PROTECTING PATIENT PRIVACY

HIPAA, HITECH, AND CALIFORNIA LAW

THREE HIPAA RULES

1. Privacy
2. Security
3. Transactions and Code Sets

PRIVACY RULE

- Protects personal health information (PHI)
- Limits use of PHI without patient authorization
- Gives patients rights over health information

SECURITY RULE

- Establishes national standards for securing patient data that is stored or transferred electronically.
- Requires placement of physical and electronic safeguards.

TRANSACTIONS AND CODE SETS

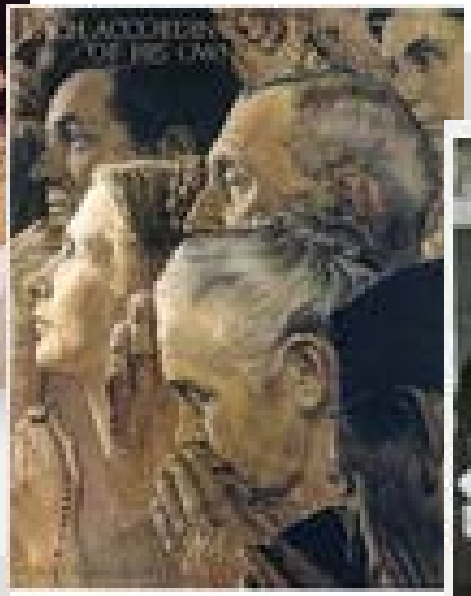
HIPAA transaction and code set standards create a uniform way to perform electronic data interchange (EDI) transactions for submitting, processing, and paying claims.

HIPAA VERSUS STATE LAW

- HIPAA provides a minimum standard – i.e. a floor
- State law MAY exceed HIPAA requirements
- California breach reporting

The Four Freedoms – Norman Rockwell, 1943

Speech



Worship

Fear

Want

PATIENT PRIVACY RIGHTS

OFFICE FOR CIVIL RIGHTS

Your Health Information Privacy Rights 1

YOUR HEALTH INFORMATION PRIVACY RIGHTS

Most of us feel that our health information is private and should be protected. That is why there is a federal law that sets rules for health care providers and health insurance companies about who can look at and receive our health information. This law, called the Health Insurance Portability and Accountability Act of 1996 (HIPAA), gives you rights over your health information, including the right to get a copy of your information, make sure it is correct, and know who has seen it.

Get It.

You can ask to see or get a copy of your medical record and other health information. If you want a copy, you may have to put your request in writing and pay for the cost of copying and mailing. In most cases, your copies must be given to you within 30 days.

Check It.

You can ask to change any wrong information in your file or add information to your file if you think something is missing or incomplete. For example, if you and your hospital agree that your file has the wrong result for a test, the hospital must change it. Even if the hospital believes the correct, you still have the right to have your disagreement noted in your file. In most cas should be updated within 60 days.

Know Who Has Seen It.

By law, your health information can be used and shared for specific reasons not directly your care, like making sure doctors give good care, making sure nursing homes are cle reporting when the flu is in your area, or reporting as required by state or federal law. In cases, you can find out who has seen your health information. You can:

Get It

Check It

Know who has seen it

NOTICE OF PRIVACY PRACTICES

Give to patient at first encounter

Display prominently in patient areas

Post on facility website

ACCOUNTING OF DISCLOSURES

- No charge for annual accounting
- Reasonable fee for additional accounting
- Certain disclosures may be made under the TPO (treatment, payment, operations) provision

RIGHT TO ACCESS

Copies of records

- Timelines
  - HIPAA – 15 days
  - California – 5 days

Charges

- HIPAA – costs of supplies and labor (but not retrieval)
- California – Varies (up to 25 cents per page)

Providers must supply records in format requested by patient whether paper or electronic

RESTRICT ACCESS

- Patient must submit written request to restrict
- Health facility is NOT required to agree
- Facility MUST honor restriction (if agreed)
- Need to have standard process to agree/deny restriction request

REQUEST CORRECTION

- Facility MUST have written policy and procedure
- Patient must submit written request
- Amend OR deny request
- Must notify patient of approval or denial

IMMUNIZATION INFORMATION

Providers may release immunization information to the child's school with verbal consent from the parent

NO RELEASE TO INSURANCE

Patients who pay cash for a service can request that information about the service be WITHHELD from the insurance company.

ONLINE ACCESS TO RECORDS

Indian Health Service will release the Personal Health Record (PHR) in September 2014 to meet Stage 2 MU requirements for online access to health information.

HITECH AND BUSINESS ASSOCIATES

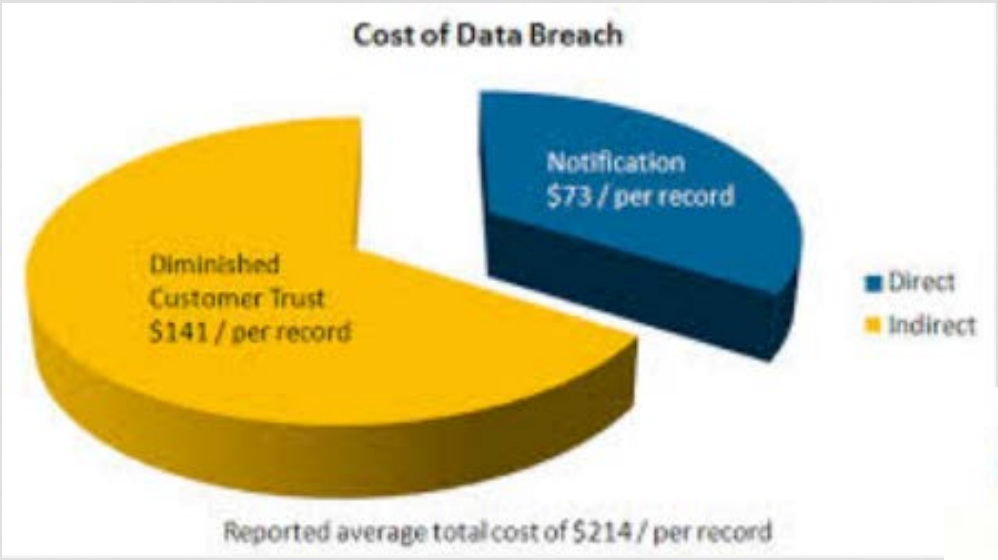
The HITECH final rule holds business associates to the same standard as covered entities

All Business Associate agreements MUST comply by September 2013

WHO IS ACCESSING PATIENT INFORMATION

- Access by “need to know” – User class
- Note titles – i.e. BH note titles with various levels of access by user class
- Sensitive patient tracking and auditing

HIPAA AND HITECH



PROTECTING PATIENT INFORMATION

- Data at rest
- Data in motion

DATA AT REST

Includes:

- Files stored on a company's local hard drive
- Copies of the file stored on onsite and offsite
- Backup tapes and files on the servers of the storage area network (SAN)

DATA IN MOTION

- Data that is exiting the network via email, web, or other Internet protocols.

SECURITY RISK ASSESSMENT

A Security Risk Assessment (SRA) helps to reveal areas where an organization's protected health information (PHI) may be at risk.

A complete SRA will consider:

- Administrative
- Technical
- Physical

QUESTIONS

???

Indian Health Service
California Area Office
MARILYN FREEMAN, RHIA
EHR and VistA Imaging
Health Information Management
Meaningful Use

650 Capitol Mall, Suite 7-100
Sacramento, CA 95814

(916) 930-3981, X362
(916) 716-1908
marilyn.freeman@ihs.gov