

The Fourth HIPAA Summit West

Healthcare Privacy and Security After HITECH and Health Reform

A Hybrid Conference and Internet Event

Introduction of Certifications

Lorna L. Waggoner - Certified HIPAA Professional

Certified HIPAA Administrator (CHA)

Certified HIPAA Professional (CHP)

Certified HIPAA Security Specialist (CHSS)





On-line learning packages

- ⑩ Allow you to work at your own pace
- ⑩ Study from anywhere you have internet access (work, home, library)
- ⑩ Gives you facts in laymen's terms
- ⑩ Offers Questions at the end of each section so you can check your learning
- ⑩ Allows you to go back and re-examine the rules when you have specific examples to follow-up on.



Certification Exam

- ⑩ Nothing under HIPAA requires you or your organization to be Certified
- ⑩ You are required to have the knowledge and follow the guidelines
- ⑩ Certification – validates your learning
- ⑩ Certification is a credential
- ⑩ Hands on experience is equally or more important



Certified HIPAA Administrator (CHA)

In depth look at the HIPAA Privacy Rule

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





Certified HIPAA Professional (CHP)

- ⑩ CHA is the first section of CHP (Privacy)
- ⑩ Electronic Transactions
- ⑩ Code Sets
- ⑩ Identifiers
- ⑩ Introduction to the Security Rule
 - ☞ Safeguards
 - ☞ Standards





Certified HIPAA Security Specialist (CHSS)

- ⑩ Introduction to the Security Rule
 - ☞ Safeguards
 - ☞ Standards
- ⑩ More in depth by detailing the Implementation Specifications
- ⑩ Discussion of Specific Technologies
- ⑩ CISSP's (other Security Credentialed)
 - ☞ Receive CHSS Certification-upon completion of CHP Certification
 - ☞ Without completing the course or taking the exam



Today's curriculum

CHA - 8:15 a.m. to 10:30 a.m.

☞ **Introduction to HIPAA - Maps to course 101**

☞ **Privacy Rule - Maps to course 102**

10:15 a.m. **Break**

10:30 a.m. to 11:30 a.m.

☞ **Introduction to HIPAA Privacy continued - Maps to course 102**

- ☞ Upon completion you will still need to take module 103 to have enough knowledge to test for CHA exam.

11:30 a.m. to 12:30 p.m.

☞ **Overview of HIPAA Security - Maps to course 105**

☞ **Not enough to take CHP or CHSS with out more information**

- ☞ To be prepared for CHP there are modules on Transactions, Code Sets and Identifiers you will need to study.
- ☞ After CHP to be prepared for CHSS there are additional modules regarding Implementation Specifications you will need to study.
- ☞ After CHP - If you are CISSP or other security credentialed individual – with CISSP number we will send you CHSS Certificate with no further requirements.



Questions



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

www.ecfirst.com

www.hipaaacademy.net

Certified HIPAA PROFESSIONAL (CHP)

Lorna Waggoner
Director of Business Development





Class Objectives

- Understand what you must do to be HIPAA compliant
- Learn specifics necessary for your organization's size
- Debunk myths and folklore
- Look ahead to pertinent pending legislation
- Prepare for the CHA exam



HIPAA Legislation

WIIFM (What's In It For Me?)

- **Will it be worth my time?**
 - **Absolutely!**
 - To protect you and your organization
 - From discrimination – as a patient
 - From Civil and Criminal Penalties
 - It is the right thing to do



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.



What will I do with this knowledge?

- You may be the HIPAA Privacy or Security Officer for your organization;
- You may be a person who handles sensitive Protected Health Information, (PHI);
- You may need to train and/or advise others in your organization;
- You may need to educate upper management about their responsibilities under this law;
- You may be a business partner and be under legal obligation to protect the confidential information transmitted to and from your customers;
- Or a list of many other things



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



After the class you should have:

1. Validation for correct practices you have already implemented;
2. A list of areas where you now know that changes are quickly needed to fill gaps;
3. A feeling of relief that some of the misinformation you had believed, and dreaded implementing, has been exposed as untrue;
4. An idea of what additional requirements are coming in the near future;
5. A clear understanding of how you can follow a suggested action plan to begin to bring your organization into compliance; and
6. A list of topics to study when preparing for the certification test.



Let's Get Started





Learning Objectives

- What is HIPAA?
- What does HIPAA do?
- Do the rules apply to me?
- If so, 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 -Kassebaum 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?

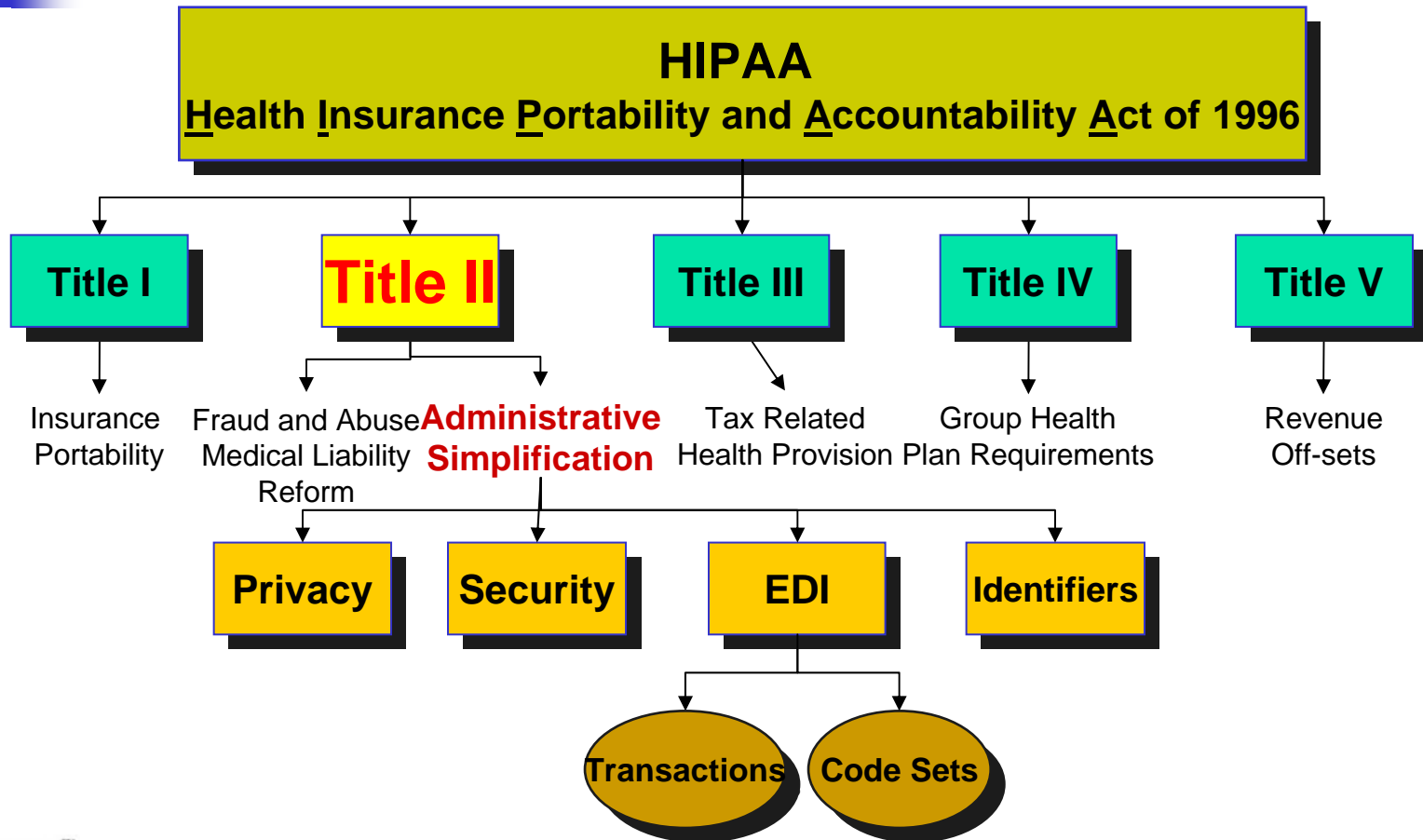
Today we see the simplicity.

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?





T.I.P.S about HIPAA Administrative Simplification Title II

Its all about.....

- Transactions and Code Sets
- Identifiers
- Privacy
- Security

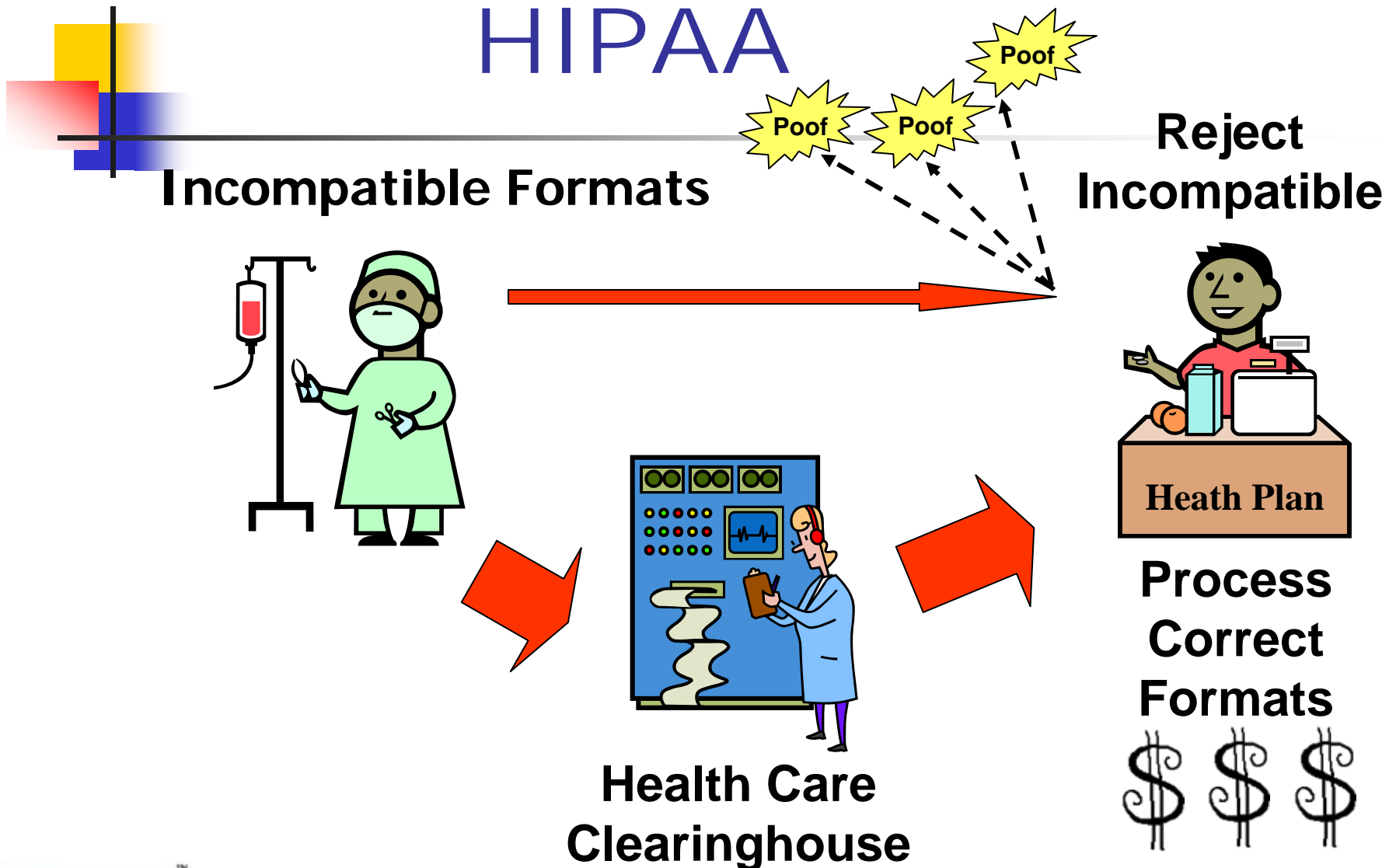


Prior to HIPAA

There were no standards:

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

Transaction Flow Prior to HIPAA





Before HIPAA – Cost estimates

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



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.



Savings can be seen in many areas

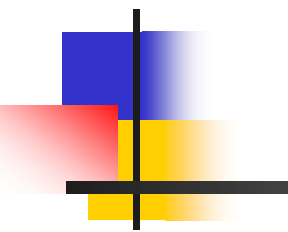
- Standardization and consistency of medical forms
- Eliminating paper documents
- Automating processes
- Reducing postal costs
- Reducing labor costs



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

ecfirst – Home of The HIPAA Academy



We will all be speaking
the same language

HIPAAALISH!



ARRA and HITECH Act

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



Who's Who and Estimated Implementation Costs

- Department of Health and Human Services (HHS)
- enforces HIPAA
- Contracted with Gartner Group
- AHA helped to pay for research



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 delegates over 20 Billion dollars for technology in 2009

Possible Implementation Costs



- Training on Claims Standards
- Programming
- Telecommunication and Server Expansion
- Software Upgrades
- Health Care Clearinghouse Fees
- Training on New Programming Languages
- Changing to Electronic Medical Records (EMR)



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

| | 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 |

Michigan Health Management Information System (MHMIS) Cost Analysis



These new laws protect millions

- Continuation of coverage
- Pre existing medical conditions
- Controlling Fraud and Abuse
- Administrative Simplification



Healthcare Industry

Largest industry in the USA

- Almost 18% of the U.S. gross domestic product
- Growing faster than the economy
- The only industry to grow in 2008-2009

Significant challenges

- Medical errors – 8th leading cause of death (HBR May 2006) 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
- 46 million uninsured in the U.S.

Deaths per 1,000 live births

Rank Country Value / - deaths per 1,000 live births **

| | | | | | |
|-----|--------------------------------------|------------|-----|---------------------------------------|------------|
| 1. | <u>Singapore</u> | 2.30deaths | 2. | <u>Sweden</u> | 2.76deaths |
| 3. | <u>Japan</u> | 2.80deaths | 4. | <u>Hong Kong</u> | 2.94deaths |
| 5 | <u>Iceland</u> | 3.27deaths | 6. | <u>France</u> | 3.41deaths |
| 7. | <u>Finland</u> | 3.52deaths | 8. | <u>Norway</u> | 3.64deaths |
| 9. | <u>Malta</u> | 3.82deaths | 10. | <u>Czech Republic</u> | 3.86deaths |
| 11. | <u>Andorra</u> | 4.03deaths | 12. | <u>Germany</u> | 4.08deaths |
| 13. | <u>Switzerland</u> | 4.28deaths | 14. | <u>Spain</u> | 4.31deaths |
| 15. | <u>Macau</u> | 4.33deaths | 16. | <u>Slovenia</u> | 4.35deaths |
| 17. | <u>Denmark</u> | 4.45deaths | 18. | <u>Austria</u> | 4.54deaths |
| 19. | <u>Belgium</u> | 4.56deaths | 20. | <u>Australia</u> | 4.57deaths |
| 21. | <u>Liechtenstein</u> | .58deaths | 22. | <u>Canada</u> | 4.63deaths |
| 23. | <u>Luxembourg</u> | 4.68deaths | 24. | <u>Netherlands</u> | 4.88deaths |
| 25. | <u>Portugal</u> | 4.92deaths | 26. | <u>United Kingdom</u> | 5.01deaths |
| 27. | <u>Ireland</u> | 5.22deaths | 28. | <u>Monaco</u> | 5.27deaths |
| 29. | <u>Greece</u> | 5.34deaths | 30. | <u>San Marino</u> | 5.53deaths |
| 31. | <u>Taiwan</u> | 5.54deaths | 32. | <u>New Zealand</u> | 5.67deaths |
| 33. | <u>Isle of Man</u> | 5.72deaths | 34. | <u>Italy</u> | 5.72deaths |
| 35. | <u>Cuba</u> | 6.04deaths | 36. | <u>Korea, South</u> | 6.05deaths |

37. [United States](#)

6.37deaths

ecfirst – Home of The HIPAA Academy ** Source = Geography IQ



Setting A National Goal Then

...ask not what your country can do for you, ask what you can do for your country

John F. Kennedy – Inaugural Speech, Jan. 20, 1961

...I believe that this nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth

John F. Kennedy – speech to Congress, May 25, 1961

... becomes the first man to walk on the Moon

American Neil Armstrong - July 20, 1969



Setting a National Goal Now

... achieve an electronic Health Record for all residents of the United States by the year 2014

President George W. Bush – Inaugural Speech January, 2004

Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires EHR by 2014.

The technology is there ...we were on the moon in 8 years!



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 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
 - Measurable and Manageable

That is not necessarily easier!

Who might be a Business Associate?

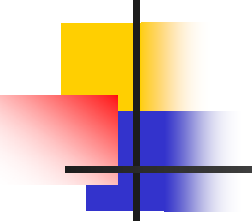
- ***Attorney***
- ***Accountant***
- ***Consultants***
- ***Cleaning Service***
- ***Data Aggregation***
- ***Vendors***





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 2/17/2010
- 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 of discovery.



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.
- 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 are required to notify HHS immediately
- HHS will post the information on their website.
- 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 # | |



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:

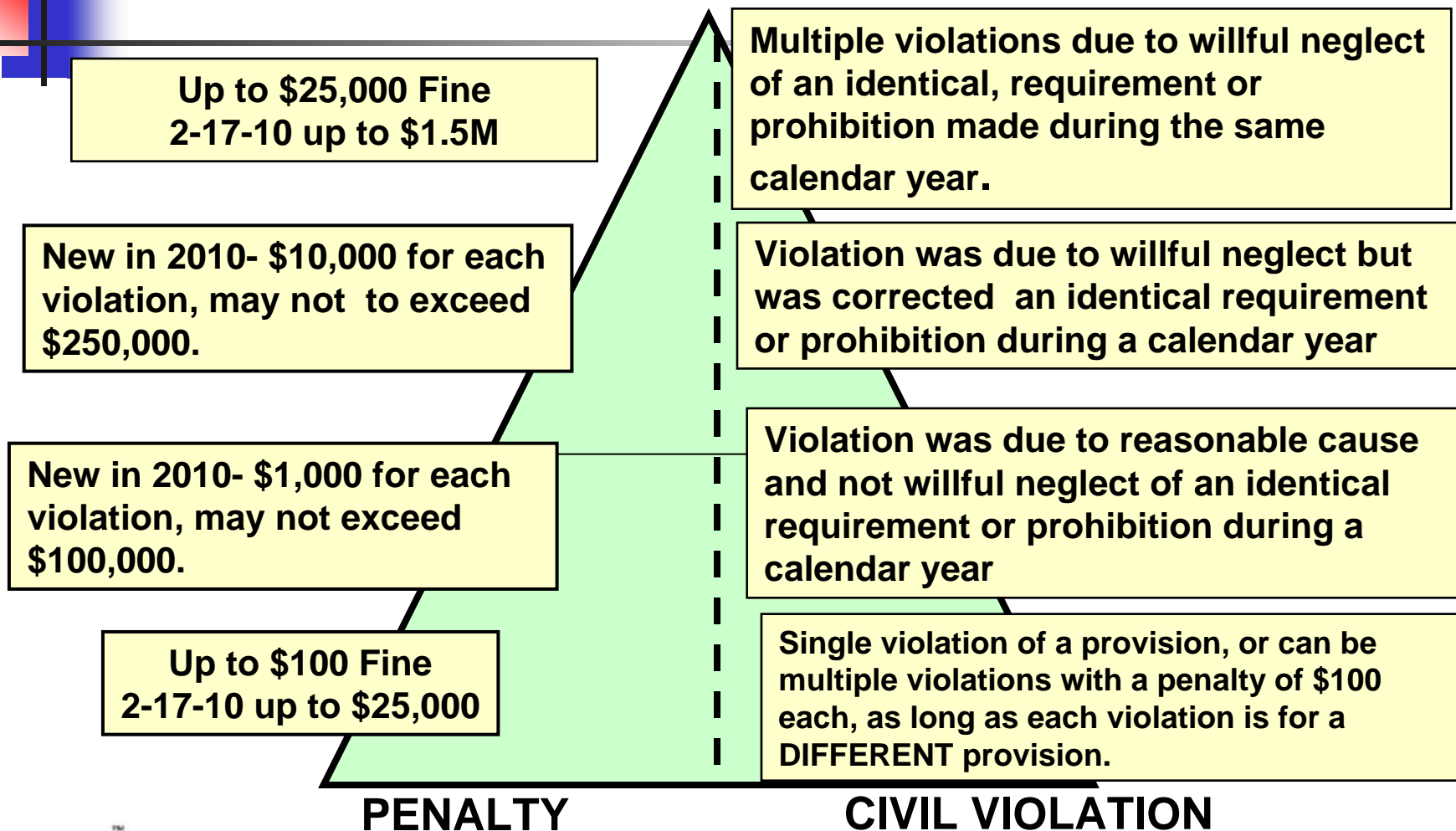
- Save money
- Improve healthcare
- Save lives

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

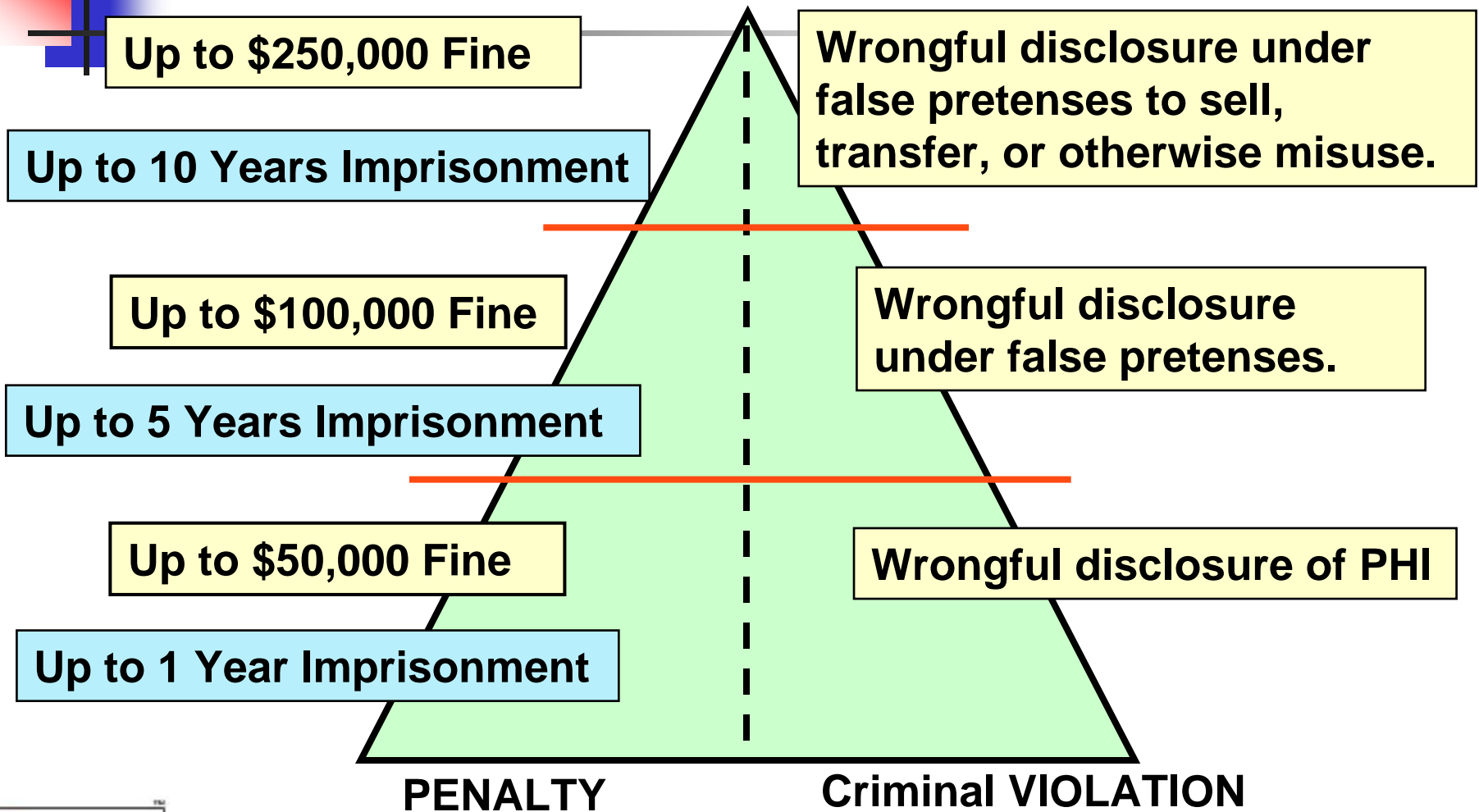




HITECH Act – big change!

- ✓ 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





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.



Business Associates

- 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 2-22-10.
 - 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!

ecfirst – Home of The HIPAA Academy



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 outlined 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

Implementation Deadlines

| Rule Title | Date Law Passed | Compliance Date | Comments |
|--|-------------------------|------------------------|---|
| HIPAA | August 21, 1996 | | |
| Transaction and Code Set | October 16, 2000 | October 16, 2002 | Covered Entities |
| Transaction and Code Set | October 16, 2000 | October 16, 2003 | Small Health Plans |
| Privacy Rule | April 14, 2001 | April 14, 2003 | Covered Entities |
| Revised Privacy Rule | Revised August 14, 2002 | April 14, 2003 | Covered Entities |
| Privacy Rule | | April 14, 2004 | Small Health Plans |
| Compliance Business Contracts in Place | | April 14, 2004 | Covered Entities AND Small Health Plans |
| Security Act | February 20, 2003 | April 21, 2005 | Covered Entities |
| | | April 21, 2006 | Small Health Plans |
| HITECH Act | February 17, 2009 | February 22, 2010 | Specified areas |

What is the Privacy Rule?

- In the beginning
- Science has created new ways.....
- State laws provided inconsistent protection...
- It started with the HHS adopting national standards for transactions

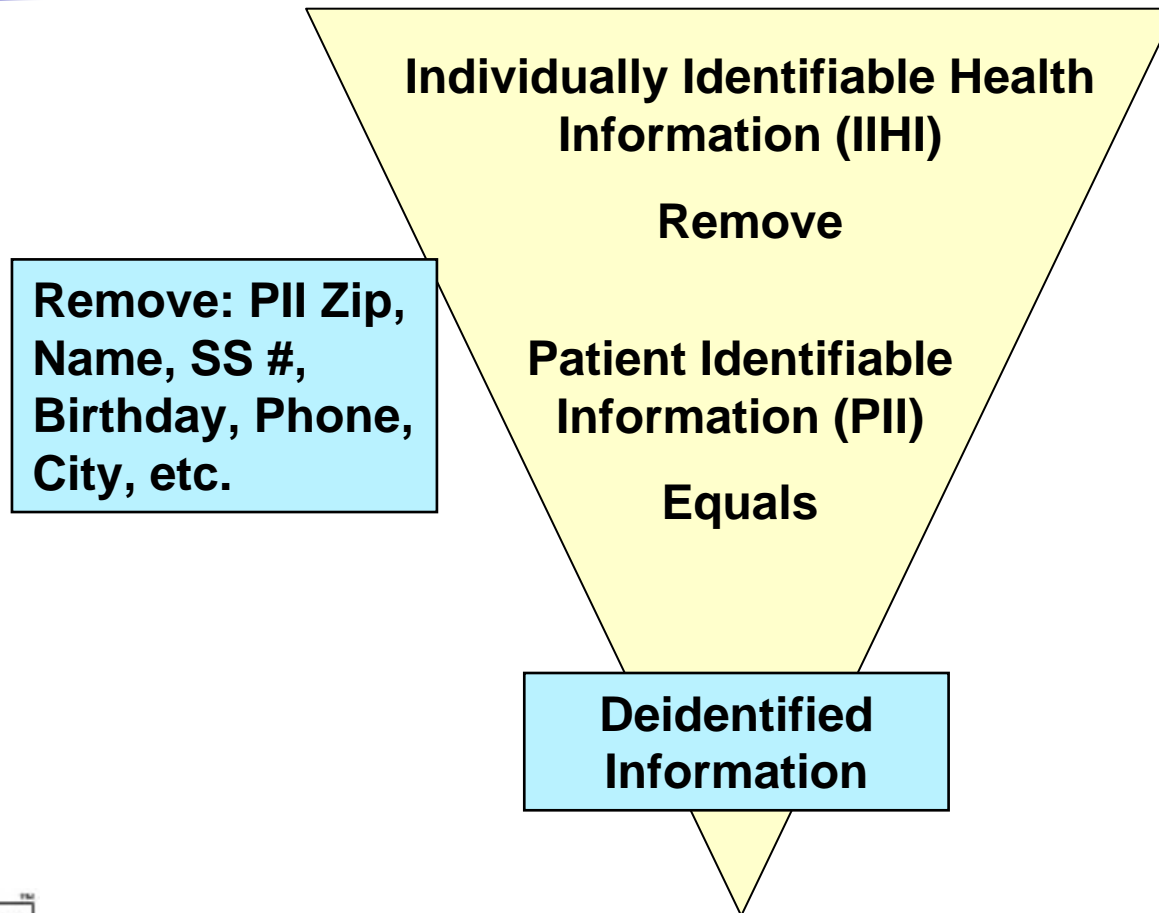




What is the Privacy Rule?

- Standards for Privacy of Individually Identifiable Health Information federal legislation, (aka The Privacy Rule)
- Provides national standards to control the flow of sensitive health information.
- Establishes real penalties (monetary, and perhaps prison terms) for disclosing this PHI improperly.

Protected Health Information



Sample identifiers – just to name a few

| | | |
|-------------|-----------------|---------------------|
| Name | City | Social Security # |
| Phone | Zip | Medical Record # |
| E-mail | State | Insurance Benefit # |
| Web URL | Tattoos | Driver's License # |
| Fingerprint | Fax | Admission Date |
| Photo | Date of Birth | Discharge Date |
| X-Ray | Date of Death | Prosthetic Device |
| MRI | Date of Surgery | Serial Numbers |



Deidentified Information

- Removing the identifiable information

Or

- A person with the appropriate knowledge

If

- You are deidentifying a small group of people



Small groups

- Over the age of 89
- Geographic areas
- Diseases effecting a small group of individuals



Safe Harbor Method

- Research
- Set by HHS
- Set of specific items that should be eliminated
- Appendix



Limited Data Sets

- Remove most common PHI items, as shown on Limited Data Set List.
 - May include dates such as birth date, admission date, dates of health care procedures or other services, and date of death.
 - May include geocodes (geographic mapping features) above the level that would identify an individual household, such as State, county, city, town census tract, precinct, or zip code.
 - Just enough PHI can remain to serve a unique purpose.
 - Not necessary to record in an Accounting of Disclosures.
- Appendix



Using and Disclosing PHI

Use

Sharing

Employing

Applying

Utilizing

Examining

Analyzing

*Information used when
moved inside
organizations*

Disclosure

Release

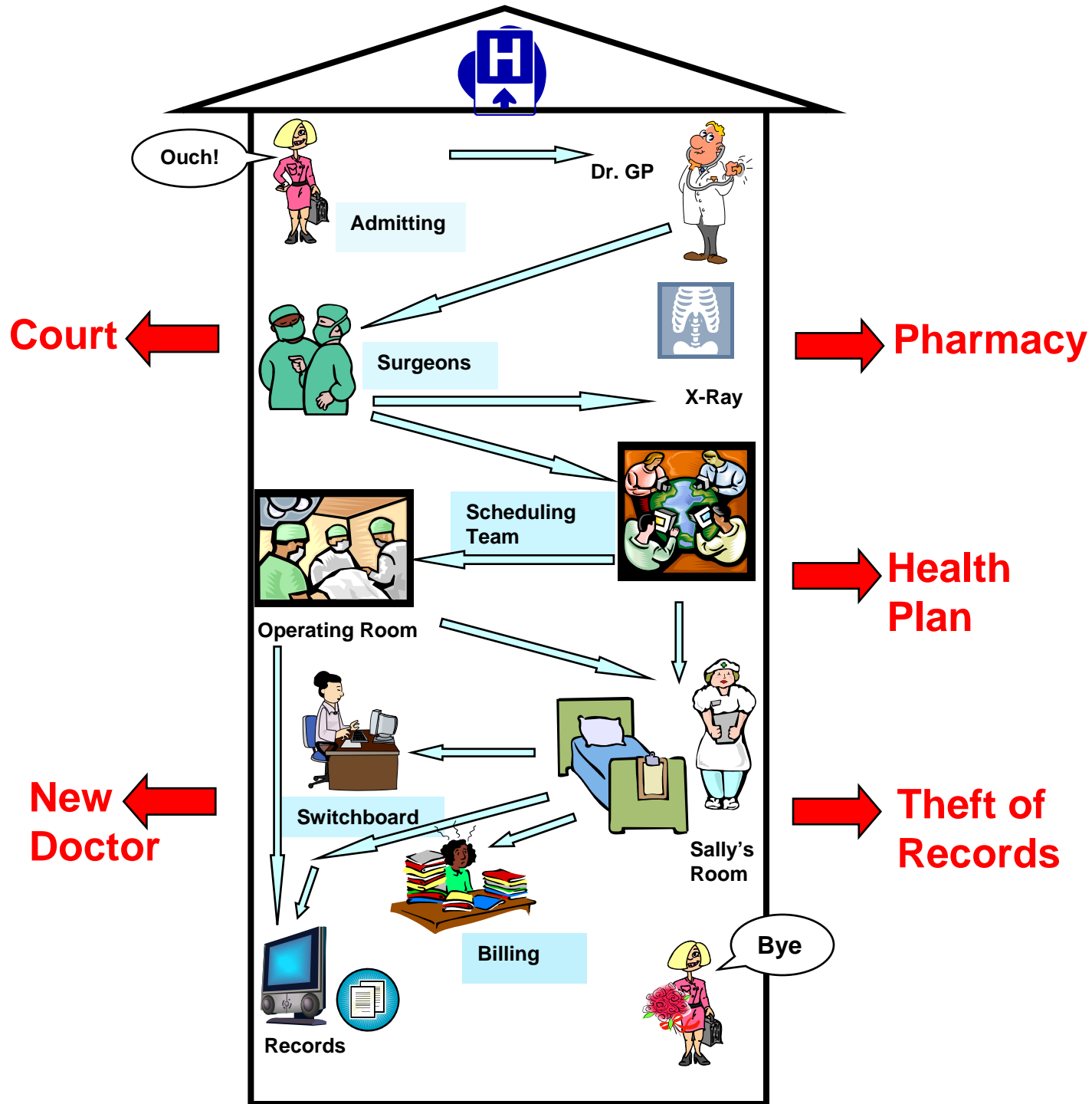
Transfer

Provision of access to

Divulging in any manner

Information disclosed

*when transmitted Outside
organizations*





Used and Disclosed PHI

PHI is “Used” within the organization, and “Disclosed” when it is transmitted outside the organization.

1. You have a right to see and get a copy of your health records.
2. You have a right to amend your health information.
3. You have a right to ask to get an Accounting of Disclosures of when and why your health information was shared for certain purposes.
4. You are entitled to receive a Notice of Privacy Practices that tells you how your health information may be used and shared.
5. You may decide if you want to give your Authorization before your health information may be used or shared for certain purposes, such as for Marketing.
6. You have the right to receive your information in a confidential manner.
7. You have a right to restrict who receives your information
8. If you believe your rights are being denied or your health information isn't being protected, you can:
 1. File a complaint with your provider or health insurer
 2. File a complaint with the U.S. Government





An Accounting of Disclosures HITECH Act

- Effective January 1, 2014
- Patients will have the right to see all of their records including TPO.
- This will be for the previous 3 years



Non-Routine Disclosures

National Priority Activities

State Licensing Boards

Public Health

Law Enforcement

Judicial and Administrative Proceedings

Research

Medical Examiner

Next of Kin Notification

Medical Error Databases

Emergency Treatment

These are tracked as
an “Accounting of Disclosures”



HITECH Act

- 1-1-2014 with EHR's
- Routine and Non Routine Disclosures
- Need to be listed
- Patients have a right to see this list
 - Doctor
 - Nurse
 - Billing



Incidental Disclosure

- *If all criteria is met, incidental use and disclosure might include:*
 - *Waiting room sign in sheets*
 - *Charts may be kept at patient bedsides*
 - *Dr's can talk to patients in semi private rooms*
 - *Dr's and nurses can discuss patient treatment at nurses stations*

Without fear of violation. HIPAA is not to interfere with quality patient care.



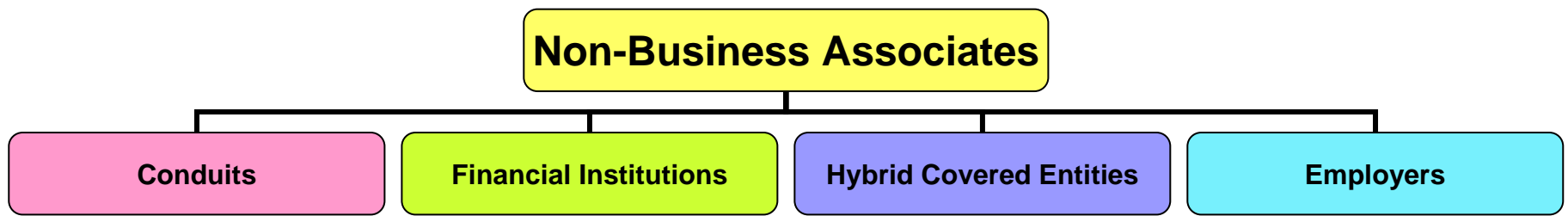
Your BA and the Collection Agency

With a BA you can share information:

- To collect on that account only
- Even if you get the information from another provider
- You can use other sources to collect
 - Ones with out BA



Others in the industry



Conduits

Conduits pass along PHI daily,
but are seldom aware of
what they are carrying.
US Postal, UPS,
FedEx, Courier Services,
or even your ISP
(Internet Service Provider)





Financial Institutions



Banks, credit card processors, automated clearinghouses, and electronic funds transfer services may pass along many of the details of health care records, but do not have access to the electronic data.



Other Covered Entities

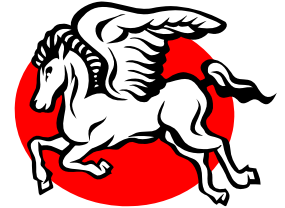
You will not need to get a BA from

- Doctor to the hospital
- Hospital to Medicare
- Dentist to Insurance Company

Hybrid Covered Entities



Some functions would qualify as HIPAA covered, yet the



organization may do other kinds of things which have nothing to do with the health care industry.



Separate PROCEDURALLY.



No need to PHYSICALLY separate the two kinds of data.



Minimum Necessary

“In every case, HIPAA requires that “use” and “disclosure” of PHI be limited to the “minimum necessary” to accomplish the intended or specified purpose.”

Minimum Necessary

- Covered entities make own assessment of what PHI is reasonably necessary for particular purpose
- Healthcare operations
 - Conduct training programs
- Disclosure and Use for Treatment
 - Explicitly exempt
 - Compartmentalization of Medical Records
 - Layers or buckets of information for various users with various authorization to view PHI





Minimum Necessary Standard

Covered Entities Must Take Reasonable Steps To See That The Use And Disclosure of PHI Is Limited To The “Minimum Necessary” To Accomplish The Intended, Specific Purpose --- and nothing more.



Non-Minimum Necessary Situations

1. When PHI is shared for treatment purposes.
2. When speaking to an individual about their own situation.
3. When you have a signed Authorization from an individual.
4. When you are using or disclosing data elements within compliance to HIPAA.
5. When disclosure to HHS is required by the Privacy Rule for enforcement purposes.
6. When there is a mandatory State Law or other law which requires disclosure.



HITECH Act

- Look for changes in this area in the future
 - Not to treatment – our providers need to access
 - Payment and Healthcare operations
 - With in 18 months of the effective date
 - Limitations
 - More clearly defined



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.

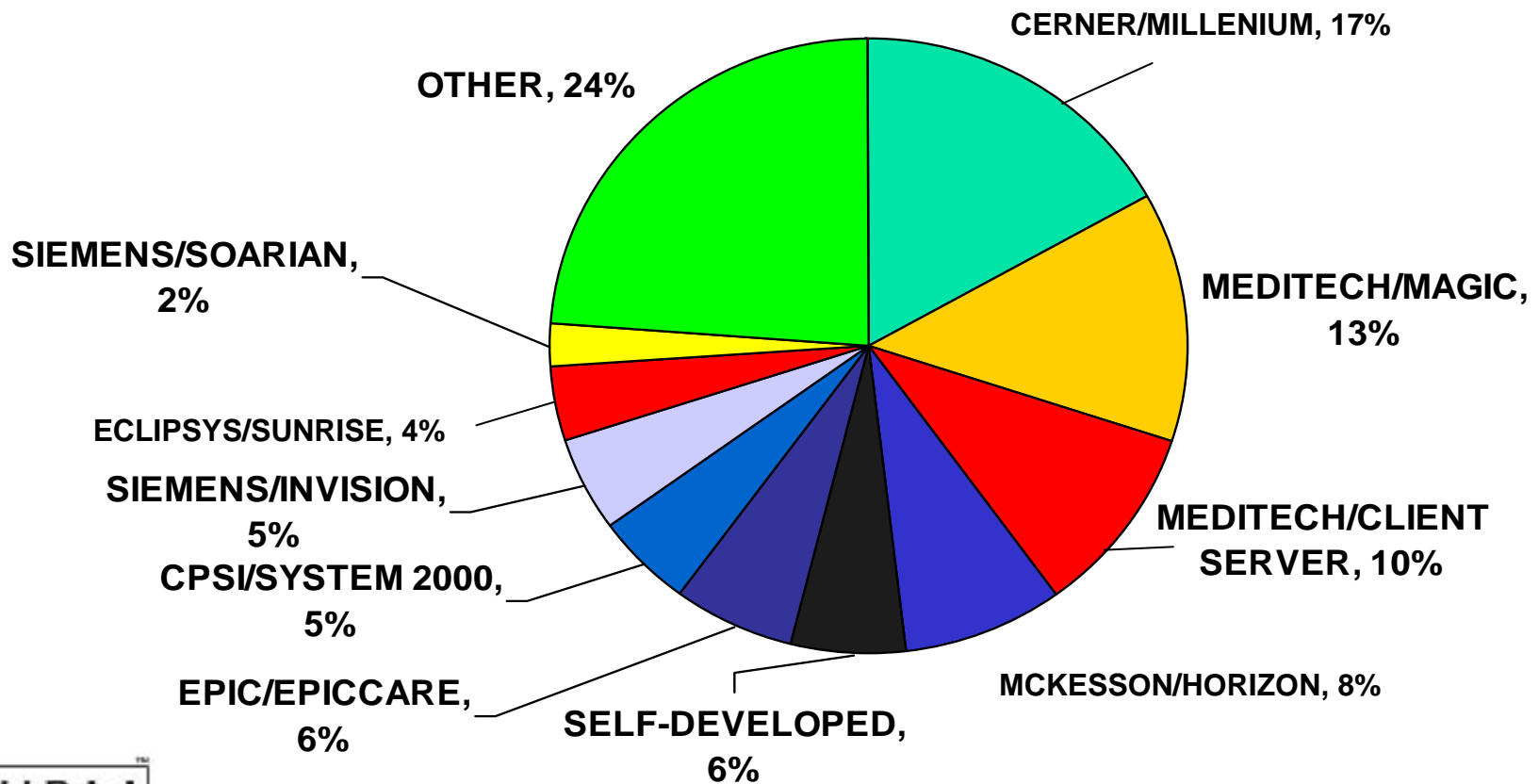
Set up a methodology which permits appropriate access and use of PHI, encouraging electronic means of using and transmitting PHI.



Where are we today?

Data from HIMSS Analytics

EMR US Hospital Market Share (n=2723 installations)

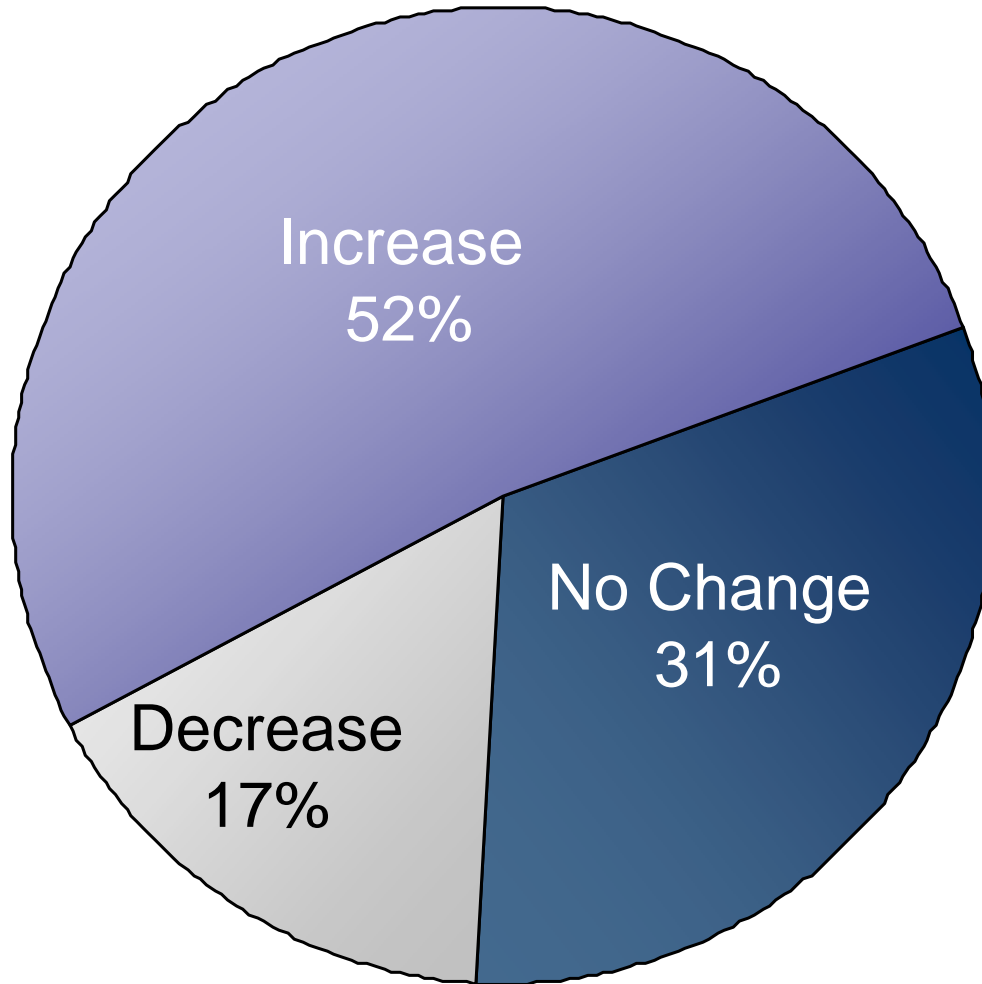


ecfirst – Home of The HIPAA Academy

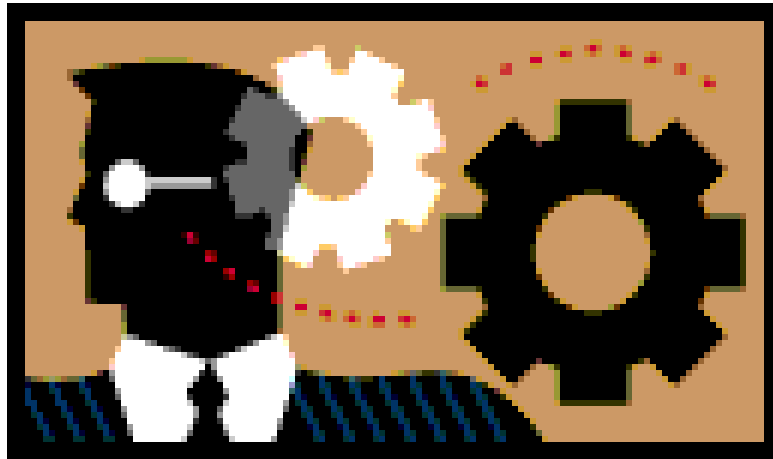
EMR Adoption Model Trends

| | | 2008 Final | 2009 Final |
|---------|---|---------------|---------------|
| Stage 7 | Medical record fully electronic; HCO able to contribute CCD as byproduct of EMR; Data warehousing/mining | 0.3% | 0.7% |
| Stage 6 | Physician documentation (structured templates), full CDSS (variance & compliance), full R-PACS | 0.5% | 1.6% |
| Stage 5 | Closed loop medication administration | 2.5% | 3.8% |
| Stage 4 | CPOE, Clinical Decision Support (clinical protocols) | 2.5% | 7.4% |
| Stage 3 | Clinical documentation (flow sheets), CDSS (error checking), PACS available outside Radiology | 35.7% | 50.9% |
| Stage 2 | Clinical Data Repository, Controlled Medical Vocabulary, CDSS inference engine, may have Document Imaging | 31.4% | 16.9% |
| Stage 1 | Ancillaries – Lab, Rad, Pharmacy – All Installed | 11.5% | 7.2% |
| Stage 0 | All Three Ancillaries Not Installed | 15.6% | 11.5% |

IT Budgets are moving up



We are moving in the
right direction



Is it secure?

| | | | |
|---------------|--|---|---------|
| 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 |

| | | | |
|---------------|--|--|-------------|
| 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 |



More recently...

January 26, 2010 - **Healthcare hacks on the rise**

Attempts to hack healthcare organizations doubled in the fourth quarter of last year, according to Atlanta-based managed security firm SecureWorks, setting the sector aside from others.

February 11, 2010 - **Number of victims grows for BlueCross data breach**

The number of victims affected by a data theft from Chattanooga-based health insurer BlueCross BlueShield has ballooned, following a decision by the company to notify family members of customers that are covered by a group plan.

March 9, 2010 - **Florida couple indicted for data theft**

A husband-and-wife team from Coral Gables has been indicted for the second time in a year for the theft and sale of privacy data. Authorities claim that in both cases, the couple received payments from personal injury lawyers in exchange for patients' personal privacy data from a local ambulance company.

From the OCR Website

| Org Name | # of records | Date | Type | Location | BA involved |
|--|--------------|-----------|-------------------|--|--------------------------------|
| Yale University | 1000 | 7/28/2010 | Theft | Laptop | |
| Holyoke Medical Center | 24750 | 7/26/2010 | Improper Disposal | Paper Records | |
| Jewish Hospital | 2089 | 7/16/2010 | Theft | Laptop | |
| Ward A. Morris, DDS | 2698 | 7/16/2010 | Theft | Desktop Computer | |
| Chattanooga Family Practice Associates, PC | 1711 | 7/15/2010 | Loss | Portable Electronic Device, Other | |
| David Gostnell, Ph.D. | 4000 | 7/7/2010 | Theft | Laptop | |
| Eastmoreland Surgical Clinic | 4328 | 7/5/2010 | Theft | Laptop, Desktop Computer, Portable Electronic Device | |
| Fort Worth Allergy and Asthma Associates | 25000 | 6/29/2010 | Theft | Network Server | |
| Charles Mitchell, MD | 6873 | 6/27/2010 | Theft | Desktop Computer | |
| Humana Inc. | 2631 | 6/25/2010 | Other | Paper Records | Matrix Imaging |
| John Deere Health Benefit Plan for Wage Employees | 1097 | 6/24/2010 | Other | Paper Records | UnitedHealth Insurance Company |
| Carolina Center for Development and Rehabilitation | 1590 | 6/24/2010 | Other | Paper Records | |
| Prince William County Community Services | 669 | 6/18/2010 | Theft | Portable Electronic Device | |
| University of Kentucky | 2027 | 6/18/2010 | Theft | Laptop | |



Defining Security

Having in place:

Controls

Countermeasures

Procedures



Common Criteria

1990's

Seven countries worked together

France , Canada, Germany, The Netherlands,
United Kingdom and United States

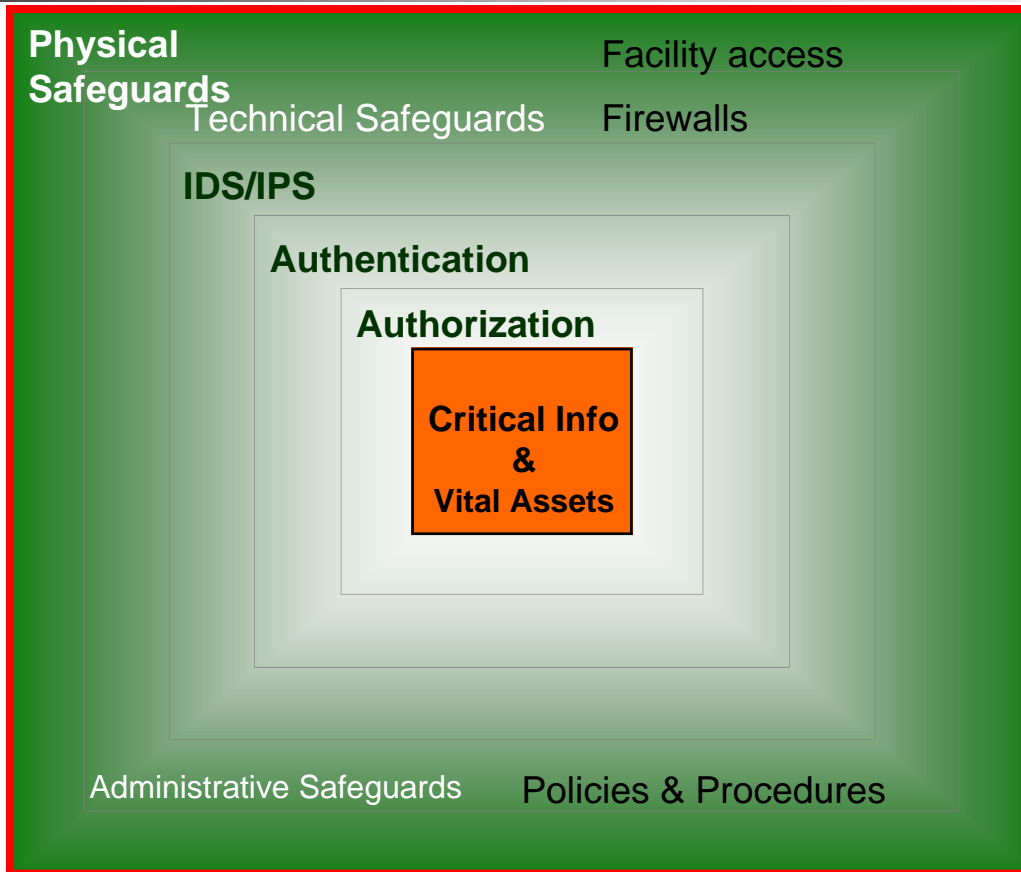


Security is minimizing the vulnerability of assets and resources

- 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.

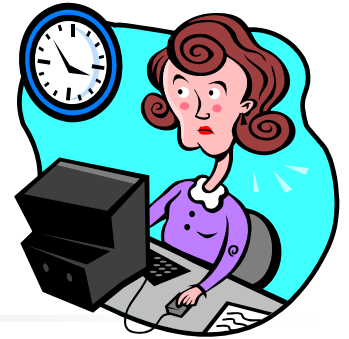
- Implement by:
 - Limiting permissions to a “need to know” basis related to job function.
 - Allow disclosure privileges only to users who have training and authority to make wise, HIPAA compliant decisions.
 - Install reliable authentication methods to identify system users and access control mechanisms 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



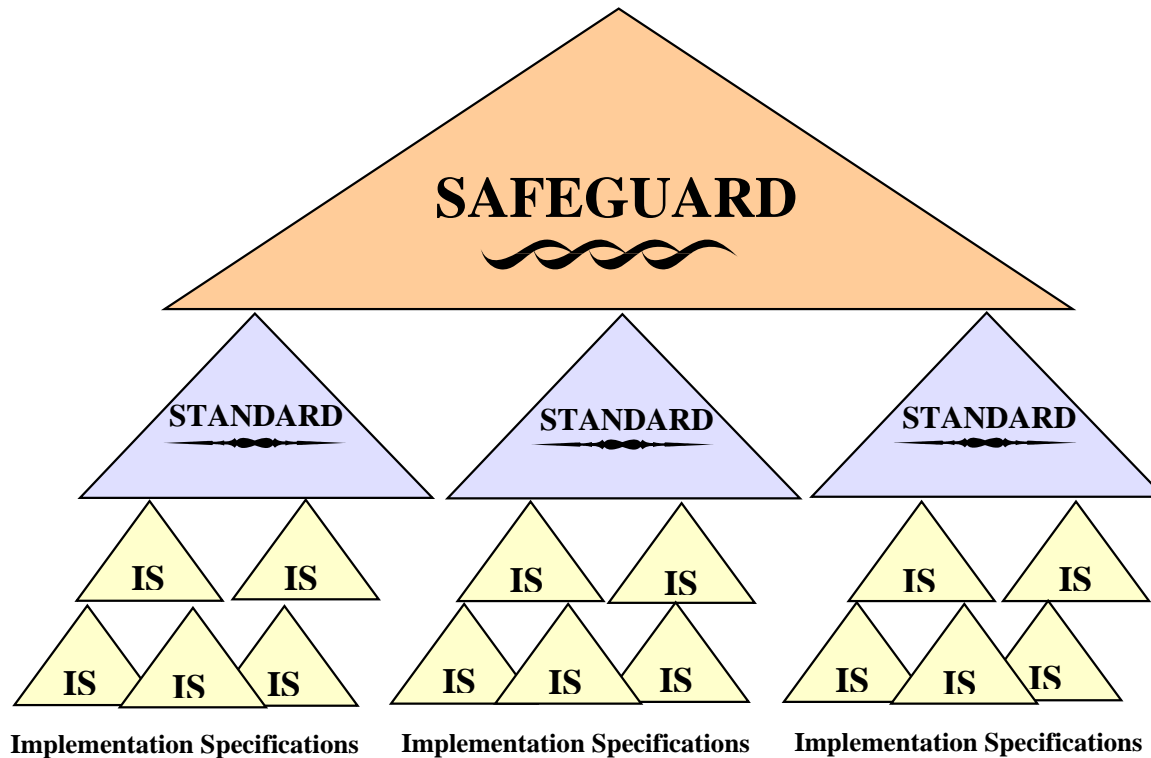
- Making PHI accessible to an authorized person when wanted and needed.
- Implement by:
 - Add policies and procedures that allow proper personnel to see and use PHI.
 - Guard against threats to the systems, and processes resulting in erroneous denial or unavailable computer systems.
 - Have appropriate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



Approach and Philosophy

Comprehensive
Technology Neutral
Scalable

Safeguards, Standards, and 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

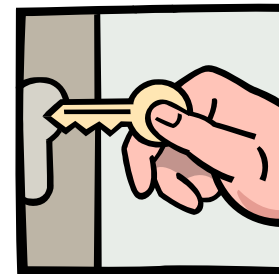


APT to Comply?

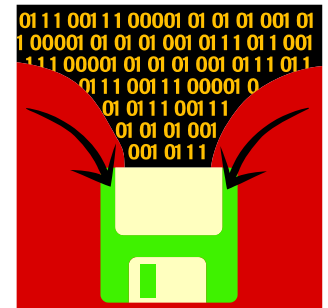
Aministrative Safeguards



Physical Safeguards



Technical Safeguards



Three HIPAA Security Domains

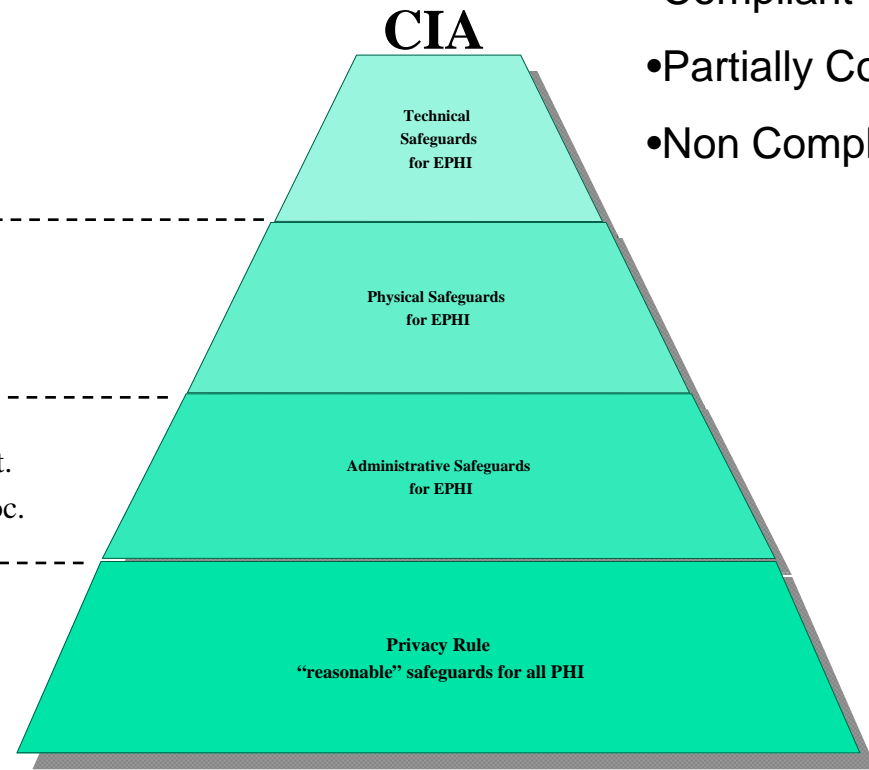
Security Standards

- 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

Within each **Security Standard** are Implementation Specifications

3 options

- Compliant
- Partially Compliant
- Non Compliant



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

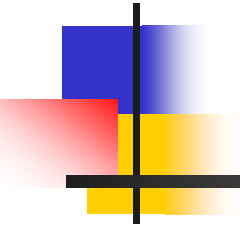
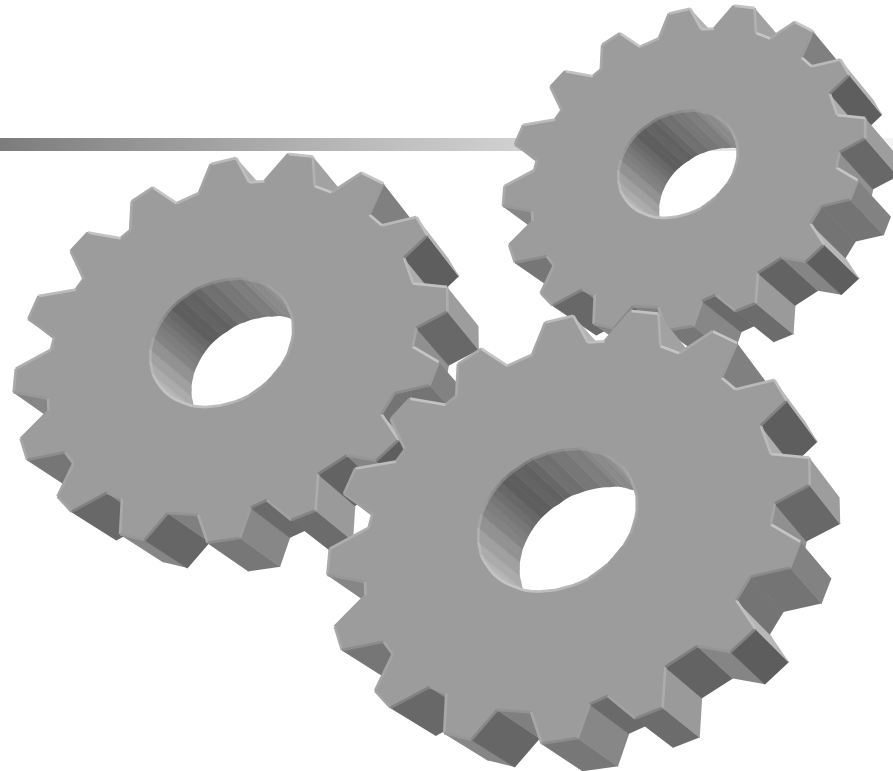
- Facility access
- Locking systems
- Monitoring for intrusion
- Environmental controls



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 |

Thursday, June 12, 2008 – Cedar Rapids Iowa, Mercy Medical Center



How do you recover from this?



What Chapter was this in at Nursing School?



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 |

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 |



Other Standards

Policies, Procedures and Documentation Requirements (164.316)

1. Policies and Procedures Standard
2. Documentation Standard



In Summary

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



Questions

