse counseling.
 - Provider's professional judgment and experience, e.g., possible victim of violence, abuse or neglect

Key HIPAA Terms & Definitions – 8

PR...Personal Representatives - Adults

- Authority to make healthcare decisions about an emancipated minor or an adult
- Right to obtain access to PHI about the individual
- Personal representative agrees to confidentiality between the patient and provider
- Exceptions: When is an adult's personal representative, guardian or conservator NOT a personal representative?
 - When California Law does not require consent of the patient's personal representative, e.g., reporting elder abuse
 - Provider's professional judgment and experience, e.g., possible victim of violence, abuse or neglect
 - The patient consents to the health care

Protected Health Information

Let's Review!

PHI is information about past, present or future medical or mental health or condition; created / received by a provider in the course of treatment/evaluation; individually identifiable; in ANY medium – written, oral or electronic.

In Addition...

PHI includes HIPAA's 18 identifiers that could be linked to the identity of the individual.

Protected Health Information Identifiers

- 1. Names**
- 2. Geocodes (zip codes)**
- 3. Dates. All elements of dates (except year, unless individual is > 89 yrs)**
- 4. Telephone numbers**
- 5. Fax numbers**
- 6. Electronic mail addresses**
- 7. Social security numbers**
- 8. Medical record numbers**
- 9. Health plan beneficiary numbers**
- 10. Account numbers**
- 11. Certificate/license numbers**
- 12. Vehicle identifiers and serial numbers (including license plate numbers)**
- 13. Device identifiers and serial numbers**
- 14. Web Universal Resource Locator (URL)**
- 15. Internet protocol (IP) address number**
- 16. Biometric identifiers (including finger or voice prints)**
- 17. Full face photographic images and any comparable images**
- 18. Any other unique identifying number, characteristic or code.**

When do HIPAA rules apply to PHI?

- When you use it
- When you disclose it
- When you store it
- When you see it on your computer
- When it is lying on your desk
- When you share it with another health care provider
- When you share it with another contracted service provider
- When you are talking about it face-to-face, in any public area
- When you are talking about it over the phone

I've got the HIPAA “Big Picture”

- Now tell me what I CAN do under HIPAA and California State Law.
- When is it okay to use & disclose PHI?
- When is it NOT okay to use & disclose PHI?
- What is the “minimum necessary” standard?

When is it OK to Use & Disclose PHI?

- TPO
 - Treatment
 - Payment
 - Healthcare Operations of the covered entity (e.g., patient transfers, QA, coding, compliance, teaching, billing, UR, etc.)
- Government requests
 - Provisions by law for reporting purposes (e.g., abuse, tumor registry, OSHPD, etc.)
- Research – IRB approval
- Patient Authorized
 - When handling a request for release of information with a patient's authorization (prescription profile, x-ray film, medical record, bill, etc.)

Reminder: Adhere to minimum necessary standard for all uses and disclosures other than treatment purposes.

When is it NOT OK to Use & Disclose PHI?

The following situations require a patient's written authorization **PRIOR** to using or disclosing PHI:

- Non-TPO purposes, e.g., a vendor's request for patients' on a specific drug
- Release of PHI to employer, e.g., a patient's boss calls to verify patient seen in ED for "x" diagnosis
- Psychotherapy Notes
- Research requests without an IRB approval
- Marketing
- Fundraising

Reminder: Adhere to minimum necessary standard for all uses and disclosures other than treatment purposes.

Minimum Necessary Standard

***“PHI is confidential...
only access the minimum amount of PHI
that
you need to know based on your job
role...”***

Minimum Necessary Standard

- “Minimum necessary” is the concept of increased confidentiality
- The sender of PHI needs to define the “need to know”, instead of releasing “all” information
- “Less is better”
- Be Aware: Fines / penalties including sanctions for disclosures and/or scrutiny for breaches will be enforced by the Office of Civil Rights (OCR)
- Be familiar with your facility’s policies that relate to privacy and security of confidential information...and abide by them!

Minimum Necessary Standard

Who, What, When – Considerations when releasing protected health information (PHI)

- Who?
 - Is the request a permitted “use / disclosure”, e.g., TPO?
 - Did the patient or representative authorize the request in writing?
 - Are there any restrictions on release of information, i.e.: Psychotherapy notes, HIV, etc.
- What?
 - Review your facility policies on disclosure of PHI (<http://manuals.ucsfmedicalcenter.org/>)
 - Adhere to releasing only that which is specified in the request
- When?
 - MNS applies to all requests for release of information

Minimum Necessary Standard

Example: Clinician request for PHI

- No limitations: Physicians and care providers who are directly and indirectly involved in the care of the patient, may access PHI without limitations.
- Physicians / care providers may disclose PHI to consulting / referring physicians.
- But...No disclosure permitted to clinicians who do not have any treatment, payment or healthcare operation responsibilities for the patient.

Minimum Necessary Standard

Example: Employee (Non-Clinician) request for a colleague's PHI

- Limitations apply to non-clinician employee requests for PHI.
- Employees who have a “need to know” based on job responsibilities may have access to PHI
- There are some exceptions, e.g., psychotherapy
- No disclosure: PHI may not be released to or accessed by employees who do not have any treatment, payment or healthcare operation responsibilities for the patient.

Self-Test

- Would you recognize the following PHI request as “non-permitted” without an authorization?
- Do you know who to refer the requests for copies of PHI to?

Examples of Non-Permitted PHI Requests

Examples:

- Clinician requesting access to spouse's PHI (Is **not** designated a personal representative)
- Clinician requesting access to a colleague's PHI;
- Non-UC pharmacy reps request for a list of patients on a treatment regimen for marketing purposes.

Reminder:

Clinician's access must be based on job duties / roles.

Examples:

- Staff member requesting access to a spouse's PHI (Is **not** designated a personal representative)
- An employee requesting access to another employee's PHI to 'check on status' out of concern.

Reminder:

Employee's access to PHI must be based on job duties / roles and the minimum necessary standard.

Let's Talk About Patient Rights and Your Responsibilities

Patient Rights

- Privacy Notice
- Patient Rights to Request:
 - a. Restrictions
 - b. Alternative communications
 - c. Accounting of disclosures
 - d. Amendments
- Complaints

Patient Right #1: Privacy Notice

- Patients must receive the “Notice of Privacy Practices” at least once after 4/14/03.
- The Notice describes the UC policy on when, why, and how information is used for treatment, payment or operations (TPO)
- We must make a ‘good-faith’ effort to obtain an acknowledgement of receipt of the notice at the initial point of patient contact (admissions, registration) or if the patient requests the notice.
- The acknowledgement must be filed in the patient’s medical record.

Patient Right #2: Requests for Access to and Copies of Designated Record Set (DRS)

- Patients may request to access their DRS and receive a copy of their DRS.
- Review the “Notice of Privacy Practices” and review facility policies for handling requests for DRS’s.
- (<http://manuals.ucsfmedicalcenter.org/>)
- Forward the request to Health Information Management Services.
- Refer to your facility policies on handling requests.

Patient Right #3: Request for Amendments / Addendums

- Patients may request amendments / addendum to their designated record set (DRS).
- Review the “Notice of Privacy Practices” which explains how patients may submit requests.
- Review policy for these requests.
- Providers may agree or disagree, but must respond within 30 days to the request.
- California Law already allows the submission of addendums.
- Refer ALL requests for amendments to Patient Relations.

Patient Right #4: Requests for an Accounting of Unauthorized Disclosures

- Patients have a right to request an accounting of external unauthorized disclosures of their designated record set (DRS) .
- Unauthorized is defined as:
 - Not covered by State Law/Statute reporting requirements
 - Not part of treatment, payment, operations
 - Not covered by HIPAA reporting requirements
 - Not covered by a patient's authorization
- Review the “Notice of Privacy Practices” which explains how patients may submit requests for accounting of disclosure;
- Review your facility's policy for handling patient requests for an accounting of disclosures.
- Refer ALL requests for accounting of disclosures to Health Information Services (Medical Records).

Patient Right #5: Restrictions

- Patients may request restrictions on disclosures of their PHI to others. UCSF is not obligated to agree to the request.
- Example: A patient may request that her physician not reveal any information to her husband, mother, brother, etc.
- If the request is reasonable and can be accommodated and we agree to the request, then we must honor the request.
- Action: Refer to facility policies on handling requests for restrictions; use of aliases; facility directory policies.
(<http://manuals.ucsfmedicalcenter.org/>)
- Be aware: “No disclosure patients” means ...NO Information may be released.

Patient Right #6: Alternative Communications

- Patients may request alternative means of communicating PHI or request that it be sent to an alternative location.
- Examples:
 - Patient requests that his bill be sent to a P.O. box, rather than a home address.
 - Patient requests that her physician make a follow-up call to her cell-phone number, rather than calling her home.
 - E-Mail: Exercise caution as email is easily misdirected; affix confidentiality statement at end of message.
- Action: Review facility policies to understand how these requests are to be handled.

Patient Right #7: Complaints

- Patients have the right to complain about violations of their privacy / security to their health plan, provider and/or the Department of Health & Human Services.
- Action:
 - Review the UC “Notice of Privacy Practices” which explains where patients may direct requests and complaints.
 - Review your facility policy for handling complaints.
(<http://manuals.ucsfmedicalcenter.org/>)

Questions About Authorizations?

Please check with your manager or supervisor.

Authorizations

- HIPAA specifies key items for a valid authorization for disclosure of PHI. These include:
- Reason for the request and expiration date
- Rescissions: Patients have the right to revoke an authorization.
- Co-ordination with any other approvals.
- Disclose: Remuneration
- Action: Refer to facility policy on authorizations and approved forms; refer requests for release of PHI to Health Information Management.

HIPAA - Personal Representatives

Disclosures to Personal Representatives for:

- Minors
- Emancipated Minors
- Adults
- Decedents

What can be disclosed to an Authorized Personal Representative?

- Use professional judgment and experience to determine what PHI should be disclosed.
- A patient's objections to disclosures should be honored
- Minimum necessary standard applies for purposes of ...
 - **Notification:** To locate or identify a family member, relative or a close personal friend involved in the patient's care
 - **Involvement:** PHI relevant to the individual's involvement in the patient's care, e.g., pick-up prescriptions, medical supplies, x-rays
 - **Payment:** Payment for healthcare services

Decedent's Rights

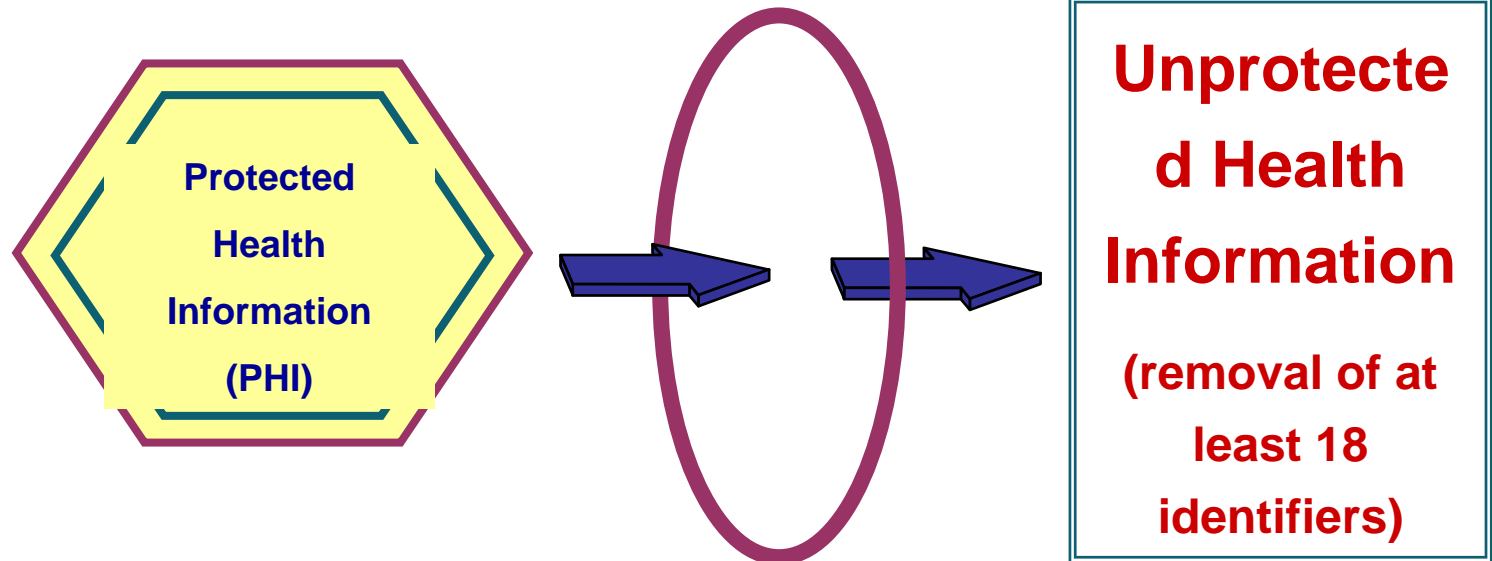
- Executor, administrator or other person, who has authority to act on behalf of a deceased person: Treat such persons as a “personal representative.”
- What can be disclosed to someone other than the decedent's Personal Representative?
- PHI about decedents has HIPAA Privacy protections
- Minimum necessary standard applies for PHI disclosure
- PHI may only be disclosed without authorization to:
 - Coroner or medical examiner - to identify the decedent and the cause of death;
 - Funeral director - as called for by law
 - Law enforcement – if death may be the result of criminal conduct
- Exception: Decedent's psychotherapy records have standard psychotherapy record protections.

If you are asked to provide aggregate data...

Considerations:

- Approval process for data requests
- Research (IRB approval necessary)
- Minimum necessary standard
- De-identify or “anonymize” the data
 - Removal of a minimum of 18 HIPAA data identifiers
 - Coding or encrypting
- Limited data set (dates only)
 - For limited purposes, e.g., health care operations, research (with IRB approval)
 - Limited data set agreement

Benefit of De-Identified Data May be used without restriction



De-Identification:

What: Removal of at least 18 PHI identifiers.

If fewer items, then the method must be certified by a statistician.

HIPAA also requires Security

- HIPAA Privacy and Security go hand-in-hand
- Privacy focus is – “What is private?”
 - PHI, individually identifiable information maintained in a designated record set
 - How and when PHI may be disclosed
 - When do you need to have an authorization?
- Security focus is – “How we keep PHI private?”
 - Protect information from accidental or intentional disclosure and from alteration, destruction or loss

HIPAA – Security Tips

- Security of electronic data:
 - Password security is key.
 - NEVER SHARE PASSWORDS.
 - Password protect your PDAs, laptops, home computers.
 - Don't leave confidential information on your computer screen or in the trash! Use locked shredder bins.
 - Use confidentiality statements and be cautious when e-mailing PHI.
 - Use caution when sending faxes. Be aware of who may view the information from both fax machines. Use cover sheets. Verify fax numbers.
 - Report breaches to your UC Privacy / Security Officer.
- Physical security of data
 - Access, transmission, storage and retention of PHI must all be secured.
 - Key access to file rooms / cabinets; automatic log-offs

HIPAA and Research

In addition to involving human subjects in clinical trials, PHI can also be associated with the use of specimen and data from humans:

- Medical records review (both living and deceased subjects)
- Biological specimen (tissue, urine, saliva)
- Biometrics (images audios, videos, fingerprints)
- Data sets (depending on type of identifiers attached)
- Recruitment of potential subjects for research from PHI sources (medical records, databases, etc).

How does a research investigator gain access to PHI from Medical Records?

Medical Records will require the investigator to show one of the following as proof of authorization to view PHI:

- Copy of CHR Approval Letter with statement of Waiver of Authorization of individual consent to access PHI
- Copy of the Informed Consent document with CHR standard wording authorizing access to individual PHI signed by the subject
- Copy of Individual Authorization for access to PHI signed by research subject

-OR-

- Exempt Certification Form with Decedent Research section completed and signed by the investigator
- Exempt Certification Form with Preparatory to Research section completed and signed by the investigator

Summary

- To build the trust with our patients, the HIPAA privacy rules call on all of us to learn and implement the privacy and security rules regarding protected health information (PHI)
- ...and abide by them!

Question #1: What is PHI?

- A. Private history information.
- B. Protected health information.
- C. Personal health information.
- D. Private health insurance.

Answer: B. Refer to slide 4 for a list of PHI data elements.

Question #2. Which of these requests for copies of medical records / billing records / images requires the patient's prior written authorization?

- A. Requests for copies of psychotherapy notes.
- B. Requests for copies of PHI from your employer.
- C. Requests for copies of your PHI from concerned fellow employees.
- D. Requests for publication / publicity.
- E. All of the above.

Answer: E. All of the above.

Question #3. Which of these is a HIPAA “disclosure” that must be logged?

- A. Release of PHI to the ME following death of a patient.
- B. Release of PHI for legal reasons.
- C. Release of PHI via e-mail or fax to the incorrect address outside of UC network.
- D. Release of PHI through a hacker attack.
- E. Lost or stolen laptop or device with PHI.
- F. All of the above.

Answer: F. See facility policies on handling breaches.

Question #4. Personal Representative

Which of these statements best describes the new HIPAA personal representative? Check all that apply.

- A.** Personal, legally authorized individual to make health care decisions on the individual's behalf
- B.** School nurse
- C.** Employer
- D.** Parent for an adult patient (not incapacitated)

Answer: A. Refer to slides 11, 12 and 13 for information on Personal Representative.

Question #5. Medical students / residents who participated in Ms. Jones's care write up the case for presentation at grand rounds.

True or False. Mark all that are true.

- A.** HIPAA's definition of "health care operations" includes conducting training programs in which students, trainees, or practitioners in healthcare learn under supervision to practice or improve their skills as healthcare providers
- B.** No authorization is needed, since this is covered in Ms. Jones's general consent
- C.** The minimum necessary information should be used, as this is not a part of direct or indirect care of Ms. Jones. Ms. Jones should not be identified by name

Answer: A, B and C are true. Refer to slides 5, 21 and 36 for more information.

Question #6. Security

With new hires & temporary personnel, when can I share my password to avoid patient care and/or billing delays? Choose the 1 correct answer.

- A. I may share my password with new personnel for up to 10 days until the person has their own password, as long as they have completed privacy training.
- B. I may post my password in a discrete area to limit access to my password.
- C. Only when temporary personnel are hired or students are visiting.
- D. Never!

Answer: D. Refer to slides 42 and 43 for more information.

HIPAA References

- General HIPAA information
<http://hipaa.ucsf.edu/>
- UCSF IT Medical Center Information
<http://it.ucsfmedicalcenter.org/>
- UCSF Information Security
<http://security.ucsf.edu>
- HIPAA Regulations
<http://www.hhs.gov/ocr/hipaa>
- HIPAA Handbook
<http://hipaa.ucsf.edu/>
- HIPAA Hotline
415-502-8448
- UCSF Privacy Officer
415-353-2750

Thank you