HIPAA and Privacy

IHS Best Practices Conference
May 24, 2017

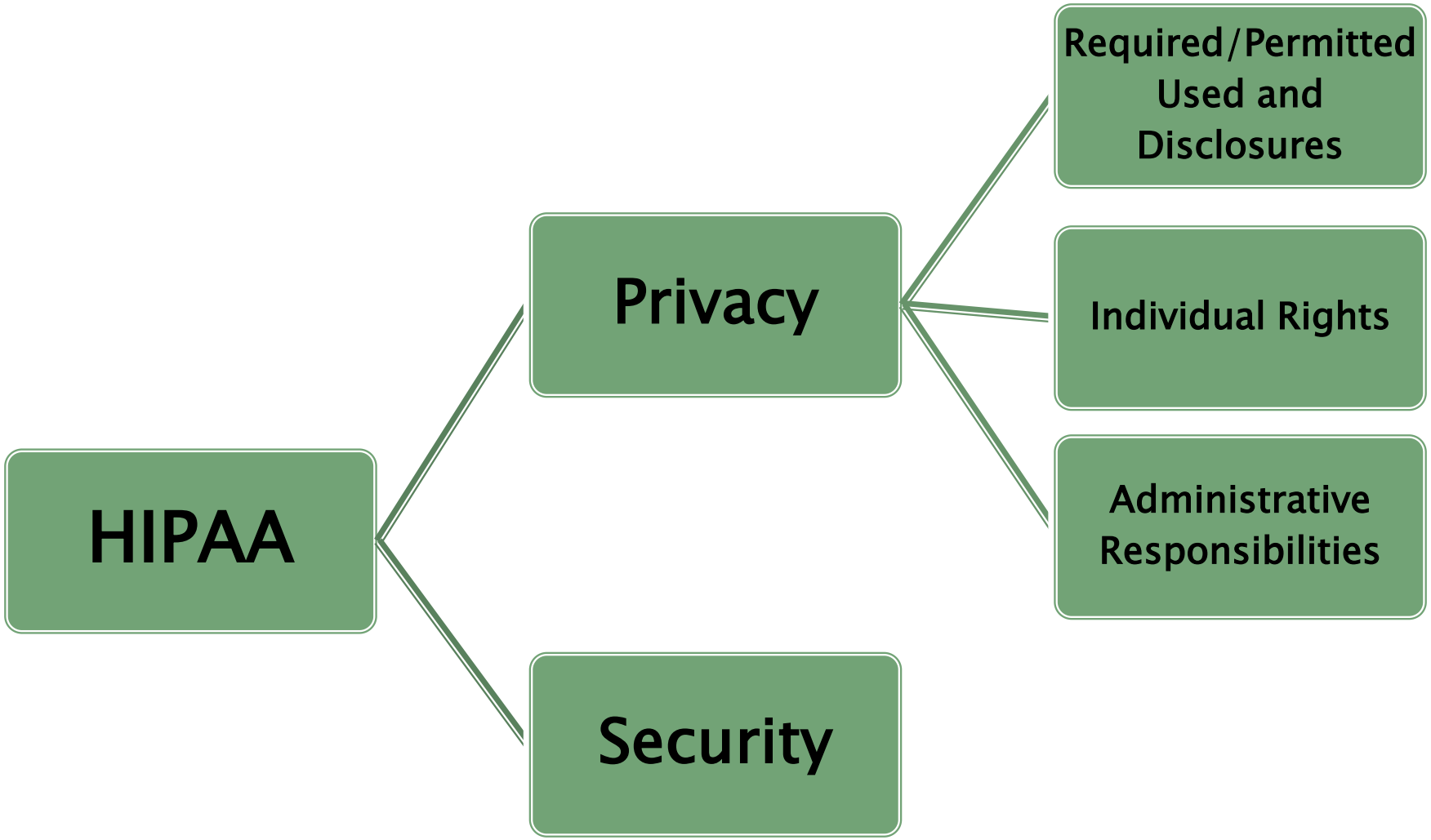
Susan Dahl, MHA, RHIA, CHC, CHPS
Chief Compliance Officer
California Rural Indian Health Board, Inc.

Objectives

- Overview HIPAA and Privacy
- Laws
- Implementation
- Sanctions

Sources: Privacy and Confidentiality

- Health Insurance Portability and Accountability Act (1996)
- Confidentiality of Medical Information Act (1982)
- HITECH Act (2010)
- Security Breach Notification Rules (2009)
- Omnibus Rule (2013)
- Patient Access to Health Records Act
- Common Law
- CA State Constitution
- Professional Associations
- And numerous other CA Health and Safety Codes


HIPAA
Privacy
Security
Required/Permitted Used and Disclosures
Individual Rights
Administrative Responsibilities

The Privacy Rule

- Sets the federal floor for health information privacy
- Establishes individual rights
- Establishes administrative requirements
- **Does not** prevent covered entities from establishing internal policies that provide greater protections, or that offer consumers greater rights
- **Does not** preempt more stringent State laws

A **covered entity** may not use or disclose protected health information except as permitted or required.

Covered Entities

HIPAA/HITECH

- **Health Plans** – A plan that pays the cost of medical care. Includes Medicare and Medicaid. Does NOT include health plans with less than 50 participants administered by the employer.
- **Health Care Providers** – A provider of medical services that transits any health information in electronic form.
- **Clearinghouses** – Processes health information from non-standard content into standard transaction. This does NOT include Third Party Administrators.
- **Business Associates** – Individuals and organizations that use health information to perform functions or service for a HIPAA Covered Entity

CMIA

- **Medical Providers**
- **Health Plans**
- **Pharmaceutical companies**

Amendment in 2008 extends health data protection to:

"any business organized for the purpose of maintaining medical information"

Business Associates

Business associate services are: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

Business associate functions and activities include:

- claims processing or administration
- data analysis
- processing or administration
- utilization review
- quality assurance
- billing
- benefit management
- practice management

A covered entity (or BA) may not **use or disclose** protected health information except as permitted or required.

Uses and Disclosures

Use – The sharing of information *within* an entity that maintains such information.

Disclosure – The release, transfer, provision of, access to, or divulging of information *outside* of the entity holding the information.

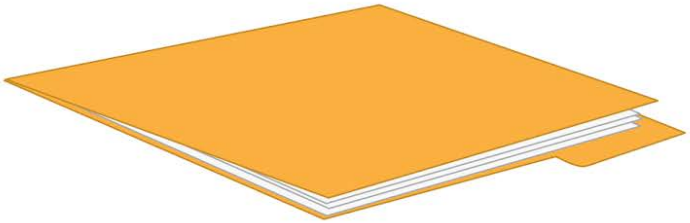
Minimum Necessary Standard

PHI may only be used or disclosed when it is necessary to satisfy a particular purpose or carry out a function.

Not everyone at the covered entity is entitled to the same information.

Patient's entire medical history

What you actually need



Role-based access to PHI

The front desk/intake staff: Responsible for the intake process and ensuring that all paperwork is filled out correctly for identification and billing purposes. Under minimum necessary, they would have access to all of the information mentioned above, but should not have access to the patient's STD test results or x-ray reports.

Role-based access to PHI

Phlebotomist: Individuals who draw the blood would likewise need access to the patient's demographic information, as well as procedure codes, etc. The phlebotomist usually verifies the patient information on the requisition a second time and uses the data to generate the identification labels that are wrapped around the vials of blood; therefore, they require access to PHI to complete their job duties.

*If they are not responsible for generating/reading the test results, they would not have access to the results system.

A CE or BA may not use or disclose **protected health information** except as permitted or required.

Protected Health Information (PHI)

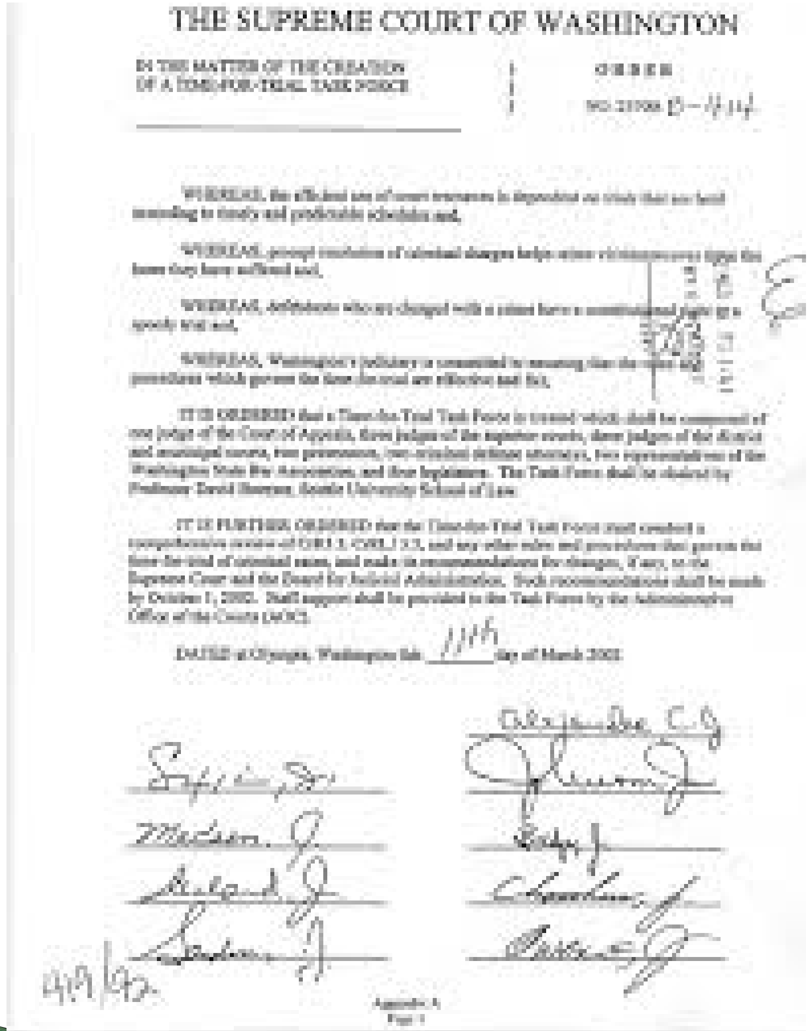
Information collected *from* an individual, created or received *by* a covered entity **and** relates to:

- the past/present/future physical or mental health condition of an individual
- the provision of healthcare to an individual or
- the past/present/future payment for the provision of healthcare to an individual

AND

- reasonably identifies the individual
- Is maintained in electronic record or any other record form

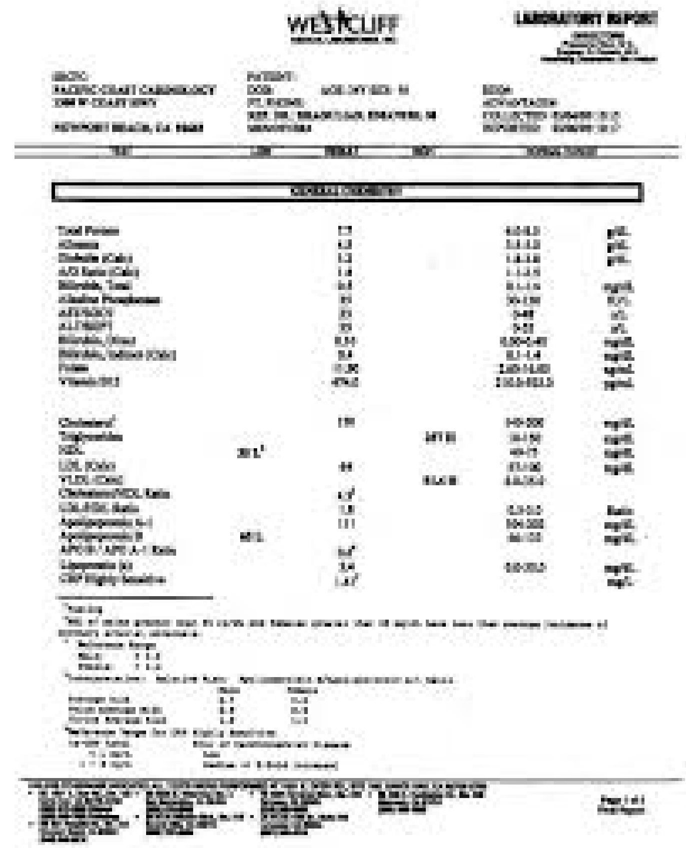
Do these contain PHI?


THE SUPREME COURT OF WASHINGTON

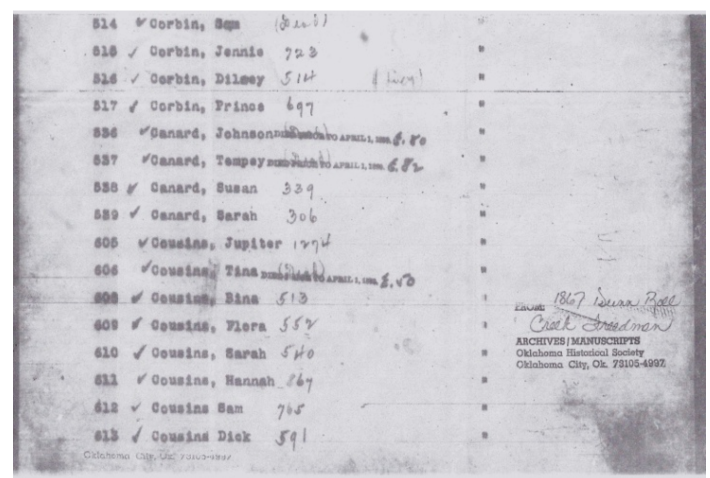
IN THE MATTER OF THE CREATION OF A TIME-FOR-TRIAL TASK FORCE

ORDER

DATED at Olympia, Washington this 11th day of March 2002.


WESTCLIFF

LABORATORY REPORT


514 ✓ Corbin, Sam
515 ✓ Corbin, Jennie 723
516 ✓ Corbin, Dilsey 514
517 ✓ Corbin, Prince 697
536 ✓ Canard, Johnson
537 ✓ Canard, Tempey
538 ✓ Canard, Susan 339
539 ✓ Canard, Sarah 306
605 ✓ Cousins, Jupiter
606 ✓ Cousins, Tina
608 ✓ Cousins, Bina 513
609 ✓ Cousins, Flora 552
610 ✓ Cousins, Sarah 540
611 ✓ Cousins, Hannah
612 ✓ Cousins Sam 765
613 ✓ Cousins Dick 591

ARCHIVES/MANUSCRIPTS
Oklahoma Historical Society
Oklahoma City, Ok. 73105-4997

CALIFORNIA RURAL INDIAN HEALTH BOARD, INC. SINCE 1969

3 – Part Test

- Is it Health Information?
- Does it reasonably identify an individual?
- Is it maintained?

If you answered YES to all 3, you are working with PHI!

If it's not PHI, or HIPAA/CMIA, do NOT apply!

Context Matters

You find page 2-of-2 of a patient's visit summary on the ground in the hallway, it includes a history of drug abuse and most recent depression screening results. *The client's name, SSN, MRN, and DOB are not on the note.*

Is this PHI?

- Is it Health Information?
- Does it reasonably identify an individual?
- Is it maintained?

A CE OR BA may not use or disclose PHI except as **permitted or required**.

Required Disclosures

The HIPAA Privacy Rule requires disclosure in two instances:

1. To the individual
2. To the federal government

California Law expands on the instances to include

- Pursuant to court order
- Search Warrant
- When otherwise specifically required by law

Permitted Disclosures

The Privacy Rule permits disclosures in six instances:

1. **Treatment**
2. **Payment**
3. **Healthcare Operations**

TPO

4. Incidental disclosures
5. Opportunity to agree or object
6. Public Policy

Case Scenario

You are the Health Information Manager with access to the NextGen EHR.

One day while eating lunch with a group of clinic staff, including a new dietician, it is mentioned that they are working on a project and could really use some specific data about patients with diabetes. After some thought, you determine that you can easily extract that data from the EHR.

Is this a permissible use of EHR data?

Does the TPO exception apply?

What part does the minimum necessary standard play?

Explain.

Case Scenario

You are a medical assistant who is preparing for tomorrows patient load. You notice a patient on the schedule who you recognize from last week. You've seen her test results, and you KNOW she is going to need a prior authorization for a referral the doctor will be making. You want to start the paperwork tonight because you want to be considerate of your patient and doctor's time tomorrow. Do you see any problems with this?

Is this a permissible use?

Does TPO exception apply?

Patient Rights

1. Notice of Privacy Practice – HIPAA
2. Inspect and Copy (Access) – HIPAA, CA
3. Accounting – HIPAA
4. Request Amendment – HIPAA Request Addendum –CA
5. Request Restriction – HIPAA
6. Request Confidential Communication – HIPAA
7. File a Complaint –HIPAA

Case Scenario

- Staff denied a client access to his records on the basis that a portion of the record was created by a physician not associated with the clinic.

- Is this okay?

Authorization

State and federal privacy laws require separate written authorization for certain types of sensitive information.

These include:

- Psychotherapy notes (HIPAA Definition)
- Drug and alcohol treatment records
- HIV status and test results, except for diagnosis, care, and treatment
- Genetic test results for a life or disability insurance application

Impermissible Use/Disclosure

- Any access, viewing, use, or disclosure not permitted by HIPAA or authorized by patient.
- Presumed to be a breach unless risk assessment determines there is low probability PHI has been compromised.

Risk Assessment

- 4 factor analysis
  - Nature and extent of PHI
  - Unauthorized person using/receiving PHI
  - Actual acquisition or viewing PHI
  - Mitigation factors

Compliance/Privacy Officer Role

- Conduct risk assessment
- Examine the events that lead to the impermissible disclosure
- Incidents provoke analysis of the relevant policies and procedures as well as training.
- Track all impermissible disclosures (including breaches) to support analysis of problems that may lead to more serious issues in the future.

  Example, just because you have not graduated to a breach for a number of impermissible disclosures and uses, it does not mean that there are no weaknesses to address

Case Scenario

You send a fax containing PHI to what you know to be a secure fax number. You find out later, you transposed two digits.

Is this an impermissible disclosure?

What if the person who received the fax calls you right away, and tell you they shredded it?

What do you do first?

Breach Notification

- California was the first state to enact a Breach Notification Law, this was not addressed by HIPAA
- HITECH enacted requirements more stringent than CA Law (unauthorized insider, or outsider access)
- Patient must be notified in writing

EXCEPT

- CA Law requires licensed entities to notify individuals affected by a breach within 15 days, as opposed to HITECH's requirement of 60 days after the day of discovery

Enforcement

- HIPAA and HITECH Act
  - Office for Civil Rights
  - Patient Complaints

- State Attorneys General
  - HITECH Act authority – Civil Actions
  - Notify HHS prior to bringing action
  - Patient complaints for non-licensed entities and individuals

Civil Monetary Penalties

- Tier 1 – Accidental. (Entity did not know, and by exercising reasonable diligence, would not have know it violated the rule)
  - $100 to $50,000 per violation, up to $1,500,000 for identical violations
- Tier 2 – Not Willful Neglect but not Accidental (Violation due to reasonable cause and not Willful Neglect)
  - $1,000 to $50,000 per violation, up to $1,500,000 for identical violations

Civil Monetary Penalties

- Tier 3 – Willful Neglect, but Corrected (Violation was due to Willful Neglect but violation was corrected during the 30 days after the entity knew or should have know that the violation occurred
  - $10,000 to $50,000 per violation, up to $1,500,000 for identical violations
- Tier 4 – Willful Neglect, Not Corrected within the 30 day period
  - $50,000 or more per violation, up to $1,500,000 for identical violations

Examples: Fines

- Theft of Unencrypted Laptop or USB
  - Hospice $50,000;
  - State and a national clinic $1.7 million
- Software & Internet
  - Clinic $100,000: Surgery schedule publicly available on Internet; staff using personal emails; no training
  - BH clinics $150,000: malware compromised security; failed to update IT resources: not follow policies
- Inappropriate disposal of records
  - Pharmacy Chain $2.25 million: PHI in dumpster
  - Hospital $800,000: left boxes in physician driveway
  - Health Plan $1.2 million: failed to erase information on Photocopiers' hard drives
- Failure to provide medical records
  - Heath Center $4.3 million ($3 million for failing to cooperate)

And There Are Criminal Provisions

- Knowingly obtaining PHI
  - Up to $50,000 and 1 year in prison
- Obtaining PHI under False Pretences
  - Up to $100,000 and up to 5 years in prison
- Intent to Sell, Transfer, or Use PHI for Commercial Advantage, Personal Gain, or Malicious Harm
  - Up to $250,000 and up to 10 years in prison

Example: Criminal Conviction

- 2003 – California medical researcher and surgeon:
  - received a dismissal notice; accessed several hundred medical records before leaving his job
  - Los Angeles hospital with patient pool including many well-known celebrities
- 2010 – pled guilty to misdemeanor charges in violation of HIPAA's medical privacy protections
  - No evidence that the doctor was trying to sell the medical records
- Sentenced to three months in a federal prison

Implementing Privacy Program

Sanctions and Enforcement

Implementation – Must Haves

- Privacy Officer
- Policies and Procedures
- Training
- Communication System
- Reporting System
- Auditing and Monitoring
- Response and Corrective Action

Privacy Officer

- Often Compliance Officer
- Sufficient time for privacy activities
- Working knowledge of state and federal laws

Policies and Procedures

- Written
- Readily available
- Current

Training

- New employee
- Annual
  - Role based
- New policies

Communication System

- Where to report issues
- Anonymous reporting
  - Hotline, drop box
- Where to go for questions
- Newsletter, email, other methods

Reporting System

- Manager/Supervisor
- CEO
- Compliance/Privacy Officer
- Reports to Governing Body/Board

Auditing and Monitoring

- Regular process
- Identified risk areas
- Internal or external
  - Compliance/Privacy Officer (auditing or monitoring)
  - Operations department (monitoring)
  - Consultant (auditing)
  - Funding agency

Response and Corrective Action

- Investigate reported issues/concerns
  - Sufficient information to investigate
- Develop Corrective Action Plan for identified issue
  - Operational staff
- Sanctions
  - Employees, contract
  - Policy, equitable/standard sanctions
- Re-audit after Corrective Action Plan implemented

For Questions or More Information

- Contact
  - Susan Dahl
    - Chief Compliance Officer
    - California Rural Indian Health Board
    - Sdahl@crihb.org
    - 916-929-9761