The Twentieth National HIPAA Summit

Healthcare Privacy and Security After HITECH and Health Reform

A Hybrid Conference and Internet Event

Introduction of Certifications

Lorna L. Waggoner - Certified HIPAA Professional

ecfirst

Certified HIPAA Administrator (CHA)

Certified HIPAA Professional (CHP)

Certified Security Compliance Specialist (CSCS)

HIPAA ACADEMY™

HIPAAacademy.Net

On-line learning packages

- Allow you to work at your own pace
- Study from anywhere you have internet access (work, home, library)
- Gives you facts in laymen's terms
- Offers Questions at the end of each section so you can check your learning
- Allows you to go back and re-examine the rules when you have specific examples to follow-up on.

Certification Exam

- Nothing under HIPAA requires you or your organization to be Certified
- You are required to have the knowledge and follow the guidelines
- Certification – validates your learning
- Certification is a credential
- Hands on experience is equally or more important

Certified HIPAA Administrator (CHA)

In depth look at the HIPAA Privacy Rule

- Patient Rights
- Penalties
- Notice of Privacy Practices
- Authorization
- Business Associate Agreements
- Use and Disclosure
- De identified information
- Minimum Necessary
- Marketing
- HITECH Act

CERTIFIED HIPAA ADMINISTRATOR™
HIPAA ACADEMY

Certified HIPAA Professional (CHP)

- CHA is the first section of CHP (Privacy)
- Electronic Transactions
- Code Sets
- Identifiers
- Introduction to the Security Rule
  - Safeguards
  - Standards
  - Implementation Specifications

CERTIFIED HIPAA
PROFESSIONAL
HIPAA ACADEMY

Certified Security Compliance Specialist (CSCS)

- Regulatory Compliance and Security
  - State of Security
  - U.S. Legislations
    - FDA’s CFR 21
    - GLB
    - NERC CSS
- Important International Regulations
- Financial Services and Security
- PCI DSS Requirements
- ISO 27001/2 Standards
- U.S. Government Security Requirements
  - California’s SB 1386 and SB 541
  - California’s AB 1950, AB 1298, and AB 211
  - Nevada’s 597.970
  - Massachusetts’s 201 CMR 17.00
  - Data Breach Challenges
  - Encryption Requirements
- NIST Standards & Guidance
- Business Continuity Planning (BCP)
- Cyber Security Strategy

CSCS™
CERTIFIED SECURITY
COMPLIANCE SPECIALIST

Today's curriculum

8:00 a.m. **Introduction and Overview**
8:15 a.m. **Introduction to HIPAA/HITECH Act**
9:00 a.m. – 9:45 a.m. **Introduction to HIPAA Privacy**
9:45 a.m. – 10:30 a.m. **Advanced HIPAA Privacy Topics**
10:30 a.m. **Break**
10:45 a.m. – 11:30 a.m. **Overview of HIPAA Security**
11:30 a.m. **Faculty Q&A**
12:00 noon to 1:00 p.m. **Lunch on our own**

Questions

Contact: Lorna.waggoner@ecfirst.com or 877-899-9974 x 17

www.ecfirst.com

www.hipaaacademy.net

HIPAA/HITECH Act Compliance Training

Instructor

Lorna L. Waggoner CHP

Director of Business Development

March 26, 2012

ecfirst

HIPAA ACADEMY™

HIPAAacademy.Net

Class Objectives

- Meet the compliance requirement of the HITECH Act as a Business Associate
- Understand what you must do to be HIPAA/HITECH compliant
- Learn specifics necessary for your organization's size
- Debunk myths and folklore

A Guarantee of Privacy

- Proactively protecting our information
- Keeping our information confidential so we are not prejudged
  - Jobs, promotions
  - Lack of healthcare
  - Unnecessary stress

H.I.P.A.A.

HIPAA is the acronym for Health Insurance Portability and Accountability Act.

Speaking the same language

- HIPAA has very specific terminology to learn
- Legal documents will be a part of your HIPAA Preparedness:
  - Policies
  - Procedures
  - Business Associate Agreements

Let’s Get Started

eHIPAA ACADEMY™

HIPAAacademy.Net

Learning Objectives Section 1

- What is HIPAA?
- What does HIPAA/HITECH do?
- Do the rules apply to me?
- What am I suppose to be doing?
- What is considered PHI?
- What are the HIPAA penalties?
- Which terminology do I need to know?
- What changes do the HITECH Act bring?

Health Insurance Portability and Accountability Act

Also known as the Kennedy -Kassenbaum Bill

Public Law 104-191 [H.R. 3103] - August 21, 1996

Ensures continuation of health insurance

Protects the privacy of patient-identifiable information in any media form

HIPAA At A Glance

- Improve Insurance Portability and Continuity
- Combat Health Care Waste, Fraud and Abuse
- Promote Medical Savings Accounts
- Improve Access to Long-Term Care

Patients Have Rights

Under HIPAA:

- Access to information
- How information is shared in certain situations
- Protecting privacy

Who knew - we did not have these rights before HIPAA?

Five HIPAA "Titles" or Parts

Title I – Health care access, portability, and renewability

Title II – Preventing health care fraud and abuse, ADMINISTRATIVE SIMPLIFICATION, Medical liability reform

Title III – Tax-Related Health Provisions

Title IV – Application and Enforcement of Group Health Plan Requirements

Title V – Revenue Offsets

Administrative Simplification??

Who came up with that phrase?

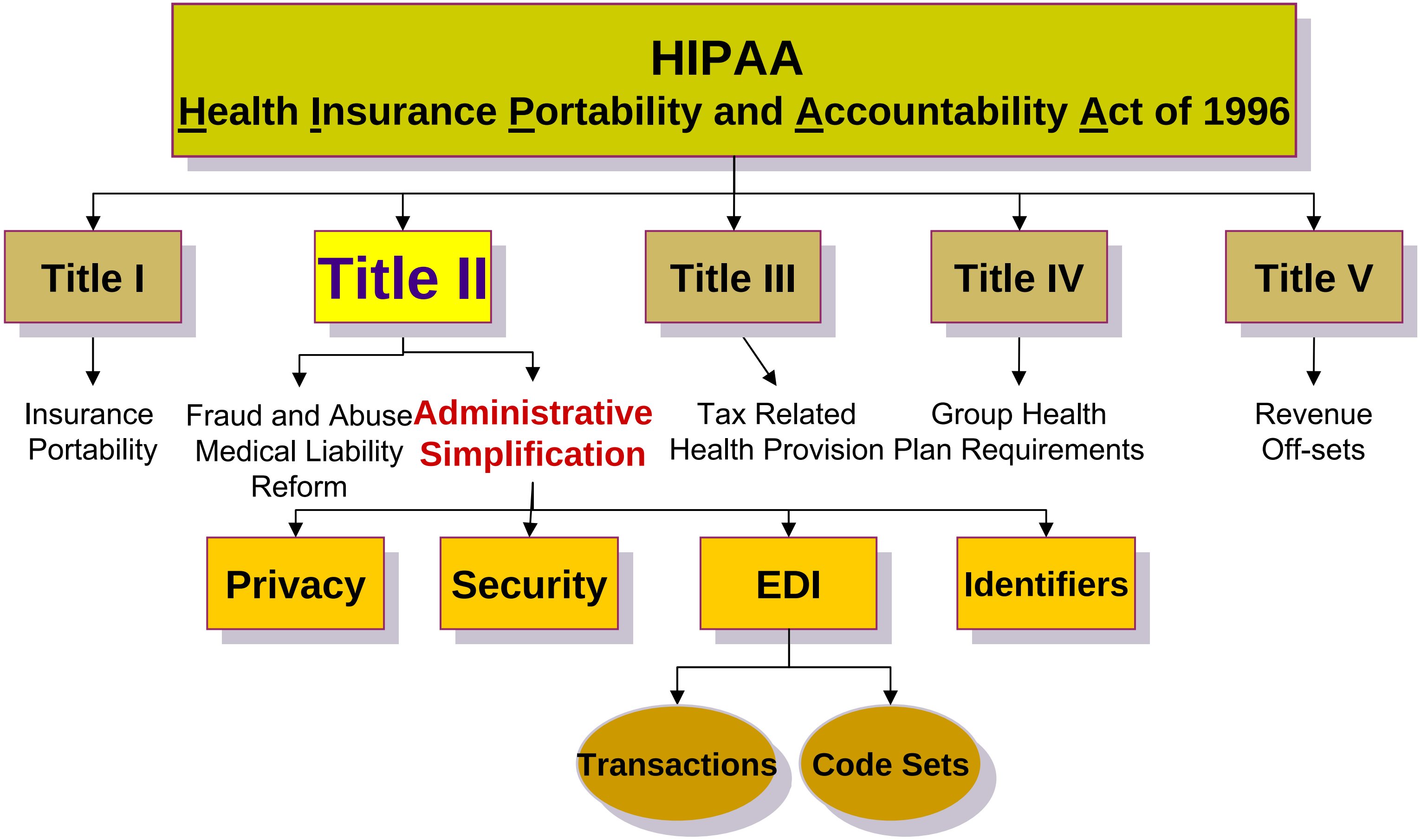
Today we see the simplicity

In 1996?

It seemed like science fiction – a computer on everyone’s desk!

It has been a big change.

How does Privacy fit into HIPAA?



HIPAA

Health Insurance Portability and Accountability Act of 1996

Title I

Insurance Portability

Title II

Fraud and Abuse Medical Liability Reform

Administrative Simplification

Privacy

Security

EDI

Transactions

Code Sets

Identifiers

Title III

Tax Related Health Provision

Title IV

Group Health Plan Requirements

Title V

Revenue Off-sets

Prior to HIPAA

There were no standards:

- Insurance companies and providers
  - Did their business
  - The way they wanted to
  - No consistency
- Unnecessary expenses

Before HIPAA – Cost estimates

- 20% of every healthcare $ spend on Administration
- 11% lost on fraud and abuse
  - Medicare fraud – huge problem
    - We were a part of the problem – carelessness

In the news – 2012
Arrest in $116 Million Fraud Scheme

An assistant administrator at a Houston hospital has been arrested on charges related to his alleged participation in a $116 million Medicare **fraud** scheme.

The **fraud indictment** alleges that Mohammed Khan used his position at the hospital to submit false claims to Medicare for mental health treatment. "According to the charges, he paid kickbacks to patient recruiters, owners of group homes and assisted living facilities and beneficiaries so that he could fill his hospital with patients for whom he could bill the government for medically unnecessary services or services that were never provided," says Lanny Breuer, assistant U.S. attorney general. The kickbacks, prosecutors say, included cigarettes, food and coupons redeemable for items at the hospital's "country stores."

The first step for HIPAA

National Standards for electronic health care transactions, codes, and identifiers will allow compatible formats between health care providers and health care plans.

Bigger Challenges

Changes to the current business practice
(they still do not see it as broken)

So many systems to deal with:

- Enterprise Resource Planning (ERP)
- Patient Billing
- Accounting
- Nursing Care Systems
- Pharmacy System
- Document Imaging
- Third Party clearinghouse system

ARRA and HITECH Act

- American Recovery and Reinvestment Act of 2009 (ARRA)
- Signed by President Obama
- February 17, 2009
- Includes Heath Information Technology for Economic and Clinical Health Act (HITECH Act)
- Many changes happened from 2/17/09 to 2/23/10

Who's Who & Estimated Implementation Costs

- Department of Health and Human Services (HHS)
- enforces HIPAA
  - Centers for Medicare and Medicaid Services (CMS)
  - Office for Civil Rights (OCR)
- Gartner Group – research
- American Hospital Association (AHA)

Cost and Estimates

- AHA said hospitals nation wide would spend 22 Billion
  - First 5 years
- Were intended to be recouped from costs savings
- Found through electronic initiatives.
- ARRA estimated over $27 Billion for technology in 2009

Top new IT investment for 2011

In an *InformationWeek Analytics'* healthcare IT priorities survey of 357 U.S. business technology professionals released earlier this year.

- EHR
- CPOE
- e-prescribing
- New computer hardware
- Upgrades to security software and IT infrastructure
  - Networking
  - web portals
  - storage products

Money was not the only concern

In 2005 research told us:

- 67% Concerned about Privacy of Medical Health information
- 52% Feel information will be used to discriminate against them in their jobs
- Only 32% will share their information with other health officials not involved in their care

Here is where we see the Savings

Manual vs. Electronic Processing

Michigan Health Management Information System (MHMIS) Cost Analysis

	Claims Submission	Claims Payment	Employee Enrollment	Claims Status Request	Patient Referral	Insurance Eligibility
Manual Costs	**$10.00**	**$10.00**	**$20.00**	**$6.00**	**$20.00**	**$6.00**
Electronic Costs	**$ 2.00**	**$ 2.00**	**$ 2.00**	**.25**	**$ 2.00**	**.25**
Potential Savings	**$ 8.00**	**$ 8.00**	**$18.00**	**$5.75**	**$18.00**	**$5.75**

A few years later a company looking at Physician Practices said the Manual costs were slightly lower but everyone agrees the Savings are somewhere between 50% - 90%

Healthcare Industry

Largest industry in the USA

- Almost 18% of the U.S. gross domestic product
- Growing faster than the economy
- Consistently grew over the past several years

Significant challenges

- Medical errors – 5th leading cause of death (2 yrs ago it was the 8th)
  - 98,000 deaths annually
  - Millennium Research Group (MRG)June 2007
  - EHR's will improve this
- 250,000 people die in the U.S. each year due to surgical errors, mistaken diagnostics, incorrect prescribing, hospital-acquired infections and inadequate care (IBM July 2006)
- 75,000 died because they did not have insurance

Improving the Quality of Care

Medical errors in the healthcare system arise from miscommunication, physician order transcription errors, adverse drug events, or incomplete patient medical records," says David Plow, Senior Analyst at MRG.

"Generally, medical errors are caused by overcrowded, understaffed clinical areas with complex workflow patterns, and incomplete or inefficient communication between clinical areas. T

In the future; professionals within each clinical area are able to access and use information pertinent to a patient's medical profile and history. As a result, HER‟'s will effectively help prevent errors and enhance patient safety.

Healthcare Industry Solutions

- Future is about innovation and integration of technology

- Increase efficiency, improve care, and save consumers time

- Save lives

Who does HIPAA apply too?

Four categories:

- Payers
- Providers
- Clearinghouses
- Business Associates

What is a Covered Entity?

1. Health Plan: Provides or pays the cost of medical care.

2. Health Care Clearinghouse: Processes health care transactions for providers and insurers.

3. Health Care Provider: Person or entity who is trained and licensed to give, bill, and be paid for health care services…

   via electronic transactions

Business Associate Test

1. Are they a performing a function for us or on our behalf?

2. Are they a member of our workforce?

3. Do they have access to PHI (Protected Health Information)?

Yes/No/Yes Pattern = Business Associate

Good News

There is no HIPAA-in-a- box solution

Entities are required to do what is:

Reasonable and Appropriate
Also
Measurable and Manageable

That is not necessarily easier!

Who might be a Business Associate?

- ***Attorney***
- ***Accountant***
- ***Consultants***
- ***Cleaning Service***
- ***Data Aggregation***
- ***Vendors***

Vital Business Contract Inclusions

1. The business associate must use the PHI ONLY for the purpose for which it was shared by the covered entity.
2. The business associate must assume the responsibility to safeguard the information from misuse.
3. The business associate must comply with the covered entity's obligation to provide individuals with access to their health information and a history of certain disclosures – for some BA's.

Health Information Technology for Economic and Clinical Health Act (HITECH Act)

- Effective 9/23/2010
- BA’s will be required to meet the same Privacy and Security Compliance regulations as Covered Entities
- They will also be subject to the penalties
- This is a sweeping change

Breaches since 2003

Business Associates

- Required to report breaches to the CE
- As stated in the BAA
- Assuming they have a BAA
- Nothing else was required

Breaches effective 9-23-09

HITECH Act

- If either CE or BA becomes aware of a Breach CE is required to report the breach to HHS.
- Will be required to notify patients if there is a breach of unsecured PHI within 60 days (calendar days) of discovery.
- California – 5 days

Definition of a Breach

- Breach refers to the unauthorized
  - acquisition, access, use, or disclosure
  - Protected Health Information (PHI)
- Discovered on the first day is known to the CE or the BA
- Compromises the security or privacy of the data
  - significant risk of financial, reputational, or other harm to the individual

Breach Resolution

- Risk Assessment
  - Mitigation of impermissible use or disclosure
    - Reduced risk or harm
  - Data returned prior to improper access
  - Type and amount of data involved
  - Document the risk

There is more……..

- Breaches involving 500 or fewer patients of the breach and must annually submit a log of breaches that occurred throughout the calendar year to HHS – OCR investigates.
- An encrypted laptop or jump drive in the hands of an unauthorized person is not considered a breach as it is undecipherable.

There is still more……

- Breaches involving 500 or more patients (from one state) are required to notify HHS immediately
- HHS will post the information on their website.
  - After they have investigated
  - A breach has been confirmed
- Additionally, the media in the jurisdiction those patients breached reside must be alerted.

None of us are getting out of this alive!

We all have to do it!

HIPAA Acronyms

Patient Identifiable Information (PII)

Here are items that will identify the patient:

Name	**Fingerprint**
Address	**Telephone #**
City	**Fax #**
Country	**Medical Record #**
Zip Code	**Insurance #**
Social Security #	

Many things Identify us – there is not a list.

IIHI

- Individually Identifiable Health information is
- PII with Health information
  - SS# or Name of an individual
  - With sore feet, heart condition or cancer

PHI

Protected Health Information
Is information that is IIHI

Just a name or a SS#
Or
Just a medical condition does not need to be protected

Why HIPAA?

"…one out of every six people engages in some form of privacy-protective behavior…including withholding information, providing inaccurate information…and – in the worst cases – avoiding care altogether."

Preamble to HIPAA regulation

HIPAA is a good thing….

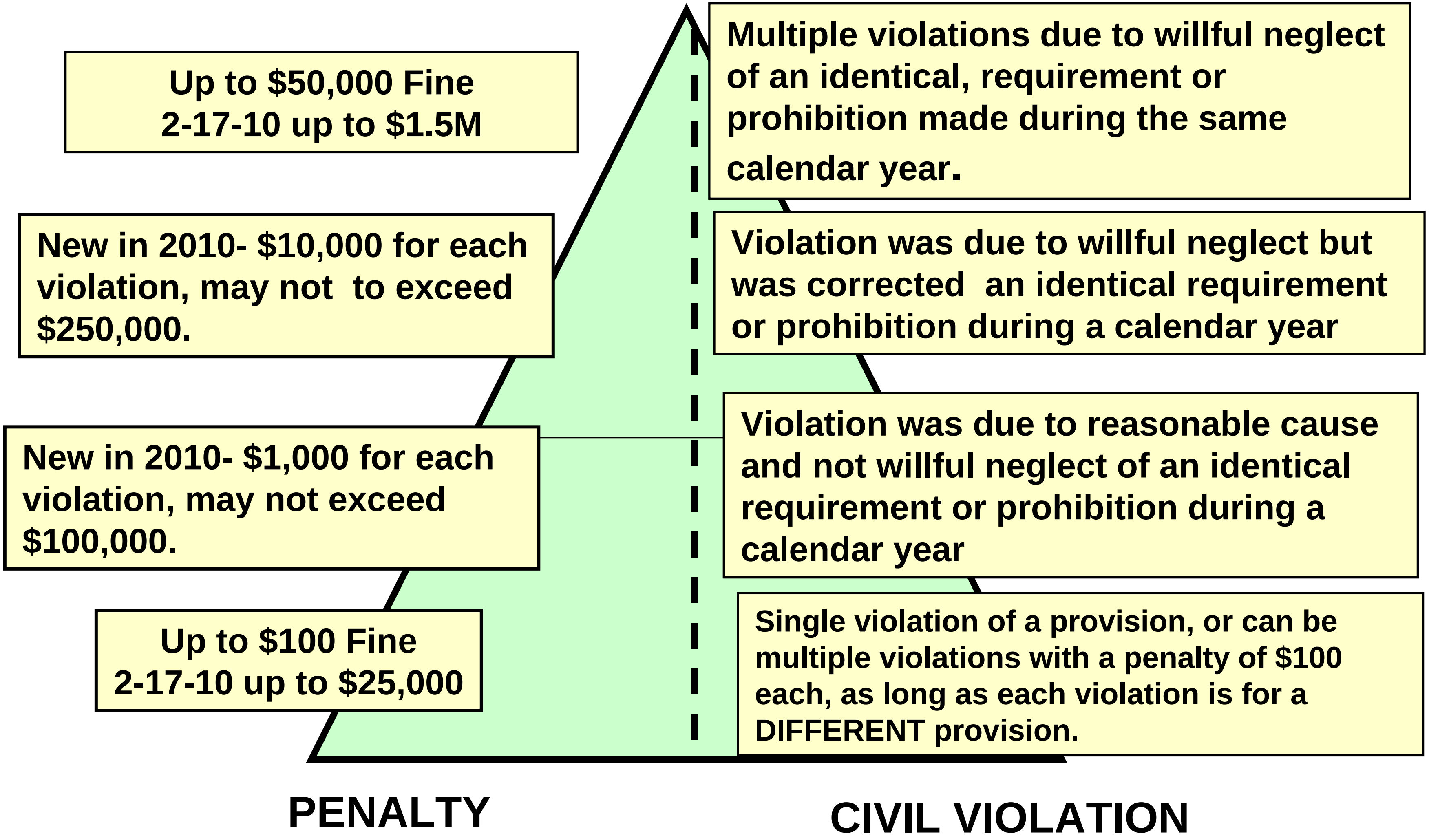
It will protect us in many ways:

- Save money
- Improve healthcare
- Save lives

Does the punishment fit the Crime?

Let's look at the Punishment for Covered Entities effective 2-22-10 it includes Business Associates.

Civil Penalties



Up to $50,000 Fine
2-17-10 up to $1.5M

Multiple violations due to willful neglect of an identical, requirement or prohibition made during the same calendar year.

New in 2010- $10,000 for each violation, may not to exceed $250,000.

Violation was due to willful neglect but was corrected an identical requirement or prohibition during a calendar year

New in 2010- $1,000 for each violation, may not exceed $100,000.

Violation was due to reasonable cause and not willful neglect of an identical requirement or prohibition during a calendar year

Up to $100 Fine
2-17-10 up to $25,000

Single violation of a provision, or can be multiple violations with a penalty of $100 each, as long as each violation is for a DIFFERENT provision.

PENALTY

CIVIL VIOLATION

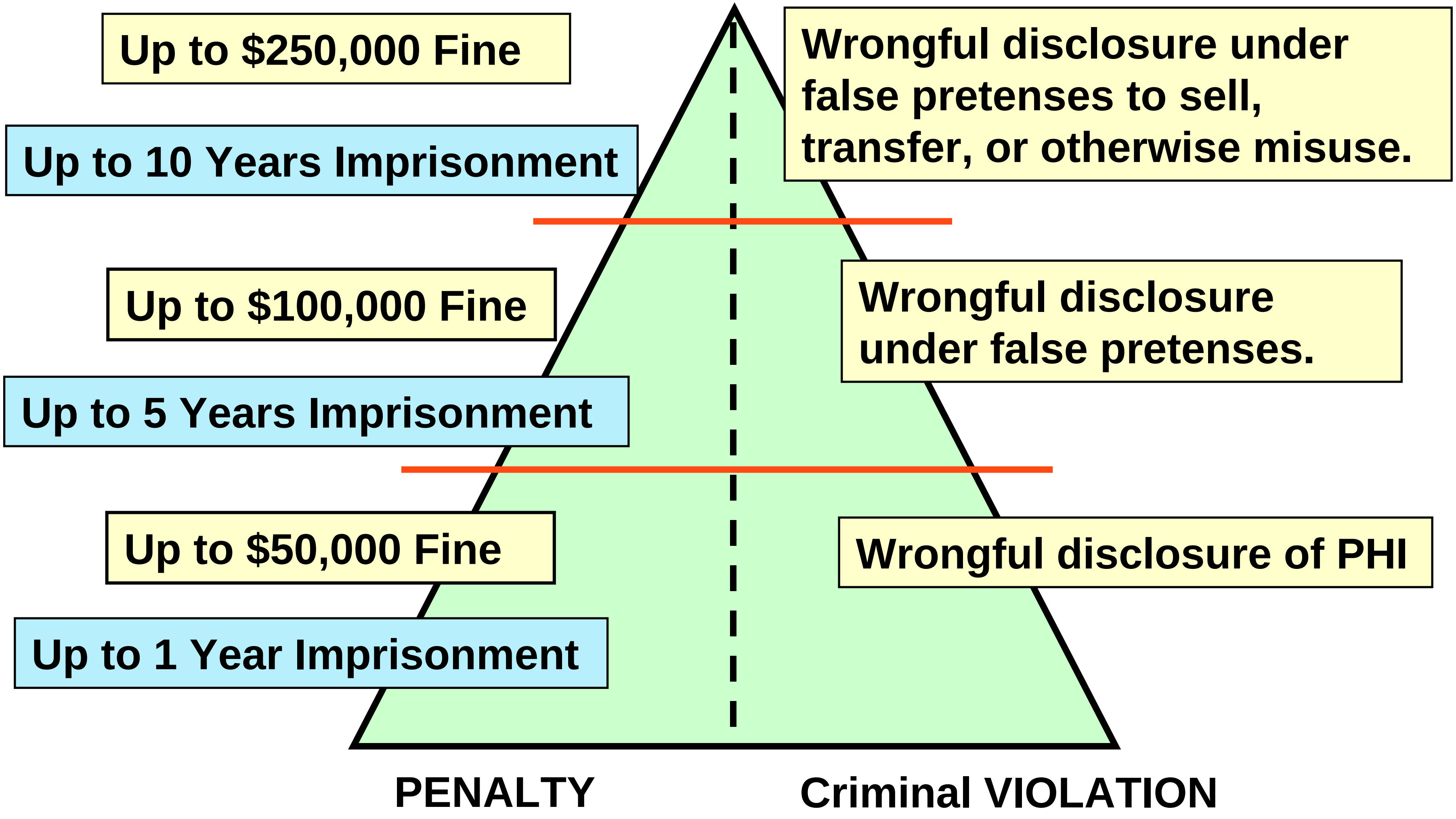
HITECH Act – big change!

Part of the $ collected on the fines go to the patients for damages.

Beginning in 2012

Talk about an incentive to file a complaint

Criminal Penalties



PENALTY	Criminal VIOLATION
Up to $250,000 Fine Up to 10 Years Imprisonment	Wrongful disclosure under false pretenses to sell, transfer, or otherwise misuse.
Up to $100,000 Fine Up to 5 Years Imprisonment	Wrongful disclosure under false pretenses.
Up to $50,000 Fine Up to 1 Year Imprisonment	Wrongful disclosure of PHI

Senior Executive Risk

- Senior Executives may be personally punished for non-conformance to HIPAA rules.
- If he or she is aware of a violation, delegating the responsibility to another person in not protection from personal penalty.
- Corporations are liable for violations of HIPAA by employees, other members of their workforce, Business Associates without contracts.

Anyone can file a complaint

Anyone who believes there has been a HIPAA violation can file a complaint with HHS up to 180 days after they first become aware of the perceived lack of compliance.

Business Associates

- Prior to HITECH BA’s required to abide by the rules of the BAA.
- If CE is aware of a breach – the contract should require them to report breaches to the CE.
- Then the CE needs to be assured the breach has been stopped and documented.
- If the BA Continues the breach the CE is required to stop doing business with them.
- If they cannot stop doing business with the BA they need to report them to HHS

Business Associates– HITECH Act

- Still required to sign a BA with CE after 2-23-10.
  - To let them know what they can do with your PHI – be specific.
- The biggest change:
  - BA is required to comply with HIPAA
  - If they find CE is not Complying the BA's are required to report to HHS.
- This is a big change too!

Small Health Plans

- Receipts of $5 million or less.
- Typically an individual or group health plan with fewer than 50 participants.
- Given an extra year to get their business practices into compliance with HIPAA.

What if State Laws Conflict?

HIPAA supersedes any contrary state law except in the following situations:

1. The Secretary of HHS determines that the state laws are necessary for the technical purposes outlines in the statute.
2. State laws that the Secretary determines address controlled substances.
3. State laws regarding the privacy of individually identifiable health information that are contrary to and more stringent than the federal requirements.

Stricter Standards

HIPAA is the floor….

Always follow the stricter standard.

State, Federal or even stricter standards your organization may have.

Privacy Rule vs. Security Rule

Privacy = Confidentiality of PHI in ALL formats: paper, oral, or electronic.

Security = PHI electronically captured, stored , used or transmitted.

It is a handshake not a handoff.

Why create the Privacy Rule?

“[The privacy rule] has been carefully crafted for this new era, to make medical records easier to see for those who should see them, and much harder to see for those who shouldn’t.”

- President William Clinton

Lesson 2 Objectives

- What is the HIPAA Security Rule?
- Defining Security
- CIA what's the scoop?
- Identify HIPAA Security Rule's design objectives
- Describe HIPAA Security Rule's core domain areas
  - Administrative Safeguards
  - Physical Safeguards
  - Technical Safeguards
- Additional Standards
- A non-technical explanation of technical issues.

The Security Rule

Security Standards for the Protection of Electronic Protected Health Information.

Compliance Date – April 20, 2006 (small health plans)

All Providers, Health Plans (even small ones), and Healthcare Clearinghouses who are covered entities must comply.

Purpose:

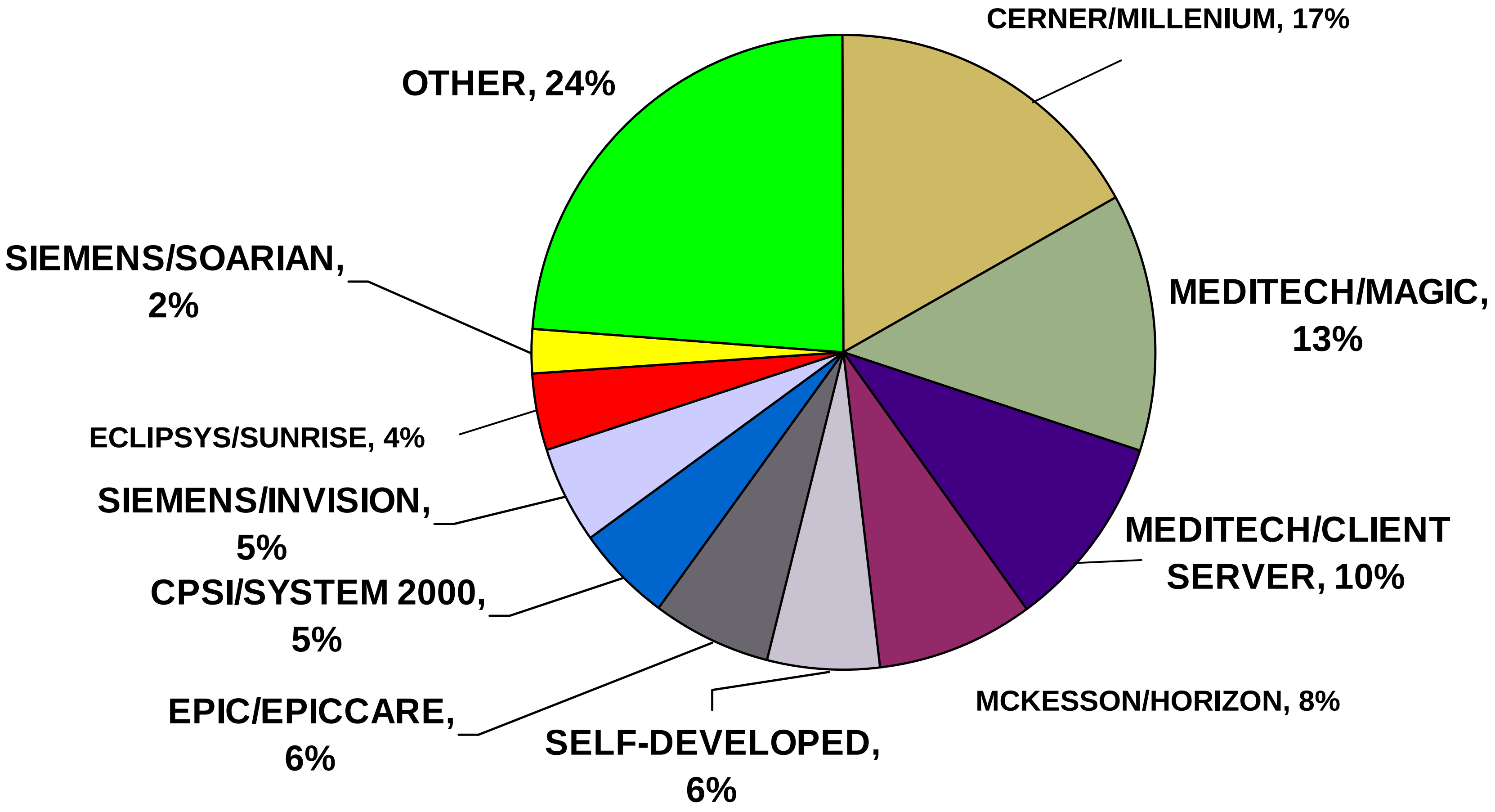
Make sure that important security safeguards are adopted to protect PHI which may be at risk.

Set up a methodology which permits appropriate access and use of PHI, encouraging electronic means of using and transmitting PHI.

Where are we today?

Data from HIMSS Analytics

EMR US Hospital Market Share (n=2723 installations)



ecfirst Home of the HIPAA Academy 2011

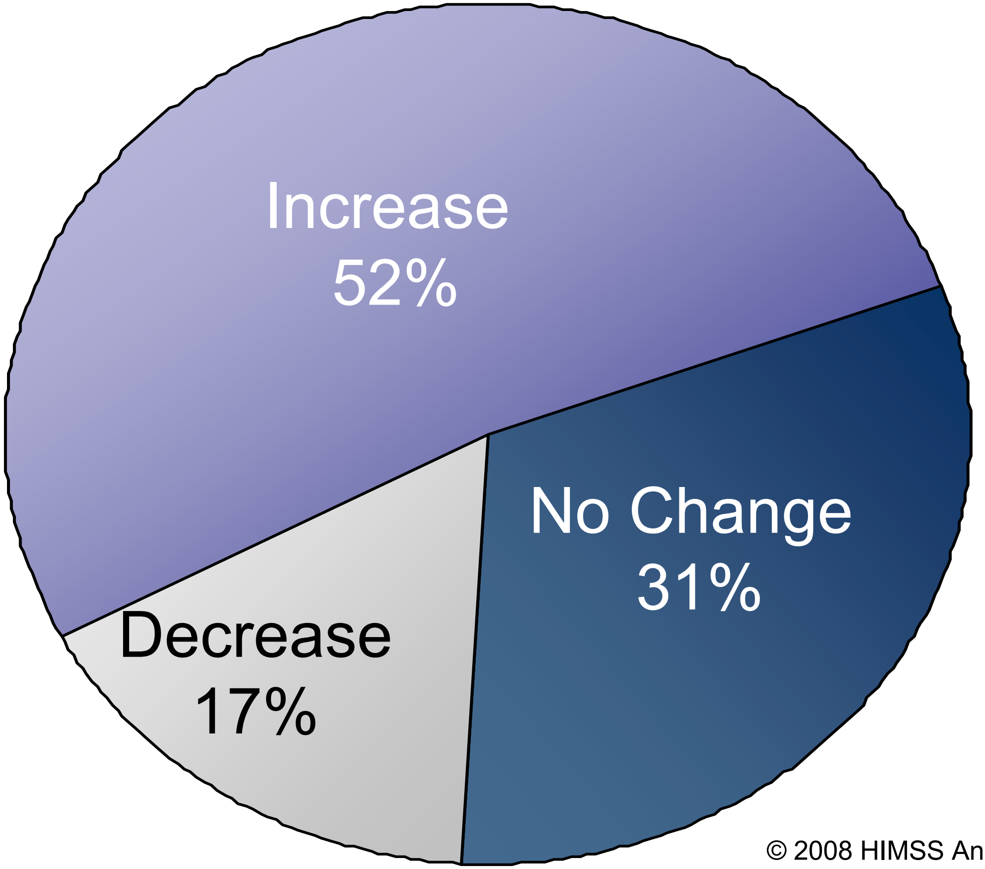
EMR Adoption Model Trends

Stage	Cumulative Capabilities	2010 Q3	2010 Final
Stage 7	Complete EMR; CCD transactions to share data; Data warehousing; Data continuity with ED, ambulatory, OP	1.0 %	1.0 %
Stage 6	Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS	2.8 %	3.2 %
Stage 5	Closed loop medication administration	3.7 %	4.5 %
Stage 4	CPOE, Clinical Decision Support (clinical protocols)	10.3 %	10.5 %
Stage 3	Nursing/clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology	49.7 %	49.0 %
Stage 2	CDR, Controlled Medical Vocabulary, CDS, may have Document Imaging; HIE capable	15.4 %	14.6 %
Stage 1	Ancillaries - Lab, Rad, Pharmacy - All Installed	6.7 %	7.1 %
Stage 0	All Three Ancillaries Not Installed	10.5 %	10.1 %

The 2011 numbers are in too

EMRAM Trended	2011 Q2	2011 Q3
Stage 7	1.1%	1.1%
Stage 6	4.0%	4.4%
Stage 5	6.1%	7.1%
Stage 4	12.3%	13.2%
Stage 3	46.3%	46.1%
Stage 2	13.7%	12.6%
Stage 1	6.6%	5.9%
Stage 0	10.0%	9.6%
Total Hospitals	n = 5310	n = 5299

IT Budgets are moving up



© 2008 HIMSS Analytics

Based on IT Budget as a Percent of Total Operating Expense for the 163 IDSs that provided data in both 2002 and 2008

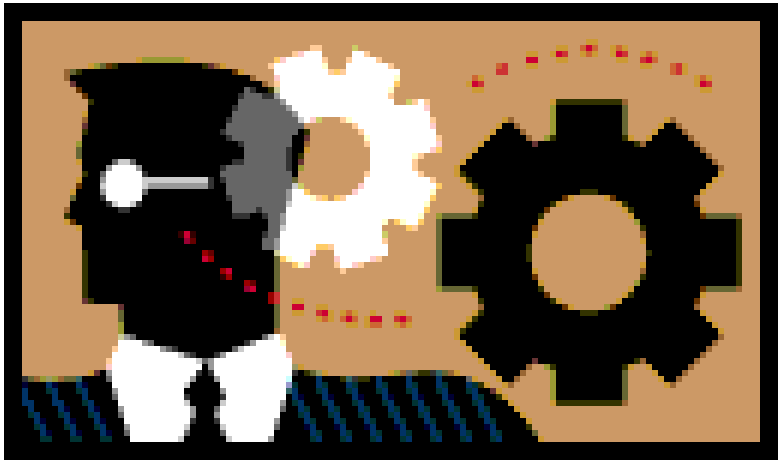
Source: HIMSS Analytics™ Database

Things are still looking UP!

- Many hospitals are making capital investments to position themselves to qualify for meaningful-use incentives.

- Hospitals' capital spending for IT application solutions in 2011
  - projected to constitute 46.5% to 48.3% of their total IT capital budgets;
  - up approximately 2% from 2009.

We are moving in the right direction



Is it secure?

www.privacyrights.org

Mar. 6, 2008	Cascade Healthcare Community (Prineville, OR)	(Prineville, OR)A computer virus may have exposed to outside eyes the names, credit card numbers, dates of birth and home addresses individuals who donated to Cascade Healthcare Community.	11,500
Mar. 10, 2008	Texas Department of Health and Human Services (Austin, TX)	Information, including Social Security numbers that could be used to steal Medicaid clients' identity may have been stored on two computers stolen during a burglary. Computers could have contained personal information only on e-mails. The e-mails, however, would normally contain only an individual's case number. It is unlikely those e-mails would have listed Social Security numbers.	Unknown
Mar. 10, 2008	Blue-Cross Blue-Shield of Western New York (Buffalo, NY	A laptop hard-drive containing vital information about members has gone missing. Blue-Cross Blue-Shield of Western New York says it is notifying its members about identity theft concerns after one of it's company laptops went missing.	40,000
Mar. 13, 2008	University Health Care (Utah) (SLC, UT)	Patient's information could have been compromised, when a laptop with names, Social Security numbers and personal health information was stolen from University Healthcare. The hospital says that someone broke into a locked office and took a lap top and a flash drive.	4,800
Mar. 26, 2008	Presbyterian Intercommunity Hospital (Whittier, CA)	About 5,000 past and current employees at Presbyterian Intercommunity Hospital had their private information stolen. The data included Social Security numbers, birth dates, full names and other records stored on a desktop computer that was stolen.	5,000
Mar. 29, 2008	Department of Human Resources (Atlanta, GA)	A thief has stolen computer records containing identifying information on current and former employees of the state Department of Human Resources, including names, Social Security numbers, birth dates and home contact information. An external hard drive that stored a database was removed by an unauthorized person.	Unknown

www.privacyrights.org

June 10, 2008	University of Utah Hospitals and Clinics (Salt Lake City,ut0	Billing records of 2.2 million patients at the University of Utah Hospitals and Clinics were stolen from a vehicle after a courier failed to immediately take them to a storage center. The records, described only as backup information tapes, contained Social Security numbers of 1.3 million people treated at the university over the last 16Y	2.2 million
July 9, 2008	Wichita Radiological Group (Wichita,	A former employee stole patient records before being fired from the Wichita Radiological Group. Tens of thousands of patient records were in the database could have been compromised.	Unknown
July 16, 2008	Greensboro Gynecology Associates (Greensboro, NC)	A backup tape of patient information was stolen from an employee who was taking the tape to an off-site storage facility for safekeeping. The stolen information included patients' names, addresses, Social Security numbers, employers, insurance companies, policy numbers and family members.	
July 23, 2008	San Francisco Human Services Department (San Francisco, CA)	Potentially thousands of files containing personal information was exposed after a San Francisco agency left confidential files in unsecured curbside garbage and recycling bins. In some cases entire case files were discarded. Blown up copies of social security cards, driver's licenses, passports, bank statements and other sensitive personal information were all left in these unlocked bins.	Unknown
July 29, 2008	Blue Cross and Blue Shield of Georgia (Atlanta, GA)	Benefit letters containing personal and health information were sent to the wrong addresses last week. The letters included the patient's name and ID number, the name of the medical provider delivering the service, and the amounts charged and owed. A small percentage of letters also contained the patient's Social Security numbers.	202,000
Feb. 3, 2009	Baystate Medical Center (Springfield , MA)	Several laptops were stolen from Baystate Medical Center's Pediatrics department. Some of those computers had patient information on them. All of the information is password protected and the computers had no financial or Social Security information on them.	Unknown

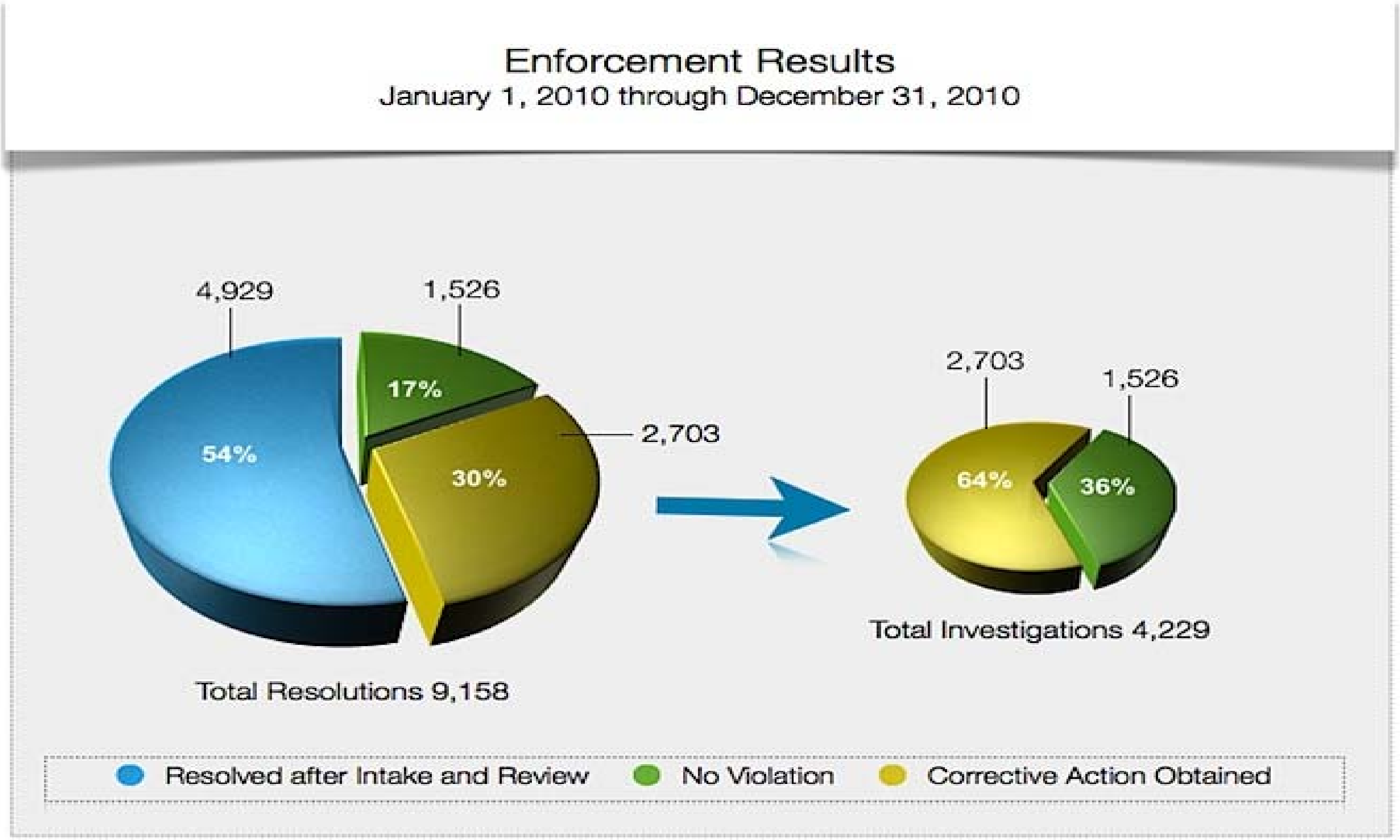
www.privacyrights.org

From January 2005 to June 24, 2009

262,576,861
total number of records containing sensitive
personal information
involved in security breaches in the U.S.

These are only the ones reported!

From the HHS website



More recently .....

Sutter Health Had Not Yet Encrypted the Device - November 16, 2011

Sutter Health, an integrated delivery system that was in the process of encrypting all its desktop computers, reports that a device that had not yet been **encrypted** was recently stolen, affecting more than 4.2 million patients.

A database holding information on about 3.3 million patients collected from 1995 through January 2011. Included are names, addresses, dates of birth, phone numbers, some e-mail addresses, medical record numbers and the name of patients' health insurance plans.

The device also contained a database with more extensive information on 943,000 Sutter Medical Foundation patients, dating from January 2005 to January 2011. This smaller database included the same demographic information as the larger database, plus dates of service and a description of diagnoses and/or procedures.

Sutter Health notes in a statement on its website that it will notify by mail the 943,000 patients who had more extensive information on the computer.

"The Sutter Health data security office has already encrypted portable laptops and BlackBerries systemwide and was in the process of encrypting desktop computers throughout the system when the theft took place," according to the statement. "Sutter Health has since accelerated its efforts to encrypt all computers and has implemented routine security software updates. ... Sutter Health also will be reinforcing security practices with staff system wide."

First HIPAA Enforcement Action Against a Business Associates

On Jan. 19, 2012, in the wake of the theft of an unencrypted laptop computer containing approximately 23,500 patients records, the Minnesota attorney general brought the first formal enforcement action against a business associate, Accretive Health, Inc., for an alleged violation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), using her authority under the Health Information Technology for Economic and Clinical Health ("HITECH") Act. Additionally, the attorney general appears deeply unsettled by the amount of information that Accretive Health collected about patients without the patients' knowledge, alleging that this lack of transparency represents deceptive and fraudulent practices under Minnesota law.

hhs.gov website today

Name of Covered Entity	State	Business Associate Involved	Individuals Affected	Date of Breach	Type of Breach	Location of Breached Information
Osceola Medical Center	WI	Hils Transcription	500	11/25/2010	Unauthorized Access/Disclosure/Hacking	Network Server
Blue Cross Blue Shield Michigan	MI	Agent Benefits Corporation	2979	11/17/2010	Unauthorized Access/Disclosure/Hacking	Network Server
Riverside Mercy Hospital and Ohio/Mercy Diagnostics	OH		1000	11/15/2010	Improper Disposal	Paper Records
California Therapy Solutions	CA		1226	11/15/2010	Theft	Portable Electronic Device, Other
Centra	VA		11982	11/12/2010	Theft	laptop
Hospital Auxilio Mutuo	PR		1000	11/9/2010	Theft, Unauthorized Access/Disclosure, Hacking/IT Incident	Laptop, Desktop Computer
Indiana Family and Social Services	IN	The Southwestern Indiana Regional Council on Aging	757	11/9/2010	Theft	Laptop
Dean Health Systems, Inc.; St. Mary's Hospital	WI		3288	11/8/2010	Theft	Laptop
Geisinger Wyoming Valley Medical Center	PA		2928	11/6/2010	Unauthorized Access/Disclosure	Email
OhioHealth Corporation dba Grant Medical Center	OH		501	11/5/2010	Theft	Laptop/Desktop computer

Defining Security

Having in place:

Controls

Countermeasures

Procedures

Common Criteria for Security

1990's

Seven countries worked together
France , Canada, Germany, The Netherlands, United Kingdom and United States

NIST standards and healthcare

- NIST has been collaborating with industry and others to improve the healthcare information infrastructure since the 1990s. NIST IT researchers have an internationally respected reputation for their knowledge, experience, and leadership. Since 2004, NIST has worked closely with the Department of Health and Human Services' Office of the National Coordinator for Health IT (HHS/ONC).

  The role of NIST is further articulated in the 2008-2012 Federal Health IT strategic plan and the Health Information Technology for Economic and Clinical Health (HITECH) Act to:

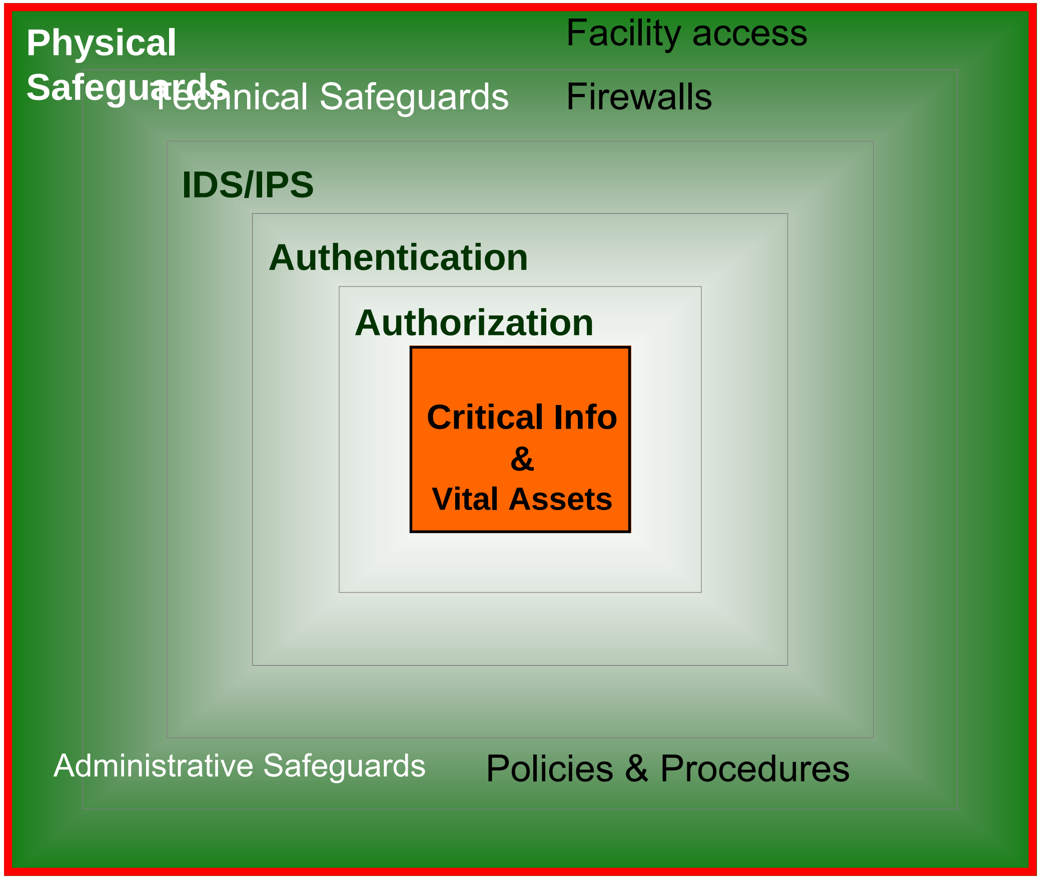
- Advance healthcare information enterprise integration through standards and testing.
- Consult on updating the Federal Health IT Strategic Plan.
- Consult on voluntary certification programs.
- Consult on health IT implementation.
- Provide pilot testing of standards and implementation specifications, as requested.

Security is minimizing the vulnerability of assets and resources

- Asset is anything of value – ePHI
- Vulnerability is any weakness that could be exploited
- Threat is a potential violation of security

Defense In-Depth

Nothing is 100% Secure



CIA

Confidentiality, Integrity and Availability are the core principles of security.

The wording of the Security Rule designates that a covered entity must protect the Confidentiality, Integrity, and Availability of electronic protected health information (EPHI).

Ensuring Confidentiality

Means by which records or systems are protected from unauthorized access.

- Implement by:
  - Limiting permissions to a "need to know" basis related to job function.
  - Allow disclosure privileges only to users who have training and authority to make decisions.
  - Install reliable authentication methods to identify system users and access control mechanisms to automatically control each employee's use of medical data.

Ensuring Integrity

- Data Integrity – Data has not been changed inappropriately, whether by accident or deliberate, malicious intent.
- Source integrity – Did the data come from the person or business you think it did, or did it come from an imposter?
- Data or information has not been altered or destroyed in an unauthorized act.
- Security backups allow reconstruction of data after a security threat or natural disaster.

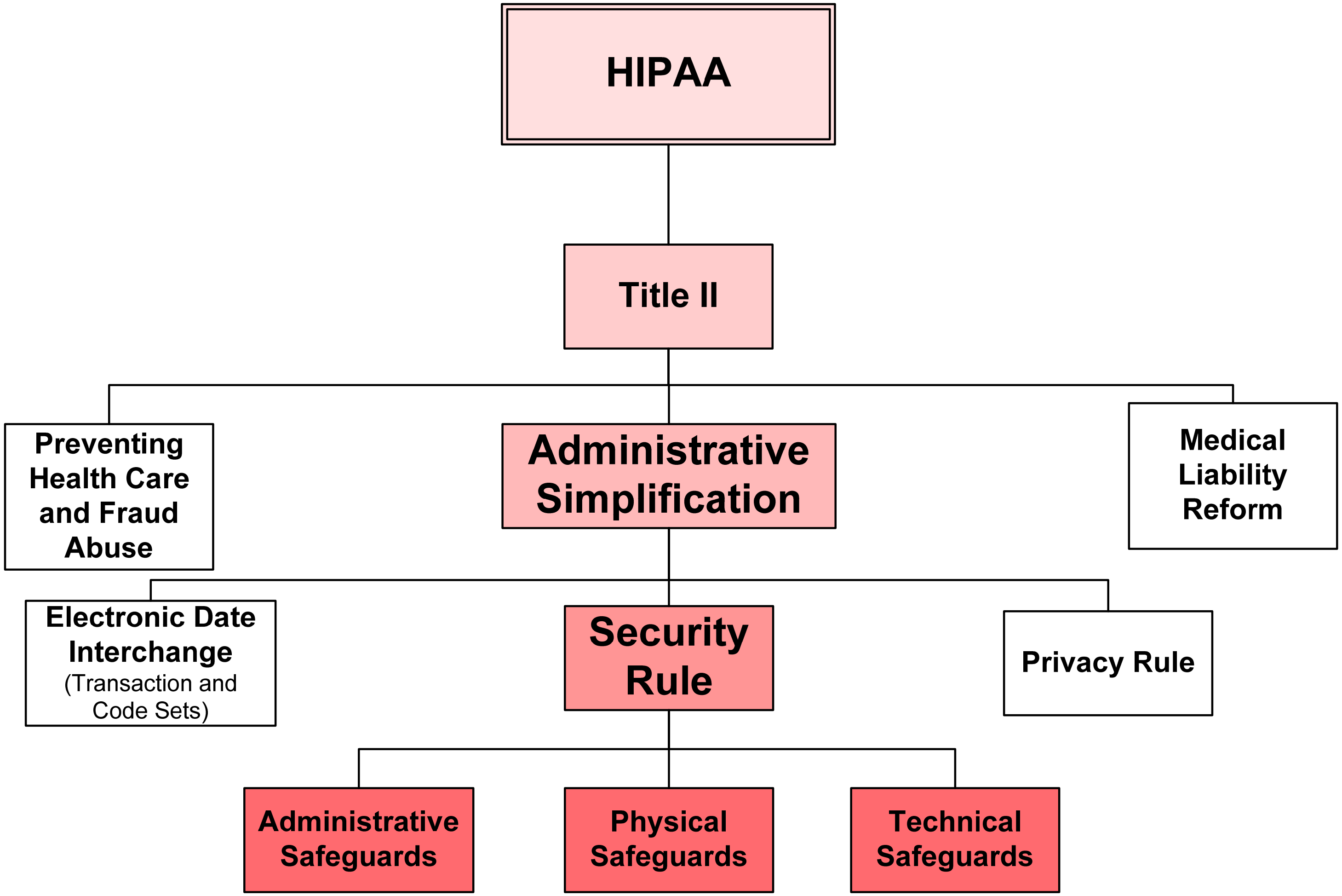
Ensuring Availability

Making PHI accessible to an authorized person when wanted and needed.

Implement by:

- Add policies and procedures that allow proper personnel to see and use PHI.
- Guard against threats to the systems, and processes resulting in erroneous denial or unavailable computer systems.
- Have appropriate backups and business continuity plans for operation in the event of an emergency.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)



HIPAA

Title II

Preventing Health Care and Fraud Abuse

Administrative Simplification

Medical Liability Reform

Electronic Date Interchange (Transaction and Code Sets)

Security Rule

Privacy Rule

Administrative Safeguards

Physical Safeguards

Technical Safeguards

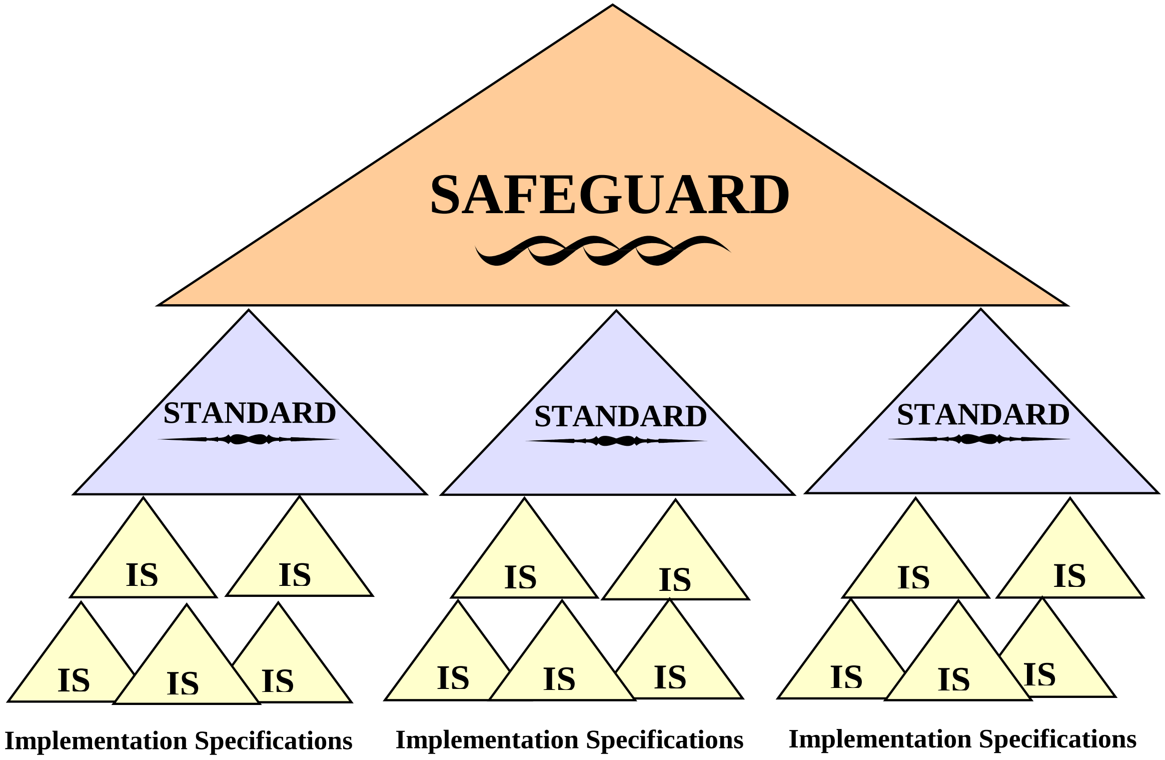
Approach and Philosophy

Comprehensive

Technology Neutral

Scalable

Safeguards, Standards, and Implementation Specifications


SAFEGUARD
STANDARD
STANDARD
STANDARD
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
IS
Implementation Specifications
Implementation Specifications
Implementation Specifications

“Required”

“Required” Implementation Specification are mandatory if your organization is a covered entity.

“Addressable” – Option One

Option One for Addressable Implementation Specifications

1. Assess whether it is a “reasonable and appropriate” safeguard in the unique environment in which you operate.
2. Is likely to contribute to protecting the PHI with which you work.

If you answer Yes to BOTH - Implement

“Addressable” – Option Two

Option Two for Addressable Specification:

If your answer would be “No”, it doesn’t make sense for us to do this because we are too small, the exposure risk is slight, or it would be overkill…..

Document why it is not “reasonable and appropriate” and do an equivalent method to insure protection of EPHI.

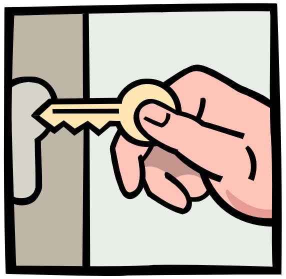
Addressable Example?

Automatic Logoff

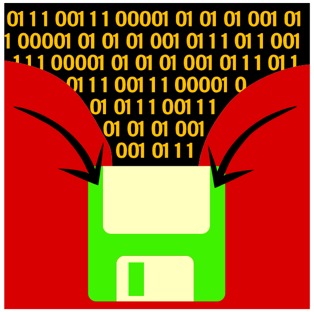
APT to Comply?

Administrative Safeguards

Physical Safeguards



Technical Safeguards



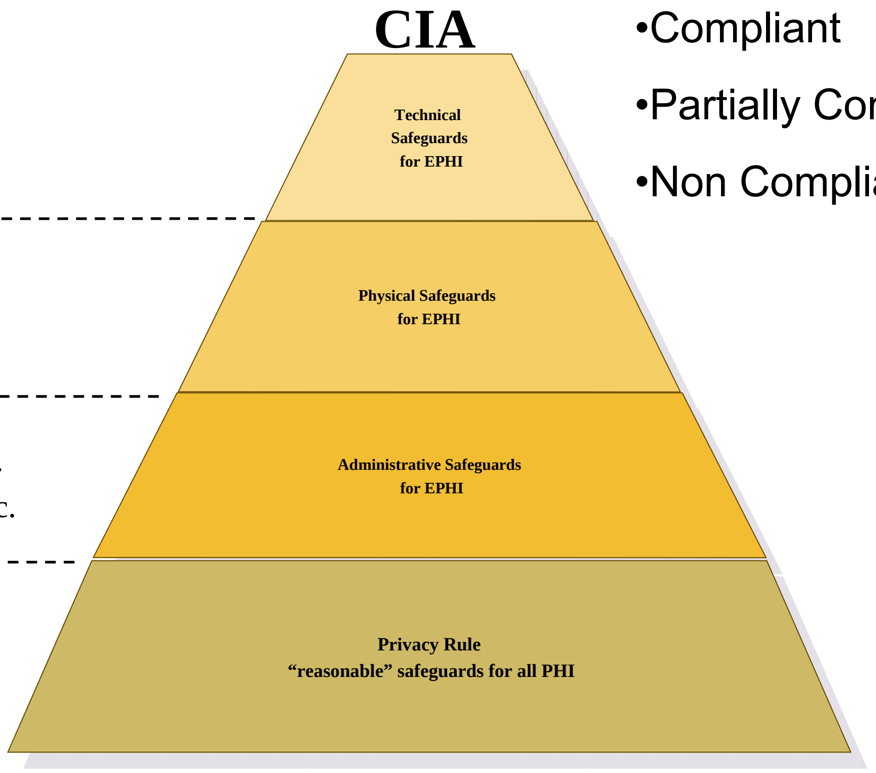
Three HIPAA Security Domains

Security Standards

- Access Control
- Audit Control
- Integrity
- Person or Entity Authentication
- Transmission Security

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device & Media Controls

- Security Mgmt. Process, Sec. Officer
- Workforce Security, Info. Access Mgmt.
- Security Training, Security Incident Proc.
- Contingency Plan, Evaluation, BACs


CIA
Technical Safeguards for EPHI
Physical Safeguards for EPHI
Administrative Safeguards for EPHI
Privacy Rule
"reasonable" safeguards for all PHI

3 options

- Compliant
- Partially Compliant
- Non Compliant

With in each **Security Standard** are Implementation Specifications

Administrative safeguards address security requirements

- Development and publication of policies
- Development of standards
- Determination of procedures and guidelines
- Personnel security requirements
- Security training

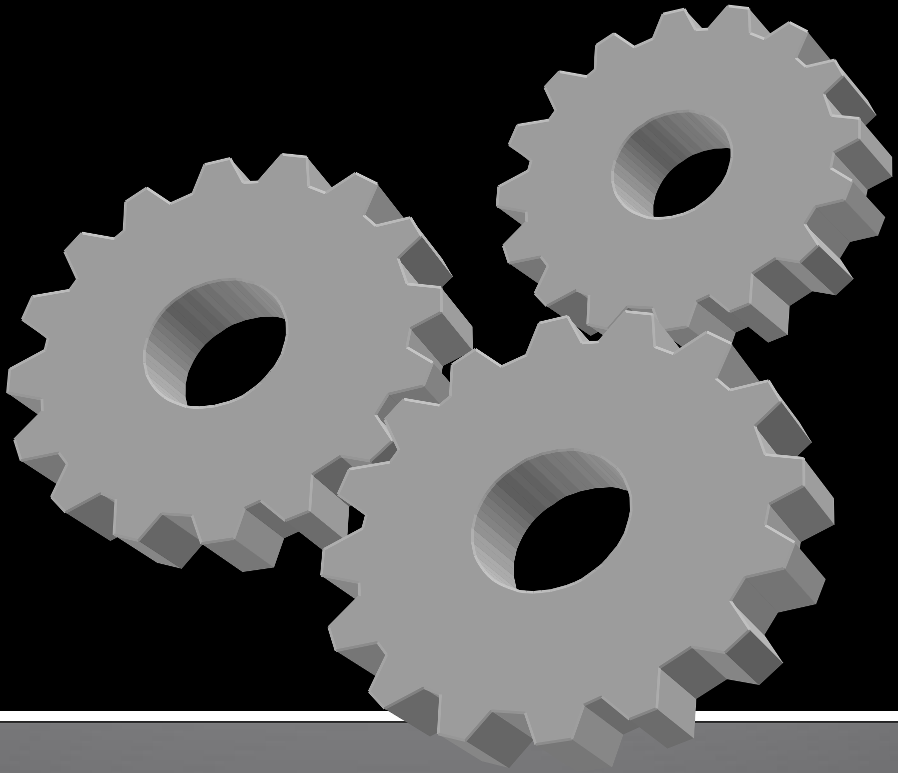
Physical safeguards address security requirements

- Facility access
- Locking systems
- Monitoring for intrusion
- Environmental controls

Technical safeguards address security requirements

- Logical access control mechanisms
- Password management
- Resource management
- Identification and authentication methods
- Security devices
- Configuration of the network

Let's get into the Details



ADMINISTRATIVE SAFEGUARDS

Standards	Implementation Specifications (R) = Required. (A) = Addressable	
Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R
Assigned Security Responsibility		R
Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A
Information Access Management	Isolating Health Care Clearinghouse Functions	R
	Access Authorization	A
	Access Establishment and Modification	A
Security Awareness and Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A
Security Incident Procedures	Response and Reporting	R
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedures	A
	Applications and Data Criticality Analysis	A
Evaluation		R
Business Associate Contracts and Other Arrangements	Written Contract or Other Arrangement	R

Security Management Process standard

Standard	Implementation specifications	R = Required
		A = Addressable

Security Management Process	Risk Analysis	R
	Risk Management	R
	Sanction Policy	R
	Information System Activity Review	R

Workforce Security

Standard	Implementation specifications	R = Required
		A = Addressable

Workforce Security	Authorization and/or Supervision	A
	Workforce Clearance Procedure	A
	Termination Procedures	A

Implement policies and procedures to ensure that all members of its workforce have appropriate access to e-PHI and to prevent those workforce members who do not have access from obtaining access to electronic protected health information

Information Access Management

Standard	Implementation specifications	R = Required
		A = Addressable

Information Access Management	Isolating Health Care Clearinghouse Function	R
	Access Authorization	A
	Access Establishment And Modification	A

Implement policies and procedures for authorizing access to e-PHI that are consistent with the applicable requirements of this standard

Security Awareness and Training

Standard	Implementation specifications	R = Required
		A = Addressable

Security Awareness and Training	Security Reminders	A
	Protection from Malicious Software	A
	Log-in Monitoring	A
	Password Management	A

Security Incident Procedures

Standard	Implementation specifications	R = Required
		A = Addressable

Security Incident Procedures	Response and Reporting	R

Implement policies and procedures to address security incidents

Documented instructions for reporting security incidents

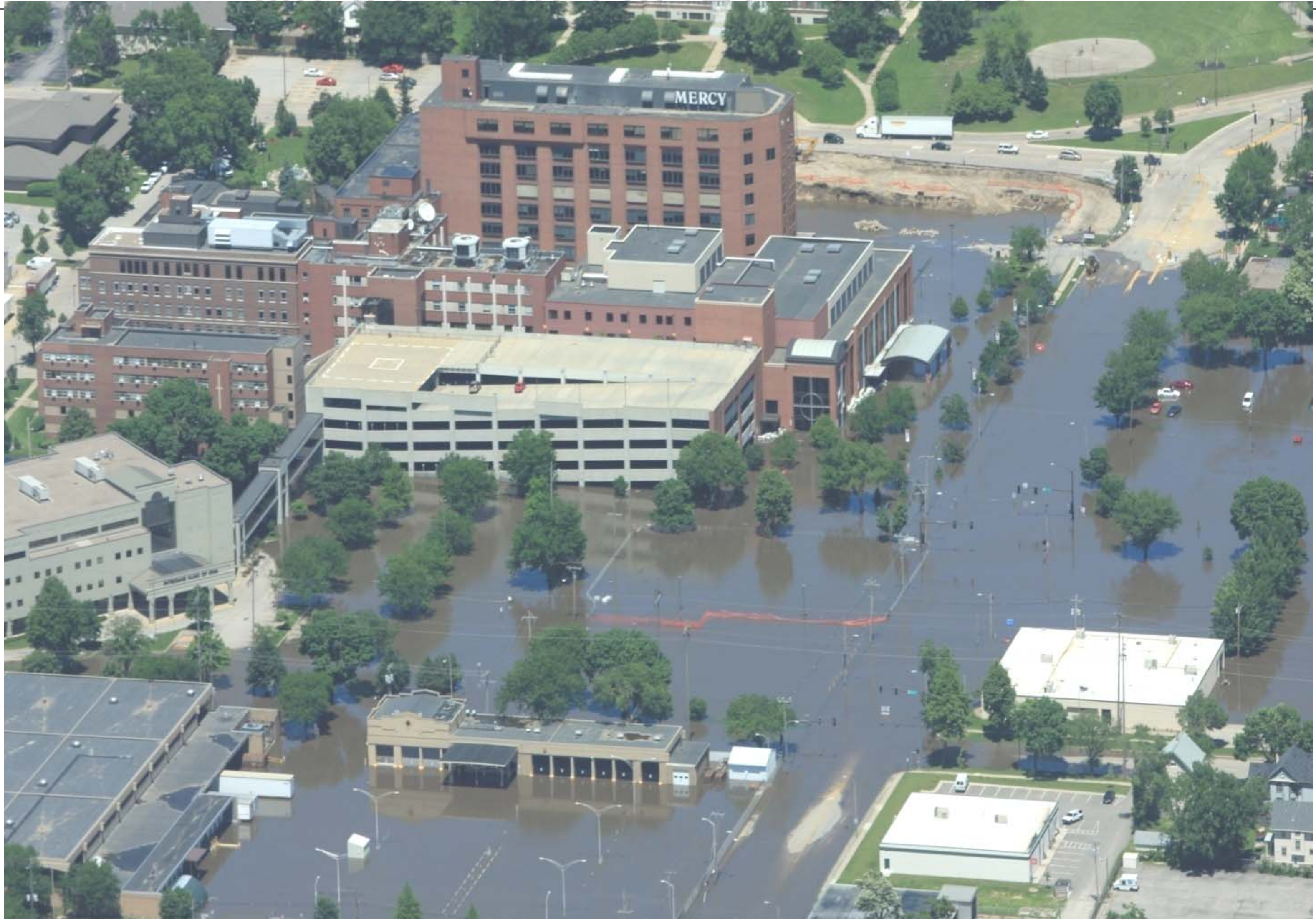
Contingency Plan

Standard	Implementation specifications	R = Required
		A = Addressable

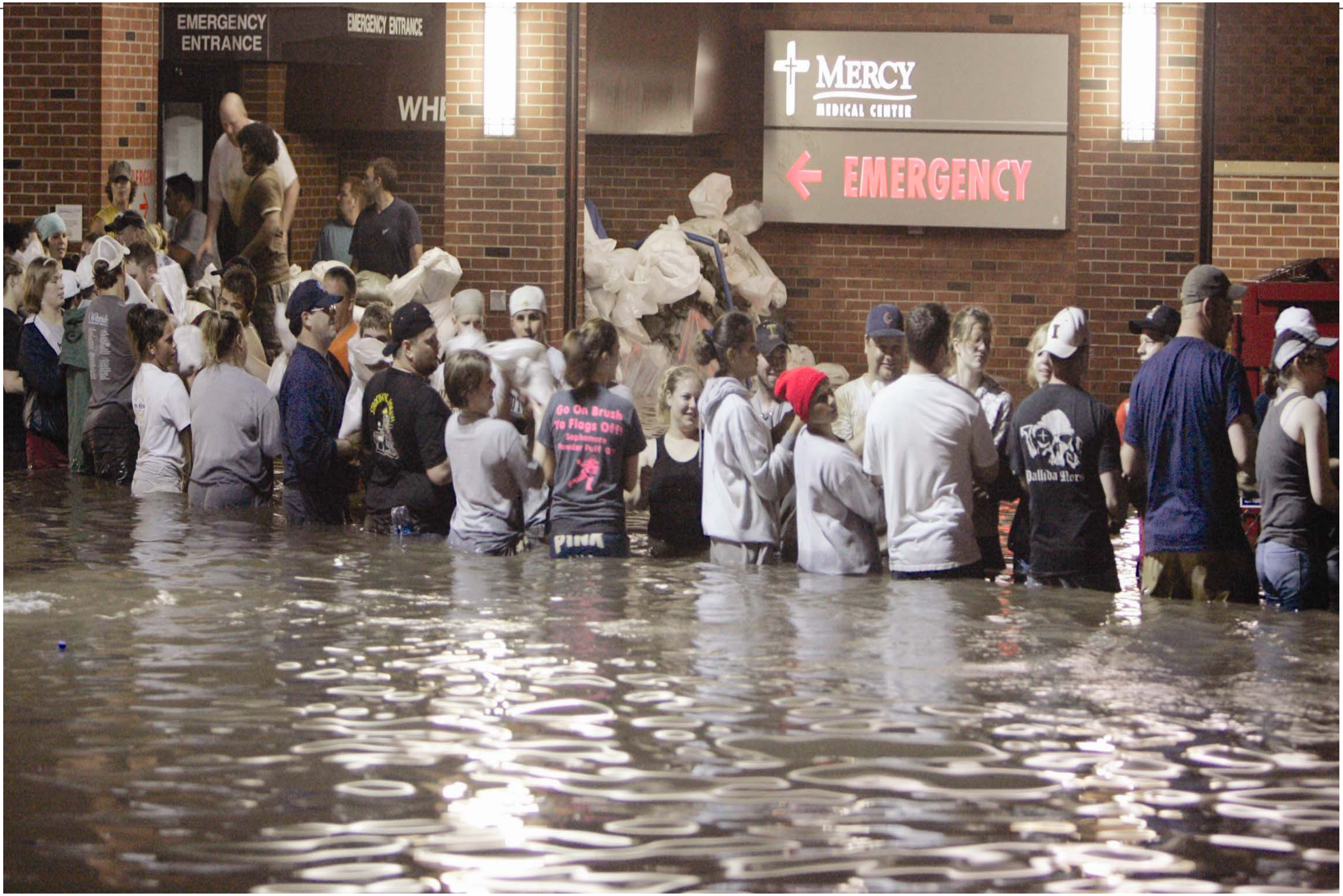
Contingency Plan	Data Backup Plan	R
	Disaster Recovery Plan	R
	Emergency Mode Operation Plan	R
	Testing and Revision Procedure	A
	Applications and Data Criticality Analysis	A

Establish (and implement as needed) policies and procedures for responding to emergencies and other occurrences that can damage systems containing e-PHI

THURSDAY, JUNE 12, 2008 – CEDAR RAPIDS IOWA, MERCY MEDICAL CENTER



How do you recover from this?



WHAT CHAPTER WAS THIS IN AT NURSING SCHOOL?

Emergency Mode Operation Plan

Required

Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of e-PHI while operating in emergency mode

Testing and Revision Procedures

Addressable

Implement procedures for periodic testing and revision of contingency plans

Applications and Data Criticality Analysis

Addressable

Assess the relative criticality of specific applications and data in support of other contingency plan components

Evaluation

Perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of e-PHI that establishes the extent to which an entity's security policies and procedures meet the requirements.

Business Associates

Are permitted to:

Create, Receive, Maintain or Transmit ePHI

If:

Assurances that BA is protecting ePHI as the CE would based on the BAA.

Business Associates are not…

Other Covered Entities

- Providers
- Insurance providers
- Medicare
- Medicaid

If a provider shares information with a BA it is a good idea to have periodic audits, effective 2-23-10 it will be a Best Practice.

Physical safeguards

In this section we examine all standards for Physical safeguards

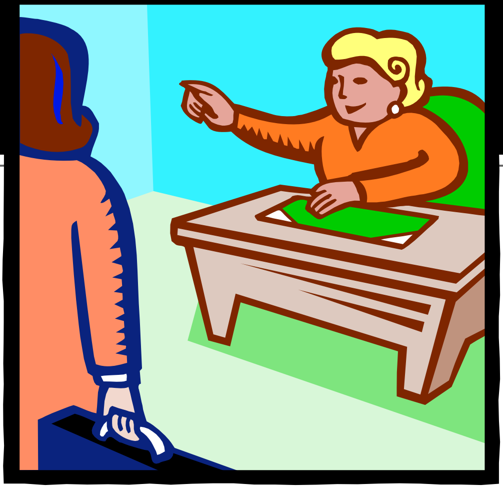
Physical safeguard requirements

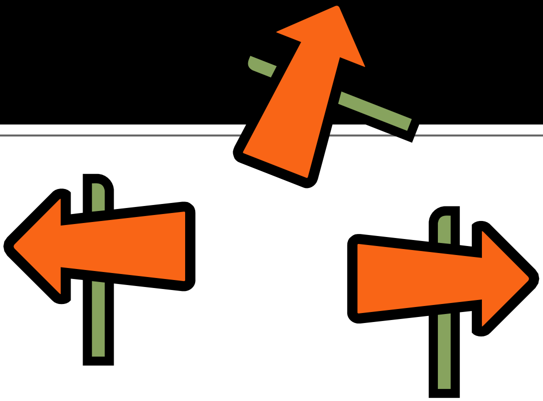
Physical measures, policies, and procedures to protect a covered entity’s electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion

Addressing security issues

- Is access to the building controlled?
- Is access to the computing facility controlled?
- Are there additional controls required for access after hours?
- Is there an audit log that records the individual, the location of access, and the time of access?
- Are systems adequately protected from theft?
- Are procedures in place to adequately dispose confidential information per HIPAA requirements?
- Are workstations secured after hours?
- Are the activities of the cleaning crew monitored?
- Has a plan been developed and tested for operating under an emergency?
- Are data backups sent to an off-site location for safe storage?
- Have procedures been developed for testing and revision of applications and systems?
- Are members of the workforce trained on key security issues?

Physical Safeguards are most aligned with the Privacy Rule





When possible, channel visitors, patients, Vendors, and non-involved employees away from areas housing electronic PHI.

PHYSICAL SAFEGUARDS

Standards	Implementation Specifications (R) = Required. (A) = Addressable	
Facility Access Controls	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A
Workstation Use		R
Workstation Security		R
Device and Media Controls	Disposal	R
	Media Re-use	R
	Accountability	A
	Data Backup and Storage	A

Facility Access Controls

Standard	Implementation specifications	R = Required
		A = Addressable

Facility Access Controls	Contingency Operations	A
	Facility Security Plan	A
	Access Control and Validation Procedures	A
	Maintenance Records	A

Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed

Important considerations:

- **Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after some type of a drill?**
- **Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?**

Workstation Use

Required

Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI

Workstation Security

Required

Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users

Device and Media Controls

Standard	Implementation specifications	R = Required
		A = Addressable

Device and Media Controls	Disposal	R
	Media Re-use	R
	Accountability	A
	Data Backup and Storage	A

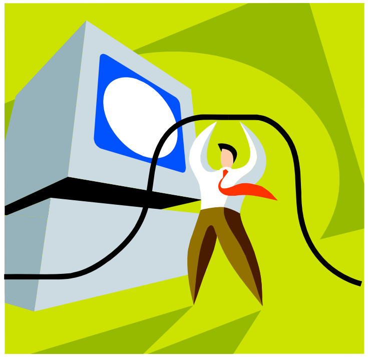
Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility

Important considerations:

Is media sanitized for reuse?

Technical safeguards

In this section we examine all standards for Technical safeguards



TECHNICAL SAFEGUARDS

Standards	Implementation Specifications (R) = Required. (A) = Addressable	
Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A
Audit Controls	(This means you must maintain a log and keep an audit trail of activity for each system.)	R
Integrity	Mechanism to Authenticate Electronic Protected Health Information (PHI)	A
Person or Entity Authentication	(This means you will control access to systems containing electronic PHI, and maintain a log and audit trail of activity for each system. All workstations should require a password for log-on and additional passwords to access key systems.)	R
Transmission Security	Integrity Controls	A
	Encryption	A

Access Control Standard

Standard	Implementation Specifications	R = Required
		A = Addressable

Access Control	Unique User Identification	R
	Emergency Access Procedure	R
	Automatic Logoff	A
	Encryption and Decryption	A

Implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights

Integrity

Addressable

Implement policies and procedures to protect EPHI from improper alteration or destruction

Important considerations:

Are data integrity and validation controls used to provide assurance that the information has not been altered and the systems functions as intended

Person or Entity Authentication standard

Required
Implement procedures to verify that a person or entity seeking access to EPHI is the one claimed

Important considerations:

Are users individually authenticated via passwords, tokens, or other means?

Mechanism to Authenticate

The objective is to implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Strong Authentication

Use two or more authentication factors
Closely tied in to non-repudiation
Authentication factors

- *Something you know (knowledge)*
- *Something you have (possession)*
- *Something you are (person)*

<u>Authentication solutions</u>

- *Tokens*
- *Smart cards*
- *Biometrics*

Technology: Authentication tokens

Dual-factor or two-factor authenticators
To use an authentication token, you need to have the token (something you have) and you need to know the PIN (something you know)

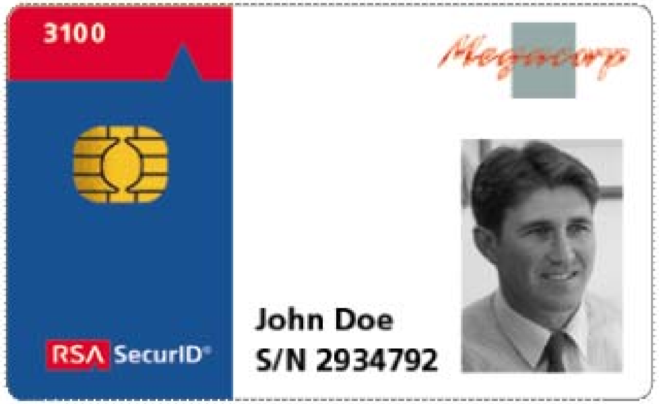
Key Fob

Card

Technology: Smart cards

A credit card-like device with both CPU and memory built-in

Used to store keys, certificates, credentials and other information



Technology: Biometrics

Verifies the identity of an individual based on measurable physiological and/or behavioral characteristics

Examples:

Fingerprints

Facial recognition

Retina scanning

Iris scanning

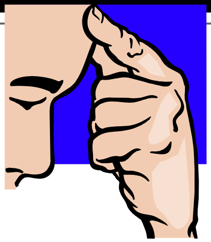
Hand geometry

Voice patterns

Bio Password

Strong Authentication

FidoD og6



Passwords = “What You Know”

Cards and Badges = What You Have”

Biometric Identification = “Who You Are”

Transmission Security standard

Standard	Implementation Specifications	R = Required
		A = Addressable

Transmission Security	Integrity Controls Encryption	A A

Implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network

Organizational Requirements

This includes the Standard, Business associate contracts or other arrangements. A covered entity is not in compliance with the standard if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate’s obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable.

Business Associate Contracts (BAC's)

If such steps were unsuccessful:

1. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity
2. Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it
3. Report to the covered entity any security incident of which it becomes aware
4. Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material

Business Associate Contracts

- Terminate the contract or arrangement, if feasible

  or

- If termination is not feasible, reported the problem to the Secretary (HHS).

Other Arrangements

When a covered entity and its business associate are both governmental entities, the covered entity is in compliance, if:

1. It enters into a memorandum of understanding (MOU) with the business associate
2. Other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate

Other Standards

Policies, Procedures and Documentation Requirements (164.316)

1. Policies and Procedures Standard
2. Documentation Standard

Policies and Procedures

- A covered entity must implement “reasonable and appropriate” policies and procedures to comply with the standards and implementation specifications.
- This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements.
- A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented.

Documentation

- A covered entity must maintain the policies and procedures implemented to comply in written (which may be electronic) form.
- If an action, activity or assessment is required to be documented
- The covered entity must maintain a written (which may be electronic) record of the action, activity, or assessment

Time Limit

- 6 years
- Remember Privacy Rule?

Availability

Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.

Updates

Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

In Summary

The core objective of HIPAA/HITECH is to protect individuals from the unapproved and unwarranted release of information related to their personal health and to increase the quality of healthcare.