The Sixteenth National HIPAA Summit: Special Edition

Healthcare Privacy and Security Training and Professional Certification

Collocated with the Privacy Symposium at Harvard - Summer 2008
(One registration - attend two conferences)

Introduction of Certifications

Lorna L. Waggoner CHP

Certified HIPAA Administrator (CHA)
Certified HIPAA Professional (CHP)
Certified HIPAA Security Specialist (CHSS)

AMERICAN HOSPITAL ASSOCIATION ™ ENDORSED BY THE

eHIPAA ACADEMY ™

HIPAAacademy.Net

On-line leaning 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

Certified HIPAA Professional (CHP)

- CHA is the first section of CHP
- Electronic Transactions
- Code Sets
- Identifiers
- Introduction to the Security Rule
  - Safeguards
  - Standards

Certified HIPAA Security Specialist (CHSS)

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

CERTIFIED HIPAA SECURITY SPECIALIST™

HIPAA ACADEMY

HIPAA ACADEMY™

Today's curriculum

- CHA - 8:15AM to 3:00PM
  - **Upon completion you will have enough knowledge to test for CHA exam.**
- Introduction to Security - 3:00PM to 5:00PM
  - **Overview of the Security Rule**
  - **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

The Sixteenth National HIPAA Summit: Special Edition

Healthcare Privacy and Security Training and Professional Certification

Collocated with the Privacy Symposium at Harvard - Summer 2008
(One registration - attend two conferences)

Certified HIPAA Administrator™

(CHA™)

Lorna L. Waggoner, CHP
Director of Business Development, The HIPAA Academy, Waukee IA

Paul T. Smith, Esq
Partner and Co chair, HIT/HIPAA Practice, Davis Wright Tremaine LLP, San Francisco CA

AMERICAN HOSPITAL ASSOCIATION ™ ENDORSED BY THE

HIPAA ACADEMY ™

HIPAAacademy.Net

Agenda

- 8:15–10:00 Introduction to HIPAA
- Break
- 10:15–12:00 Introduction to HIPAA Privacy
- Lunch
- 1:00-2:45 Advanced HIPAA Privacy Topics
- Break
- 3:00–4:45 Introduction to HIPAA Security
- 4:45–5:00 Summary with Q&A

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.

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**

Learning Objectives Module 1

- What is HIPAA?
- What does HIPAA 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?

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?

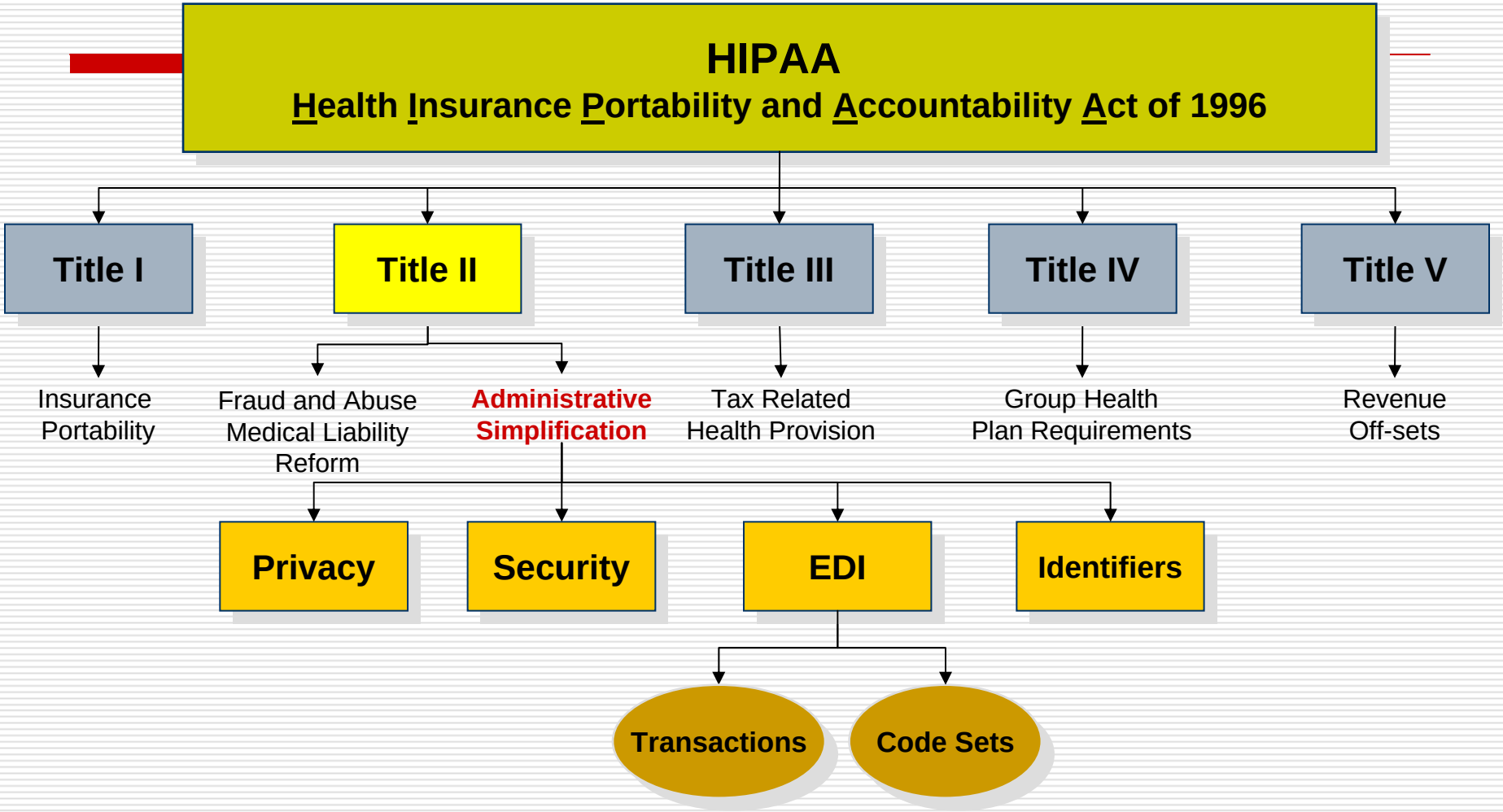
Five HIPAA "Titles" or Parts

- **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?



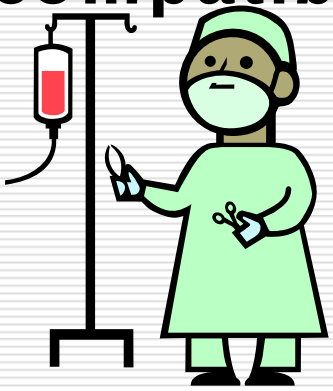
T.I.P.S about HIPAA Administrate Simplification Title II

Its all about.....

- Transactions and Code Sets
- Identifiers
- Privacy
- Security

Current Transaction Flow

- **Incompatible Formats**



Poof

Poof

Poof

Reject Incompatible

Process Correct Formats

Health Care Clearinghouse

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**

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

We will all be speaking the same language

HIPAALISH!

Department of Health and Human Services (HHS)

- Manages and enforces HIPAA Compliance
  - OCR – Privacy
  - CMS – Security and Transactions
- Gartner Group does research on costs
- American Hospital Association (AHA) helped to fund research to determine costs

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 is 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

Healthcare Industry

- Largest industry in the USA
  - 17% of the U.S. gross domestic product
  - Growing faster than the economy

- Significant challenges
  - Medical errors – 8th leading cause of death (HBR May 2006)
  - 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.

Healthcare Industry Solutions

- Future is about innovation and integration of technology
- Increase efficiency, improve care, and save consumers time
- Save lives

Bigger Challenges

- Changes to the current business practices
  - (they 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 clearing house system

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!

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

Who does HIPAA apply too?

- Four categories:
  - Payers
  - Providers
  - Clearinghouses
  - Business Associates

What's 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 covered function for us or on our behalf?
2. Are they a member of our workforce?
3. Do they use PHI (Protected Health Information)?

- **Yes / No / Yes Pattern = Business Associate**

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.

- None of us are getting out of this alive!
- We should 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 #	

- **"...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

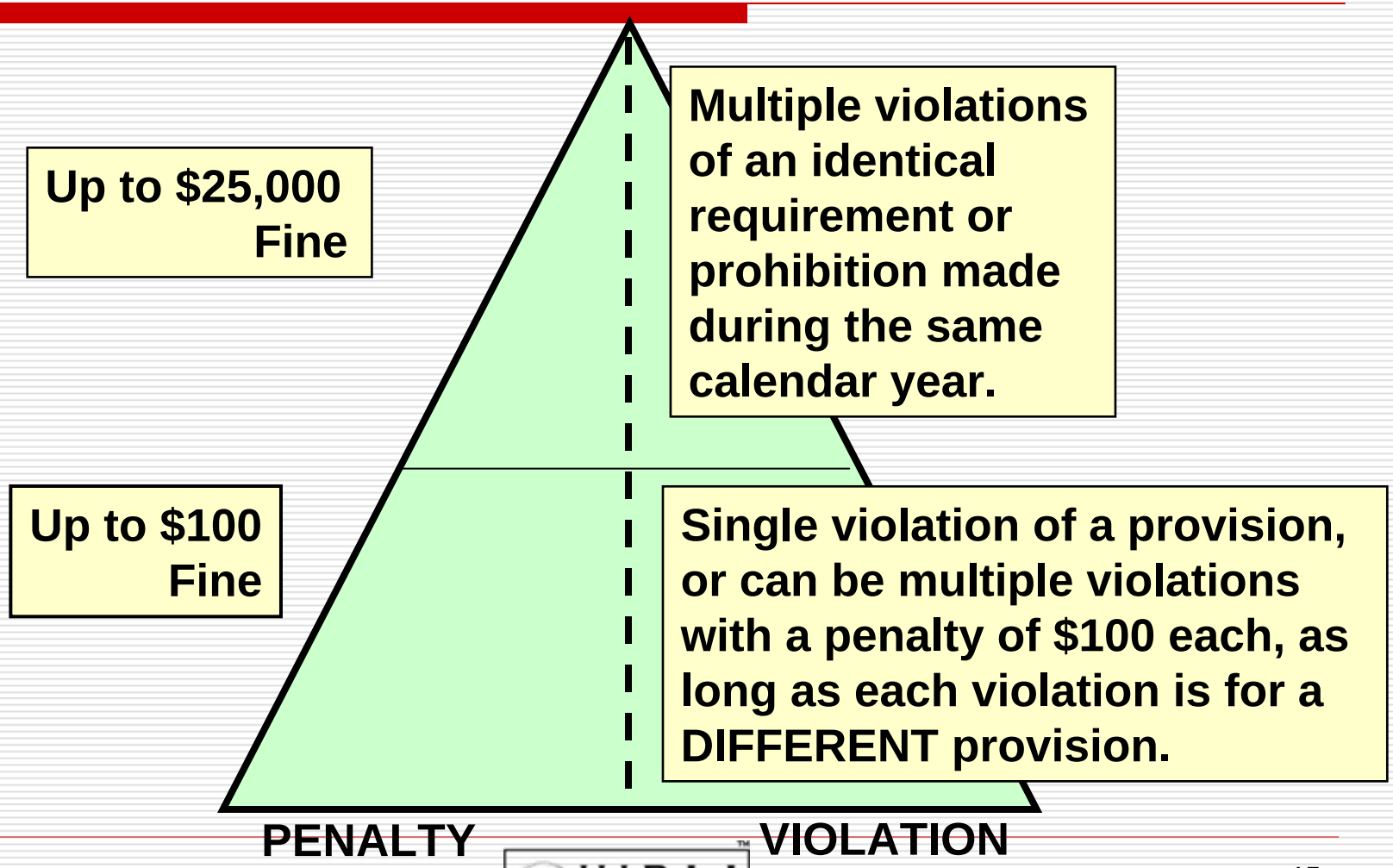
HIPAA is a good thing....

- It will protect us in many ways:
  - Save money
  - Improve healthcare
  - Save lives

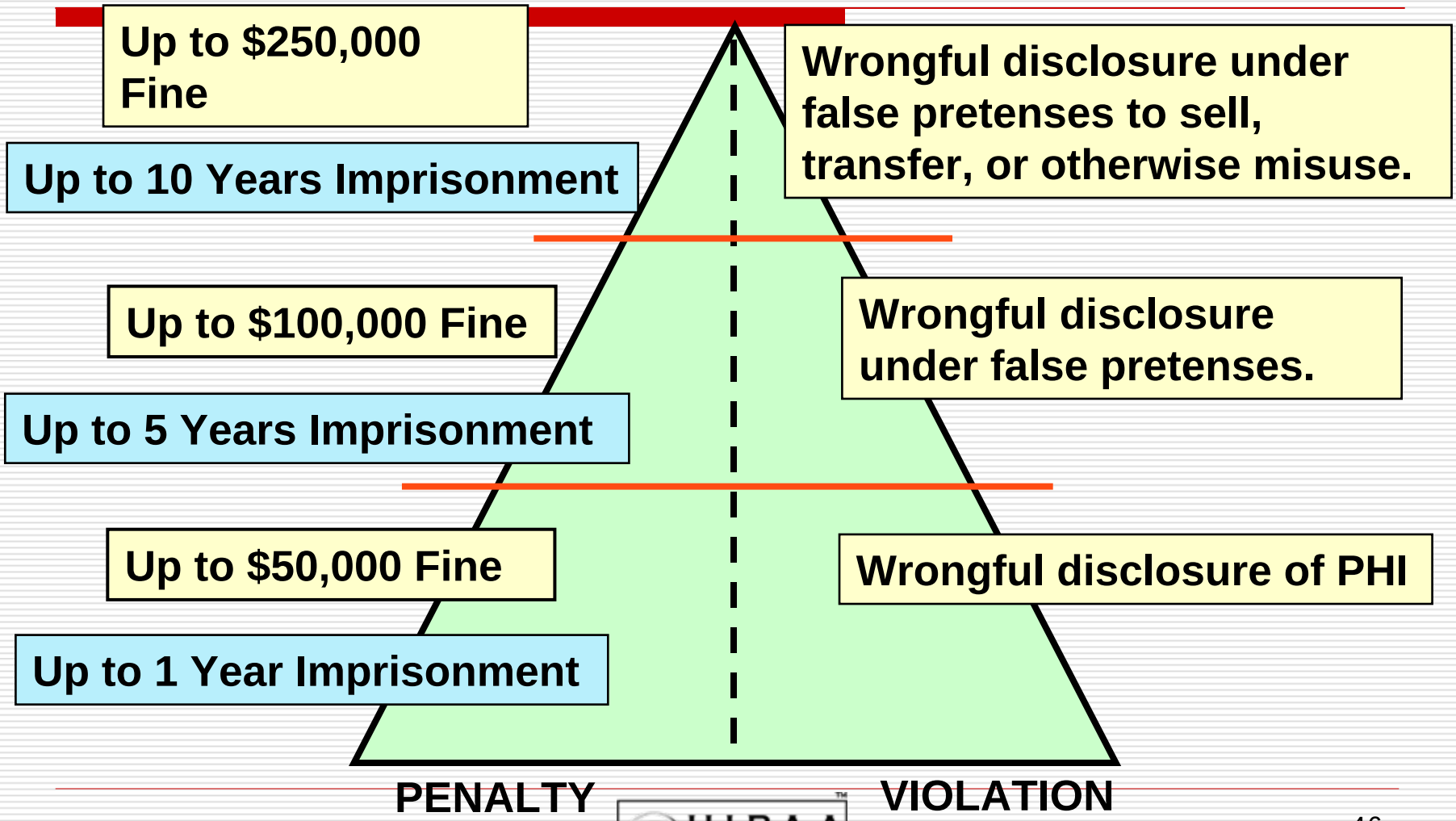
Does the punishment fit the Crime?

Let's look at the Punishment

Civil Penalties



Criminal Penalties



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.**

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.
- Covered Entities are liable for violations of HIPAA by employees, other members of their workforce, Business Associates without contracts.

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.

Business Associate Penalties?

- Business Associates are not covered entities and cannot be investigated under HIPAA laws.
- They have no threat of civil or criminal penalties resulting from non-compliance to HIPAA standards.
- They can, however, face civil litigation as a result of failure to perform HIPAA related safeguards outlined in the business contract with the covered entity.

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.

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

	Date Law Passed	Compliance Date	Comments
HIPAA	August 21, 1996		
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 Rule	February 20, 2003	April 21, 2005	Covered Entities
Security Rule		April 21, 2006	Small Health Plans

Check Your Knowledge

- Any covered entity and the Senior Executives can be penalized up to 1 year in prison and a 50,000 fine for:

  - A. Wrongful Disclosure of PHI
  - B. Wrongful disclosure to another Covered Entity.
  - C. Wrongful disclosure under false pretenses.
  - D. Wrongful disclosure under false pretenses to sell, transfer, or otherwise misuse

Check Your Knowledge

- HIPAA rules and regulations became law in:
- (Select the correct answer)

A. 1942
B. 1996
C. 2005
D. 2003
E. 1999

Check Your Knowledge

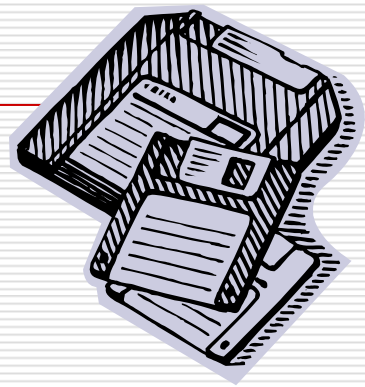
- HIPAA defines Covered Entities as:
- (Check all that apply)

A. Payers
B. Vendors
C. Providers
D. Business Associates
E. Clearinghouses

Advanced HIPAA Privacy

- What is the Privacy Act?
- How Can I Use and Disclose PHI?
- Do Patients Have Any Rights?
- What New Forms Do I Need?
- Do I Have to Authorize Everything?
- Who are Non-Business Associates?
- Employers – What Role Is This Anyway?
- Who decides “Minimum Necessary”?
- To Market or Not To Market?
- Privacy Wrap up – what is done?

What is the Privacy Rule?



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

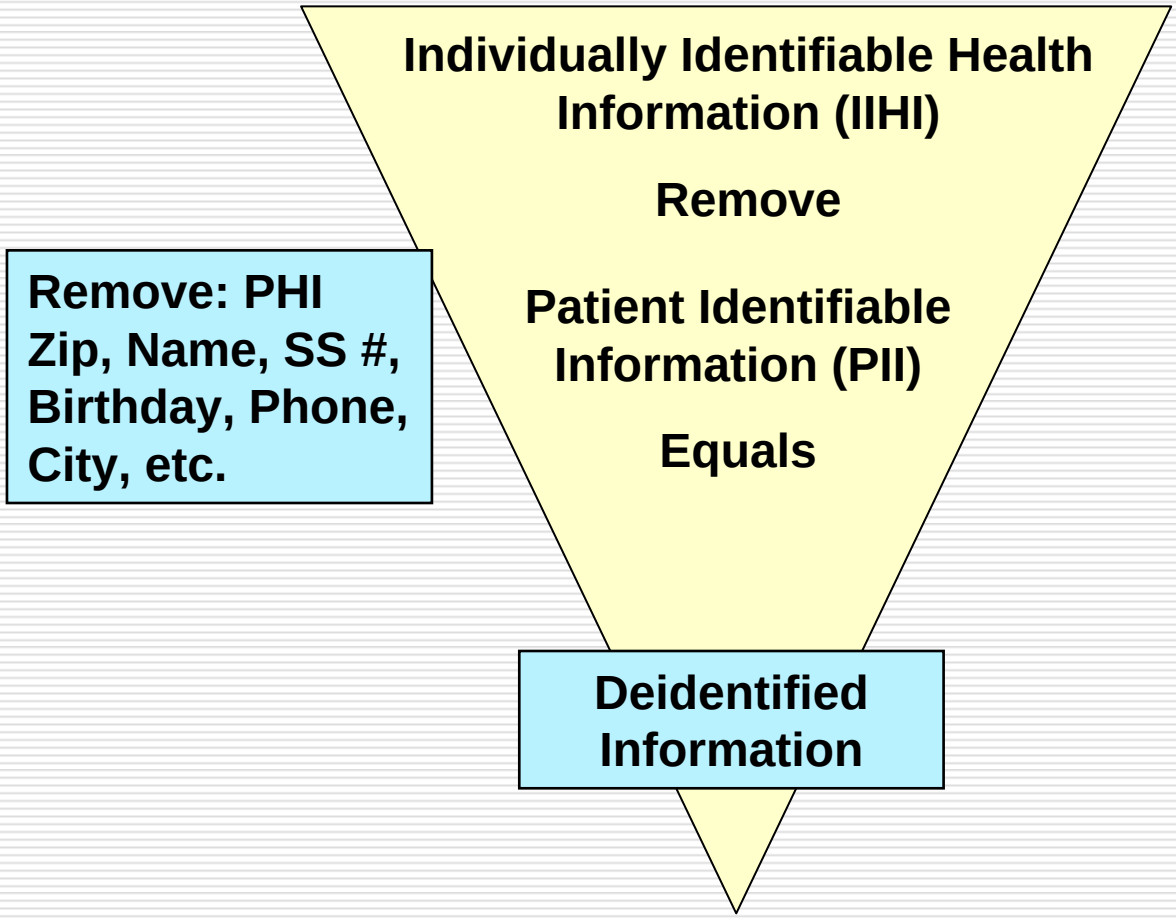
What is the Privacy Rule?

- 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 data improperly.

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

Protected Health Information



Other identifiers

- We can be identified by other things:
  - Older Americans
  - Sexually Transmitted Diseases
  - Small Geographic areas

Deidentified Information

- Removing the identifiable information
  - Or
- A person with the appropriate knowledge
  - If
- you are deidentifying a small group of people

Deidentified Information

- Appropriate knowledge:
- Statistician
  - Small groups
    - Older Americans
    - HIV or other sexually transmitted diseases
    - Geographical areas with smaller population

Safe Harbor Method

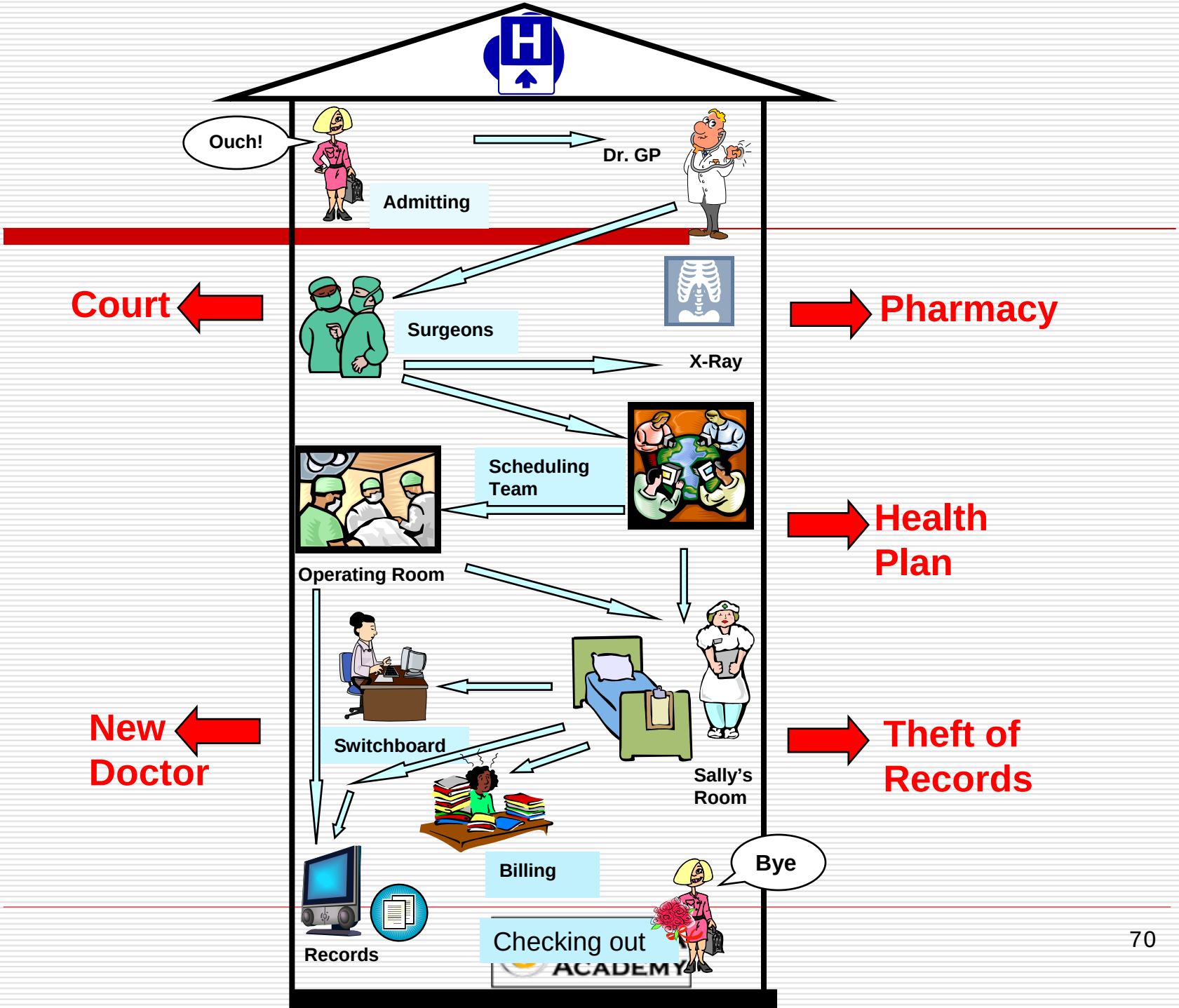
- Set by DHS
- Set of specific items that should be eliminated
- A list of 18 items
- Re-identification codes are allowed

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 track, precinct, or zip code.
- Just enough PHI can remain to serve a unique purpose.
- Not necessary to record in an Accounting of Disclosures.
- Re identification codes are not permitted

Using and Disclosing PHI

- *Use*
  - *Sharing*
  - *employing*
  - *applying*
  - *utilizing*
  - *examining*
  - *analyzing*
  - *information used when moved Inside organization*
- *Disclosure*
  - *release*
  - *transfer*
  - *provision of access to*
  - *divulging in any manner*
  - *information disclosed when transmitted Outside organizations*


Ouch!
Admitting
Dr. GP
Court
Surgeons
X-Ray
Pharmacy
Scheduling Team
Health Plan
Operating Room
New Doctor
Switchboard
Sally's Room
Theft of Records
Billing
Bye
Records
Checking out

Used and Disclosed PHI

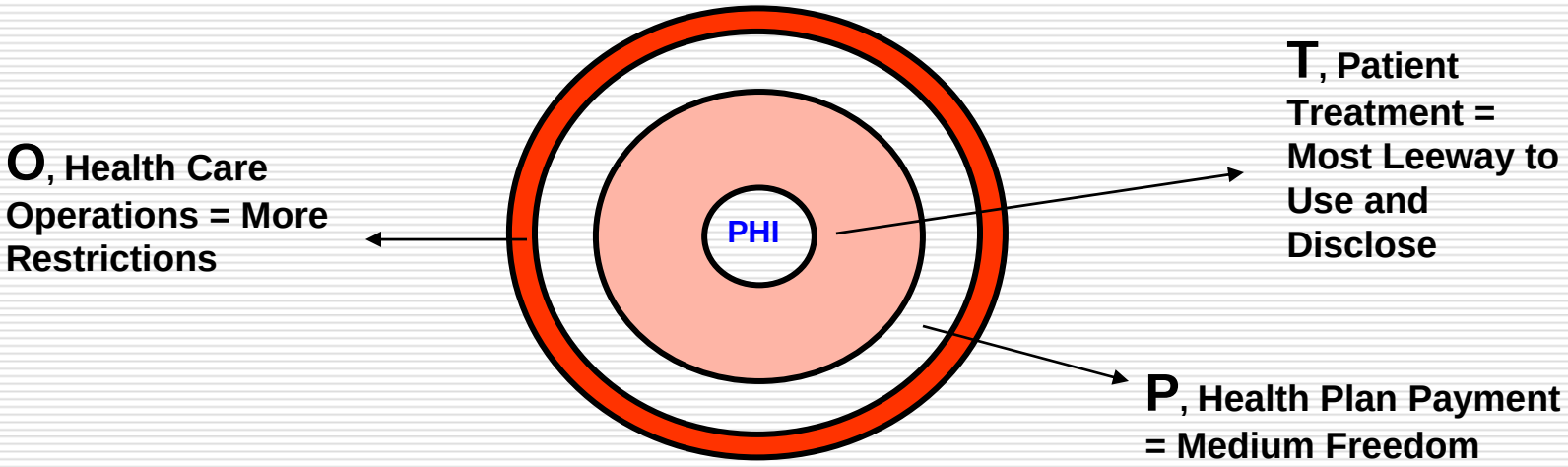
- **PHI is "Used" within the organization, "Disclosed" when it is transmitted outside the organization.**

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**

Four Kinds of Disclosure

- Routine
  -  Mandatory
- Non-ROutiNe
  - *Incidental*

Treatment, Payment and Healthcare Operations (TPO) are Routine.



Mandatory Disclosure
only 2 situations

1. PHI It must be disclosed (with certain exceptions) given to the patient, when he/she asks to review or copy it.

2. PHI It must be disclosed given to the Department of Health and Human Services (HHS) for regulatory compliance action which may be undertaken in enforcing the Privacy Rule.

Patient Rights - Receive a copy of your records - a mandatory disclosure

- Patients have a right to receive a copy of their medical information.
  - They can get a copy
  - You can charge what it costs
  - Reasonable costs
  - within a reasonable time frame
    - What is reasonable?

Patient Rights – Amend Records

- Patients can amend their records
  - *If a patient sees an error in their medical record they have a right to have it amended.*
    - *Medical records are not corrected or changed*
    - *Medical records are amended*
- The covered entity can accept a request for amendment
- The covered entity can deny the request of amendment

Patient Rights – Amend Records

- *if denied, provide written denial notice*
- *permit individual to submit written response to denial notice*
- *covered entity may then write rebuttal*
- *All communications must be attached to the disputed information for all subsequent disclosures of the disputed information*

Patient Rights
An Accounting of Disclosures

- *Patient can request a list of disclosures made by a covered entity*
- *Who has looked at my medical record?*

Non-Routine Disclosures

- National Priority Activities
  - State Licensing Boards
- Public Health
  - Research
- Judicial and Administrative Proceedings
  - Law Enforcement
- Medical Examiner
  - Next of Kin Notification
- Medical Error Databases
  - Emergency Treatment

Accounting of Discloures

- All non-routine disclosures are tracked as an “Accounting of Disclosures”
- A requirement under HIPAA

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.***

Unprotected Information

- HIPAA does not protect health information in the hands of non-covered entities.
- However, as a general rule covered entities may disclose protected health information to non-covered entities only:
  - to health care providers for treatment
  - to contractors who have signed a confidentiality agreement
  - to government agencies where permitted or required by other laws, or
  - with specific patient authorization.

Forms, Forms, Forms

- Consent
- Authorization
- Notice of Privacy Practices

Consent Forms (Optional)

- No Consent Form is needed for
- TPO (Treatment, Payment or Operations)

- Unnecessary Authorizations
  - =
- Unnecessary Legal Liability

- If you erroneously have the patient sign to allow TPO uses, they also have the right to revoke that usage.

- Privacy Rule covers your use of TPO, and it can't be revoked.
  - Leave it alone!
- **However, your state may have a consent requirement!**

Authorization

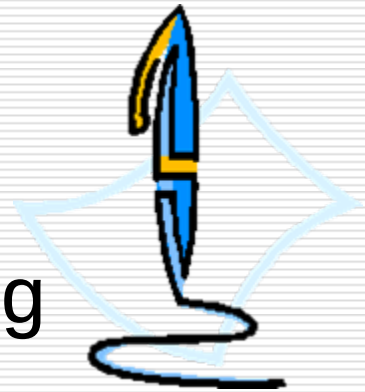
- Customized document
- Can't refuse treatment or coverage
- Detailed and Specific
- Includes expiration date
- Disclosures made by valid authorization do not need to be tracked and reported to the individual

Core Data Elements of Authorization

- Description of information used
- Identification of person authorized to use/disclose information
- Party to whom disclosure/use will be made
- Expiration Date
- Statement of right to revoke
- Re-disclosure is allowed
- Representative's authority to act
- Plain language

Authorization for Use and Disclosure

- Authorization
  - describes specific elements and disclosure of PHI
  - permits disclosure and use by covered entity that obtains authorization
- Revocations
  - Generally, must be in writing
  - Should be dated



Compound Authorizations

- Authorizations can be combined with other “like” authorizations
  - a research authorization can be combined with any
  - other specific request that relates to the same study
- Unlike authorizations cannot be combined.
  - not research with notifying the media

Authorization Restrictions

- Patients have a right to Restrict Authorizations
- They can authorize all or a portion of the information they authorize release of.
- Patients can also revoke authorization

Defective Authorizations

- Authorization is invalid if:
  - expiration date or event has passed
  - form is incompletely filled out
  - it is revoked
  - if a condition of treatment on it
  - anything on the form is known to be false by the covered entity

Notice of Privacy Practices

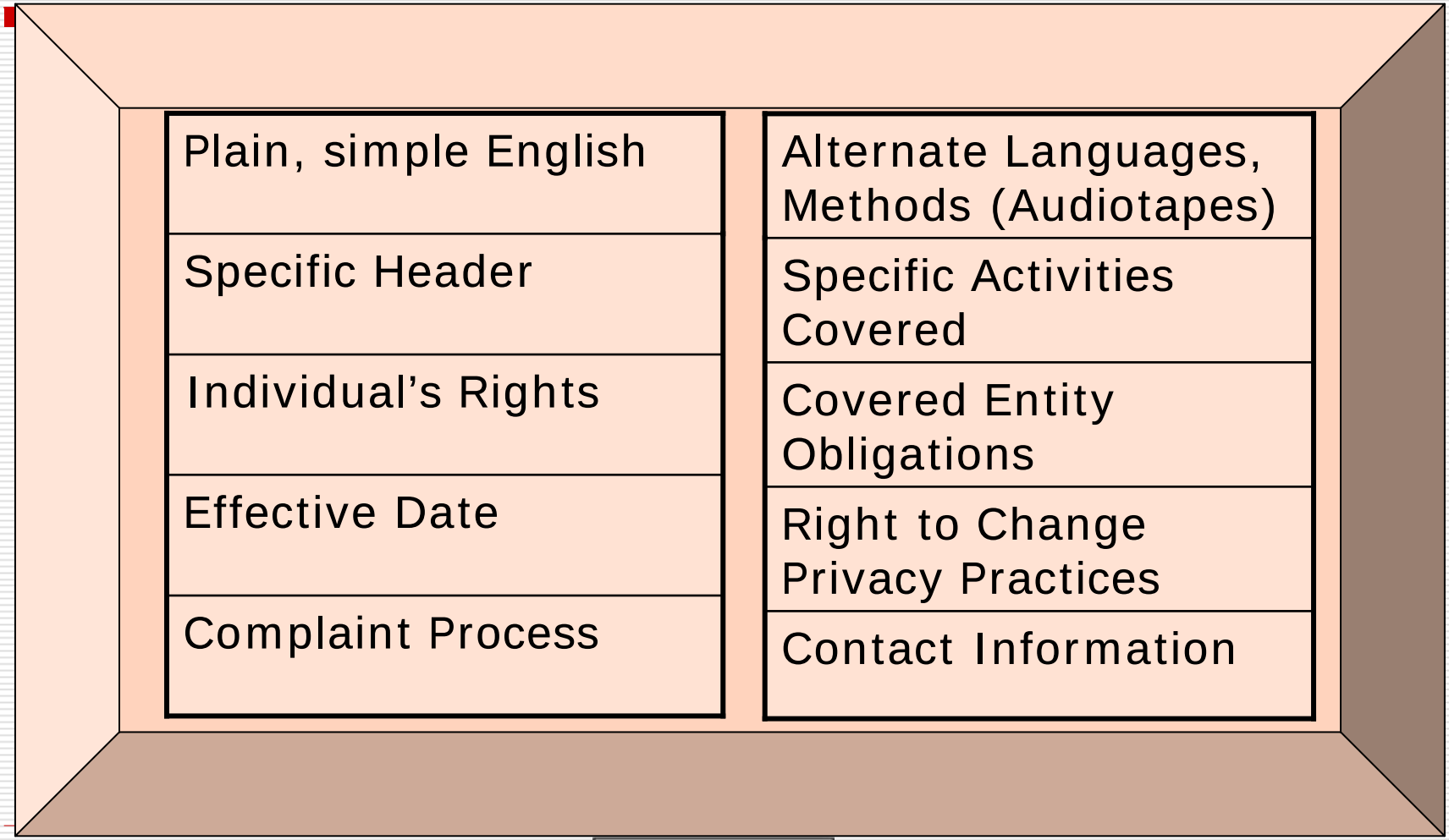
- must describe use and disclosure of PHI and the individual's rights
- must describe the covered entity's duties
  - legally obligated to protect PHI, provide Notice, and abide by terms
- indicate how to register complaints
- specify a point of contact
- specify an effective date

Notice of Privacy Practices

- Specific wording in the Heading

  - "This Notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review carefully."

Notice of Privacy Practices Guidelines



Other Notice Requirements

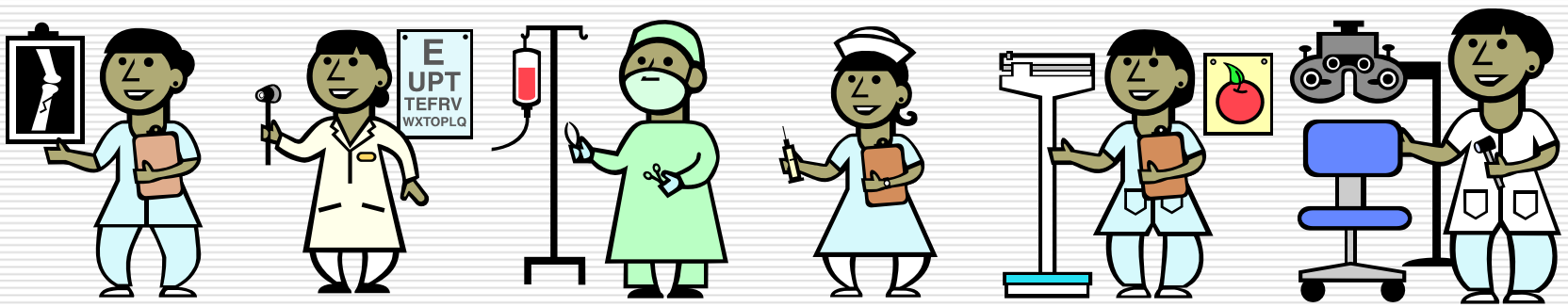
- Changes
  - The entity reserves the right to make changes if and when things change.
  - If significant changes are made a new NOPP must go out again or every 3 years (Payors).
- Activity in Notice
  - If no activity is included then the entity must obtain individuals authorization
    - If your facility puts the patient name on their door.
      - List in NOPP
      - Patient can opt out

Electronic Notice

- Notices can be sent electronically
- Covered Entities with web sites must prominently post their Notice on the site
- Notices can be sent via e-mail
- if first treatment is electronic (such as an Internet pharmacy) must provide an electronic Notice in response to that treatment

Direct Treatment Providers

- ***Provide Notice of Privacy Practice (NOPP) first date of service. (Good faith effort.)***
- ***Written Acknowledgement of Receipt.***
- ***(Good faith effort.)***
- ***Posted Notice in Providers office***
- ***Take-home copies available.***

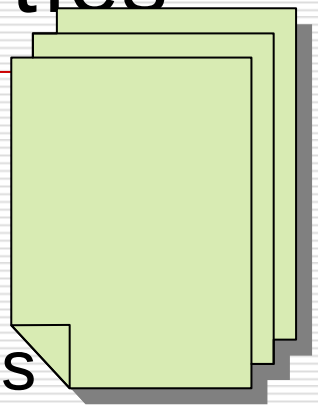


Organized Health Care Arrangement (OHCA) Utilize, Joint Notice

- ***Covered entities that are part of an OHCA group***
- ***physicians working in a clinically integrated setting can agree to a collective way to handle PHI and share it among themselves.***
- ***Each entity has agreed to be bound by the "signed off" of the OHCA's group PHI privacy practices.***

1. *Each entity is specifically described, so that the recipient knows who is obligated by this notice to protect their personal information.*
2. *Each covered site or location is listed.*
3. *The OHCA They makes a good faith efforts to obtain for ONE of the participating entities to get a written Acknowledgement of Receipt*

Health Plan NOPP Responsibilities



- Make a Notice available on request.
- Give a Notice to new plan participants the time they enroll.
- Give a Notice to currently covered participants within 60 days of a material revision.
-
- At least every 3 years, those covered by the plan must be alerted that a Notice is available and how to get one.

GIVE, GET, KEEP

GIVE
Notice of Privacy Practice

GET
Acknowledgement of Receipt

KEEP for 6+ years
1 Copy Each Notice Version
All Signed Acknowledgements
All Authorizations for Release of PHI
All Accountings of Disclosure

Record Keeping

- ***Notice of Privacy Practices (NOPP)***
  - ***including written acknowledgements of receipt***
- ***Authorizations***
- ***Consents***

Must be retained for a minimum of 6 years from the date created, or when last in effect.

Unique Release Situations

- **Third Party Labs- not authorized to release information to the patient.**
- **Food and Drug Administration – can be given PHI in the spirit of Public Health.**
- **Psychotherapy Notes - Are not a part of the medical Record.**
- **Personal Representatives – have the same rights as patients.**

Patient Rights
Confidential Communications

- Patients have a right to receive their information in a confidential manner
  - Alternate Address
  - Alternate Phone

Fair Debt Collection Practices Act

- Regulates the activities of those who regul collect debts from others.
- Protects consumers from abuse, harassment, false and misleading tricks, and illegal collection practices.
- For personal, family, or household debt, but does cover debt for MEDICAL CARE.
- Does not conflict with HIPAA legislation.

Business Associates

- Person or entity who performs functions on the behalf of a covered entity
- May have access to PHI.
- Not a member of entity's workforce
- Privacy violations of business associates:
  - entity not liable for privacy violations
  - not required to actively monitor or oversee
  - entity must take reasonable steps to cure breach or end violation

Who might be a Business Associate?

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

Privacy Violations of Business Associates

- **Covered Entity is not liable for privacy violations of a Business Associate**
- ***Business Associate must advise Covered Entity if violations occur.***
- ***Entity must take "reasonable steps" to cure the breach or end the violation.***
- ***Entity must terminate contract if feasible. If violations continue or report the Business Associate to the HHS.***
- ***If entity does not follow these steps they are in violation.***

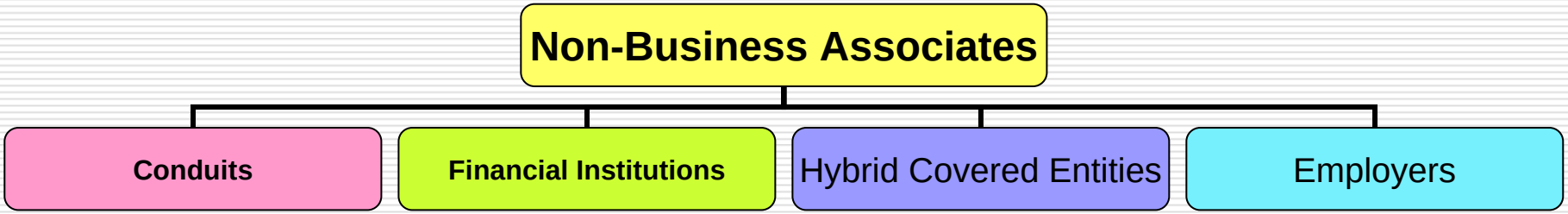
Business Associate Contract:

- *Must do two things:*

1. Specify what the PHI received will be, how the Business Associate can use it, and when it can be disclosed, if necessary.

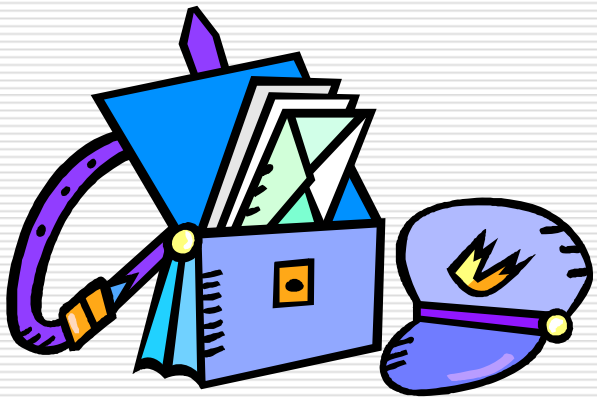
2. Impose clear expectations that the Business Associate will protect PHI, and require them to notify you if there has been a violation.

Non-Business Associates



Conduits

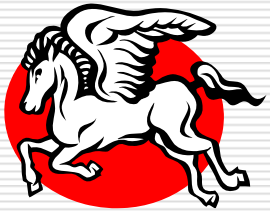
- Conduits pass along PHI daily,
- but are seldom aware of
- what they are carrying.
- US Postal, UPS,
- FedEx, Courier Services,
- or even your ISP
- (Internet Service Provider)



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.

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.

Employers

- Under HIPAA, Hospitals Protect
  - Data They Create, Receive, or
  - Maintain Regarding Employees
    - as Patients.

- Under HIPAA, Hospitals as Employe
- are Not Required to Protect
- Employee Records as PHI.

Government Access to PHI

- *HHS will have access to PHI, on a case by case basis, during the investigation of any complaints which have been filed with them.*
- *The Secretary of HHS has divided the enforcement responsibilities in support of HIPAA.*
- *Receiving and investigating complaints, as they may relate to the Privacy Rule, to the OCR (Office for Civil Rights).*
- *The Administrator of CMS (Centers for Medicare and Medicaid Services) will handle potential violations of the Transaction and Code Set Rule, the National Employer Identifier Number, and the Security Rule.*

More control over law enforcement with HIPAA

- Federal, state, and local law enforcement agencies did not get their roles expanded by HIPAA.
- Have more limited access to medical data than in the past.
- Gone are the days of a policeman walking into the emergency room to question doctors and nurses about the details of a patient's condition, to get personal identification and contact information from hospital records, or to gather lab results and samples for scrutiny in the police lab.

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 Provisions Excluded

- Treatment Purposes
- Individual who is the subject of the information
- Required for Compliance with HIPAA
- If HHS requires information for enforcement of the rule
- Required by law

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.

Reasonable Reliance

- Public Agency Representative
- Another Covered Entity
- Workforce Member or Business Associate
- A Researcher from Institutional Review Board (IRB) or Privacy Board

To Market or Not To Market?

- The communication isn't marketing when
  1. It describes a covered entities' own products or services, or information regarding how payment for those services will be handled.
  2. It has to do with the treatment of the individual.
  3. It shares information to coordinate the care or investigate alternative treatments, therapies, or providers for the benefit of the patient.

This is not Marketing

- Describing providers in a network
- Describing the covered entities own health-related products or services
- Describing the benefits of a health plan
- Anything about the individual's treatment
- Case management or care coordination for the individual
- Directions or recommendations for alternative treatments, therapies, health care providers, or settings of care to that individual
- General information about health

Providers can:

- *Disclosure of PHI for marketing when communication is*
  - *face-to-face (Your doctor providing samples)*
  - *of nominal value (Pens or key chains)*

(These are the only two exceptions!)

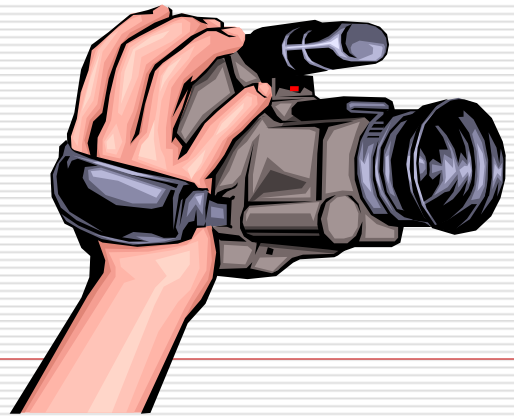
- *Anything else requires an authorization*
  - *The authorization must include a statement whenever the marketing involves direct or indirect remuneration to the covered entity from a third party.*

Protect Oral PHI

- Assign a Privacy Officer
- Train Employees
- Post Reminders
- Lower Your Voice
- Choose Voice Mail Wording Carefully
- Watch For Reception Room Violations
- Be Aware in Back Offices
- Protect Audiotapes
- Sign Language Exposure
- Guard Cell Phone Dialogues

Designated Record Sets

- Taped or Recorded patient information becomes
- a “designated record set” and must be protected as PHI.



Are Co-Workers Protected?

- Respect the privacy of co-workers and colleagues who are patients.
- Do not discuss the health care services of your co-workers with anyone not directly involved in their care.
- Do not ask co-workers why they are patients.
- Do not access their PHI unless it is for patient care or billing purposes.

Keep your ears and eyes open!

- We should all be thinking about HIPAA everyday
- Always protecting PHI
- Is there just one little improvement I can make today
- This will not require us to rebuild our office space
- Reasonable and Appropriate!

Check Your Knowledge

- **There are several forms due to HIPAA which one is optional?**
- (Select the correct answer)

- A. Notice of Privacy Practices
- B. Authorization
- C. Consent
- D. Consent for Treatment
- E. Acknowledgement of Authorization

Check Your Knowledge

- **Business Associates**
- (Select the correct answer)

A. Are a part of the workforce
B. Do not have access to PHI
C. Must have an office in the facility
D. Have access to PHI to do their job
E. Do not need a written agreement

Check Your Knowledge

- **Under HIPAA Marketing is:**
- (Select the correct answer)

A. Telling patients about the services the provider offers

B. Telling patients about alternate treatment options

C. Selling patient information to a drug company

D. Giving patients free samples (face to face)

E. Getting the clients authorization to give their information to a third party.

Introduction to Security

- What is the HIPAA Security Rule?
- Are Computer threats real?
- 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.

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. 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**
April 8, 2008	**WellPoint (Indianapolis, IN)**	**Personal information that may have included Social Security numbers and pharmacy or medical data for customers in several states was exposed online over the past year.**	**128,000**
April 8, 2008	**WellCare Health Plans Inc. (Atlanta, GA)**	**Private records of members of health insurance programs for the poor or working poor were accidentally made available on the Internet for several days. Those whose data was made available on the Internet included members of Medicaid, the federal health program for the poor, and PeachCare for Kids, a federal-state insurance plan for children of the working poor. About 10,500 members' Social Security numbers may have been viewed by unauthorized people on the Internet, all members of Medicaid or PeachCare. There is a possibility that an initial 59,000 members may have had some personal information made accessible.**	**71,000**

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

www.privacyrights.org

- From January 2005 to July 29, 2008

- 234,467,328 total number of records containing sensitive personal information involved in security breaches in the U.S.

- These are only the ones reported!

Defining Security

- Having in place:
  - Controls
  - Countermeasures
  - Procedures

Common Criteria

- 1990's

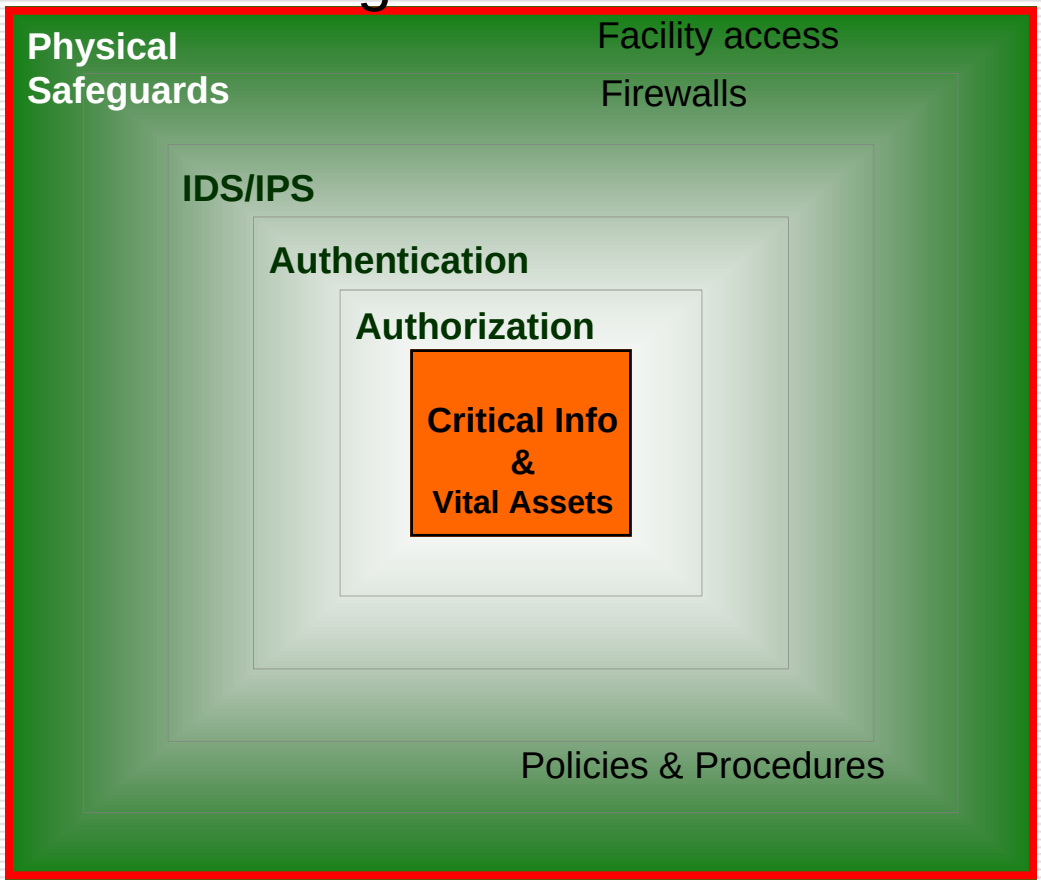
- Seven countries worked together
- France , Canada, Germany, The Netherlands, United Kingdom and United States

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).

Insuring 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

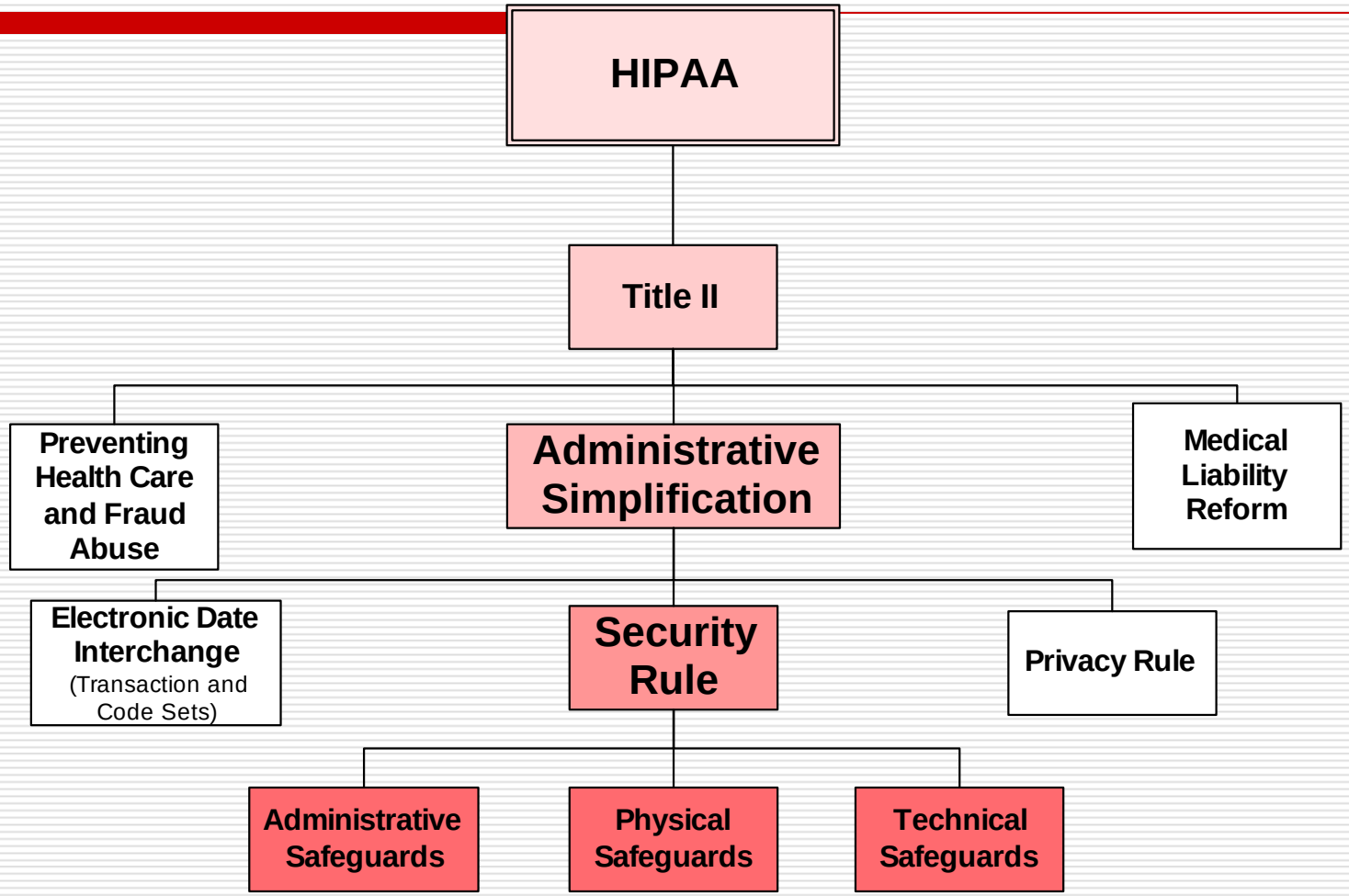
- Data Integrity – Data has not been changed inappropriately, whether by accident or deliberate, malicious intent.
- Source integrity – Did the data come from the person or business you think it did, or did it come from an imposter?
- Data or information has not been altered or destroyed in an unauthorized 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.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)



Approach and Philosophy

- Comprehensive
- Technology Neutral
- Scalable

Comprehensive

- Comprehensive. They cover all aspects of security safeguards, including:
  - Identification
  - Authentication
  - Access Control
  - Accountability and Non-Repudiation
  - Integrity
  - Communications
  - Administration

Technology Neutral

- Standards can be implemented using a broad range of off-the-shelf and user-developed technologies and security solutions

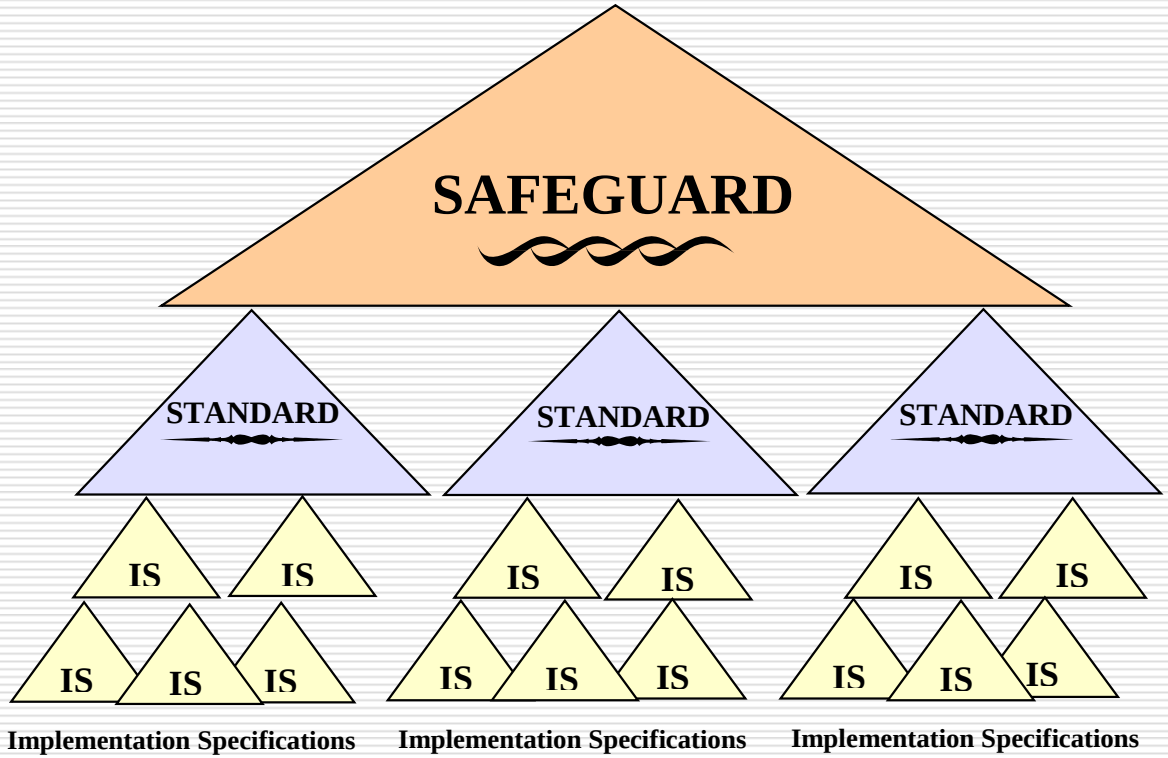
Scaleable

- The goals of the regulations can be achieved by entities of all sizes, from single practitioners to large multinational healthcare organizations

HIPAA Security is - One Size Fits All

- The regulations explicitly recognize that very small organizations will be able to satisfy the requirements with less elaborate approaches than larger, more complex organizations.

Safeguards, Standards, and Implementation Specifications



"Required"

- "Required" Implementation Specification are mandatory if your organization is a covered entity.

"Addressable" – Option One

- 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

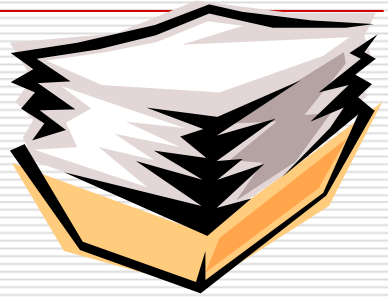
- Option Two for Addressable specification:
  - If your answer would be “No”, it doesn’t make sense for us to do this because we are too small, the exposure risk is slight, or it would be overkill…..
  - Document why it is not “reasonable and appropriate” and do an equivalent method to insure protection of EPHI.

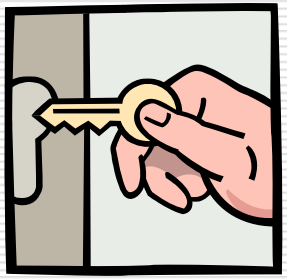
Options “Required or Addressable

- **Nothing is optional and all needs to be documented.**

APT to Comply?

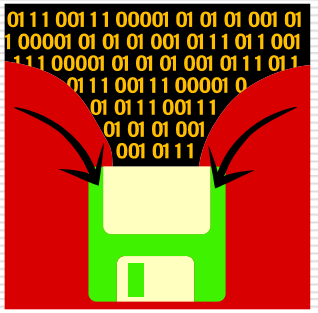
- Administrative Safeguards



- 

- Physical Safeguards

- Technical Safeguards



Three HIPAA Security Domains

Security Standards

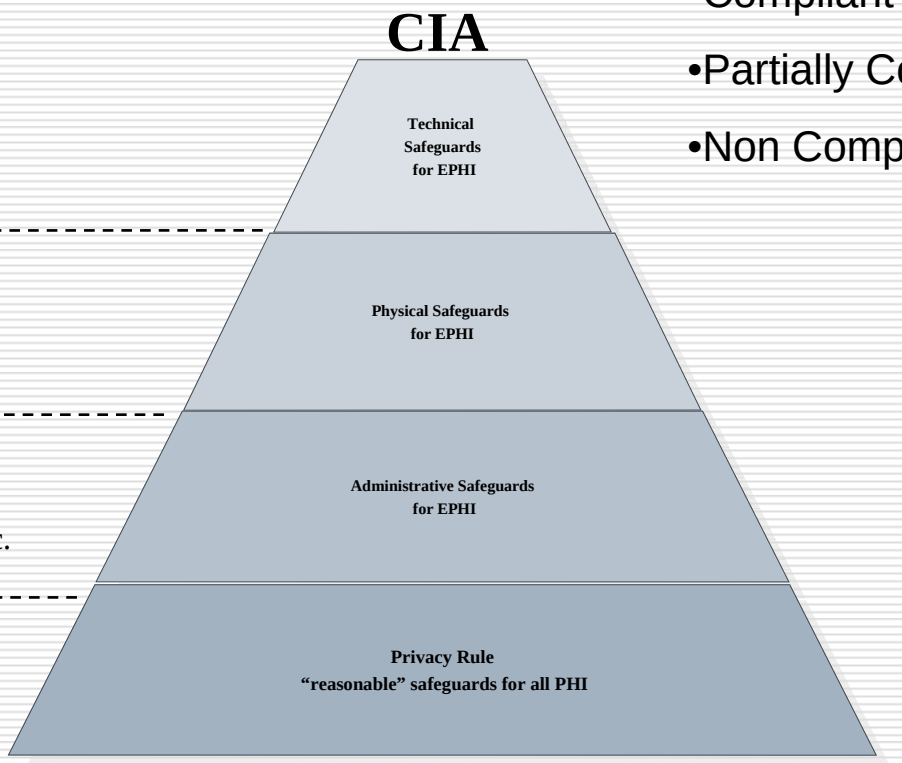
3 options

- Compliant
- Partially Compliant
- Non Compliant

- 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



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

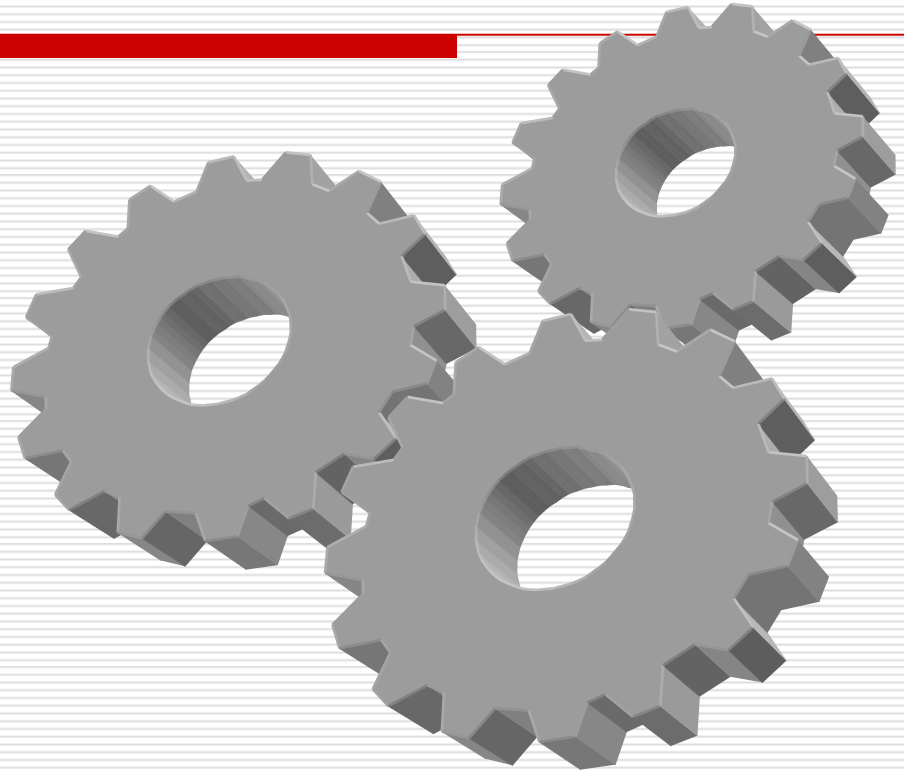
Physical safeguards address security requirements

- 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



HIPAA ACADEMY™
HIPAAacademy.Net

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

Assigned Security Responsibility

- Requires covered entities to identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity

Security Officer

- Required by the HIPAA Security Rule
- Manage and supervise the use of security measures to protect data
- Supervise personnel in relation to the protection of data

Security Officer objectives

- Documenting the information security policies and procedures instituted by the organization's Information Security Committee
- Implementing the organization's information security policies and procedures
- Coordinating the activities of the Information Security Committee
- Providing direct information security training to all employees, contractors, alliances, and other third parties
- Monitoring compliance with the organization's information security policies and procedures among employees, contractors, alliances, and other third parties, and referring problems to appropriate department managers or administrators

Security Officer objectives, continued

- Monitoring internal control systems to ensure that appropriate information access levels and security clearances are maintained
- Performing information security risk assessments and serving as the internal auditor for information security processes
- Preparing the organization's disaster recovery and business continuity plans for information systems
- Serving as an internal information security consultant to the organization
- Monitoring advancements in information security technologies

Security Officer objectives - continued

- Monitoring changes in legislation and accreditation standards that affect information security
- Initiating, facilitating, and promoting activities to foster information security awareness within the organization
- Serving as the information security liaison for users of clinical, administrative, and behavioral systems
- Reviewing all system-related information security plans throughout the organization's network, and acting as liaison to the Information Systems Department

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

Business Associates

- Are permitted to:
  - Create, Receive, Maintain or Transmit ePHI
- If:
  - Assurances that BA is protecting ePHI as the CE would.

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

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

Physical Safeguards are most aligned with the Privacy Rule

Concepts around directing visitors away from areas where there are Patients or medical records.

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

- requires covered entities to implement policies and procedures that specify
  - the proper functions to be performed
  - the manner in which those functions are to be performed
  - the physical attributes of the surroundings of a specific workstation
  - class of workstation that can access electronic protected health information.

Workstation Security

- requires covered entities to implement physical safeguards for all workstations that access electronic protected health information, 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

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*

Audit Controls

- requires covered entities to implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

Integrity Controls

- requires covered entities to implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

Person or Entity Authentication standard

- *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?*

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*

Technology: Biometrics

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

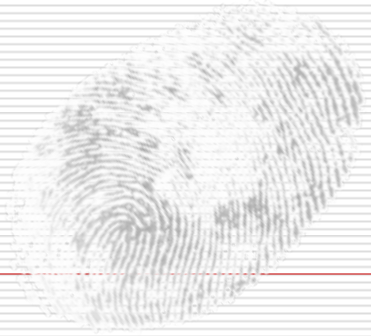
- *Examples:*
  - *Fingerprints*
  - *Facial recognition*
  - *Retina scanning*
  - *Iris scanning*
  - *Hand geometry*
  - *Voice patterns*
  - *Bio Password*

Biometric Technology

- 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	A
	Encryption	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)

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

Group Health Plans

- **The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to:**

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 group health plan;
2. Ensure that the adequate separation required is supported by reasonable and appropriate security measures;
3. Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and
4. Report to the group health plan any security incident of which it becomes aware.

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 of this subpart. A covered entity may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.

Documentation

- A covered entity must maintain the policies and procedures implemented to comply with this subpart 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

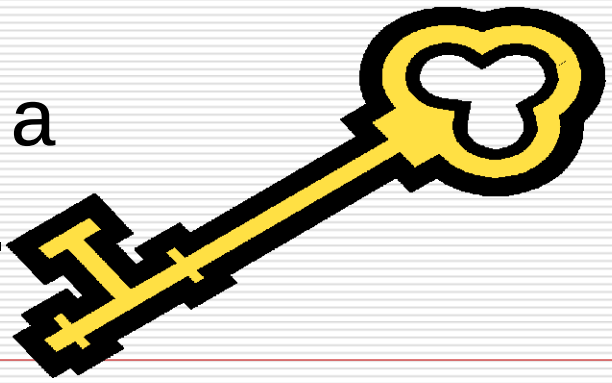
- Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Some non-technical explanations

To some technical solutions

Encryption and Decryption

- Roots found in the science of Cryptography. (In Greek, *kryptos* means hidden)
- Looking to hide the meaning of the message, not the message itself.
- Uses algorithm techniques, such as cipher substitution.
- Decryption done with a
- key (a “codebook”).



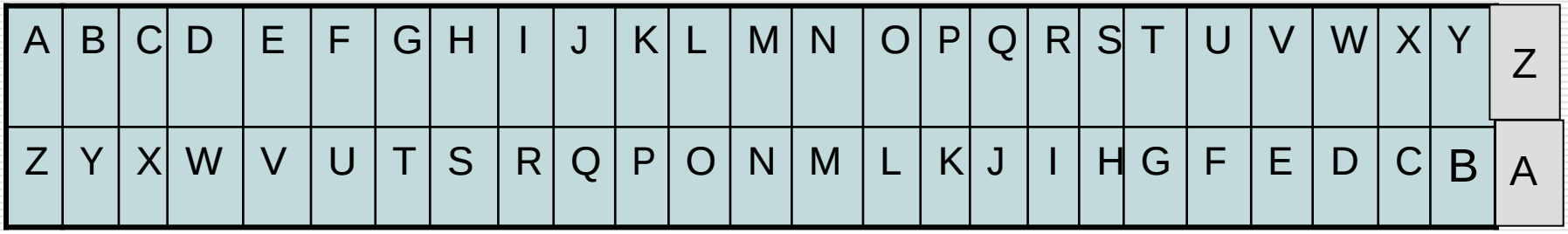
Here is an encrypted message

- OLIMZ
- RH
- SZKKB

Symmetrical and Asymmetrical

- Cipher substitution algorithms use symmetrical “keys”. (Each side uses the same method to code and decode).
- Public-key encryption the “key” is distributed freely for coding purposes.
- A Private-key is kept secure by the person wishing to unencrypt (decode) the message.

Here is the key



HERE IS THE DECRYPTED MESSAGE

- O = L
- L = O
- I = R
- M =N
- Z = A

- R = I
- H= S

- S= H
- Z= A
- K= P
- K= P
- B= Y

In Summary

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

Check Your Knowledge

- The three safeguards that for the acronym APT are:
- (Select the correct one)

A. Applications, Policies and Training
B. Administrative, Physical and Technical
C. Additional Policy Team
D. Access, Procedures and Technology

Check Your Knowledge

A. The Implementation Specifications found under the Standard “Access Control” of Technical Safeguard are:

B. (Select all of the correct answers)

C. Unique User Identification

D. Emergency Access Procedure

E. Isolate the Clearinghouse function

F. Automatic Logoff

G. Encryption and Decryption

Check Your Knowledge

A. There are two directives for complying with the Implementation Specifications none are optional they are either:

B. (Select the correct answer)

C. Unique or Similar
D. Required or Addressable
E. Automatic or Manual
F. Encryption or Decryption

Check Your Knowledge

A. The HIPAA Security Rule is a business plan to secure or networks and infrastructure to protect:

B. (Select the correct answer)

C. Healthcare Providers
D. Covered Entities
E. All patient information
F. Electronic Protected Health Information
G. All electronic medical information

Questions

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

www.ecfirst.com

www.hipaaacademy.net

HIPAA Academy
HIPAAacademy.Net