CONFIDENTIALITY COALITION

HIPAA 101

What you need to know about health information privacy and security

July 21, 2016

Tina Olson Grande
Chair, Confidentiality Coalition

CONFIDENTIALITY COALITION

Membership

Aetna
America's Health Insurance Plans
American Hospital Association
American Pharmacists Association
American Society for Radiation Oncology
AmerisourceBergen
Amgen
AMN Healthcare
Anthem
Ascension
Association of American Medical Colleges
Association of Clinical Research Organizations
athenahealth
Augmedix
Baylor Scott & White Health
Bio-Reference Laboratories
Blue Cross Blue Shield Association
BlueCross BlueShield of Tennessee
Boehringer Ingelheim
C.R. Bard
Cardinal Health
Change Healthcare
Cigna
Cleveland Clinic
College of American Pathologists
Cotiviti
CVS Health
dEpid/dt Consulting Inc.
Eli Lilly and Company
Express Scripts
Federation of American Hospitals
Franciscan Missionaries of Our Lady Health System
Genetic Alliance
Golden Living
Health Information Trust Alliance
Healthcare Leadership Council
IMS Health
Indiana University Health
Intermountain Healthcare
Johnson & Johnson
Kaiser Permanente
Leidos
Marshfield Clinic Health System
Maxim Healthcare Services
Mayo Clinic
McKesson Corporation
Medical Group Management Association
Medtronic
MemorialCare Health System
Merck
MetLife
National Association of Chain Drug Stores
National Association of Psychiatric Health Systems
NewYork-Presbyterian Hospital
NorthShore University HealthSystem
Novartis Pharmaceuticals
Novo Nordisk
Owens & Minor
Pfizer
Pharmaceutical Care Management Association
Premier healthcare alliance
Privacy Analytics
Sanofi US
SCAN Health Plan
Select Medical
State Farm
Stryker
Surescripts
Takeda Pharmaceuticals
Texas Health Resources
Teladoc
TransUnion
Vizient
Walgreens
Weight Watchers International
Workgroup for Electronic Data Interchange
ZS Associates

HIPAA

Introduction to the Privacy Rule

David Bloch
Principal Legal Counsel
Medtronic

For discussion purposes only. Does not constitute legal advice

HIPAA and HITECH

Act	Health Insurance Portability and Accountability Act of 1996	Health Information Technology for Economic and Clinical Health Act
Public Law Number	104-191	111-5 Title XIII of Div. A, Title IV of Div. B
Purpose	Improve the efficiency and effectiveness of the health care system by standardizing the electronic exchange of administrative and financial information	Promote health information technology and improve privacy and security provisions of HIPAA
Key Privacy Provisions	• Addressed the privacy and security of patient records and other forms of Protected Health Information • Implemented through regulations in 45 C.F.R. Parts 160-164	• Added new audit provisions • Enhanced accountability for Business Associates • Required notification of affected individuals if a breach of unsecured Protected Health Information has occurred • Expanded enforcement to state attorneys general • Increased penalties

Who is Covered by HIPAA Regulations?

Health Care Providers

- That transmit information electronically in connection with covered transactions
  - Health care claims
  - Health plan enrollment
  - Health plan eligibility
  - First report of injury
  - Coordination of benefits

Health Plans

- HMOs
- Health insurance companies
- Medicaid & Medicare
- Group health plans, i.e., employer-sponsored health plans
- Military and veterans health care programs

Health Care Clearinghouses

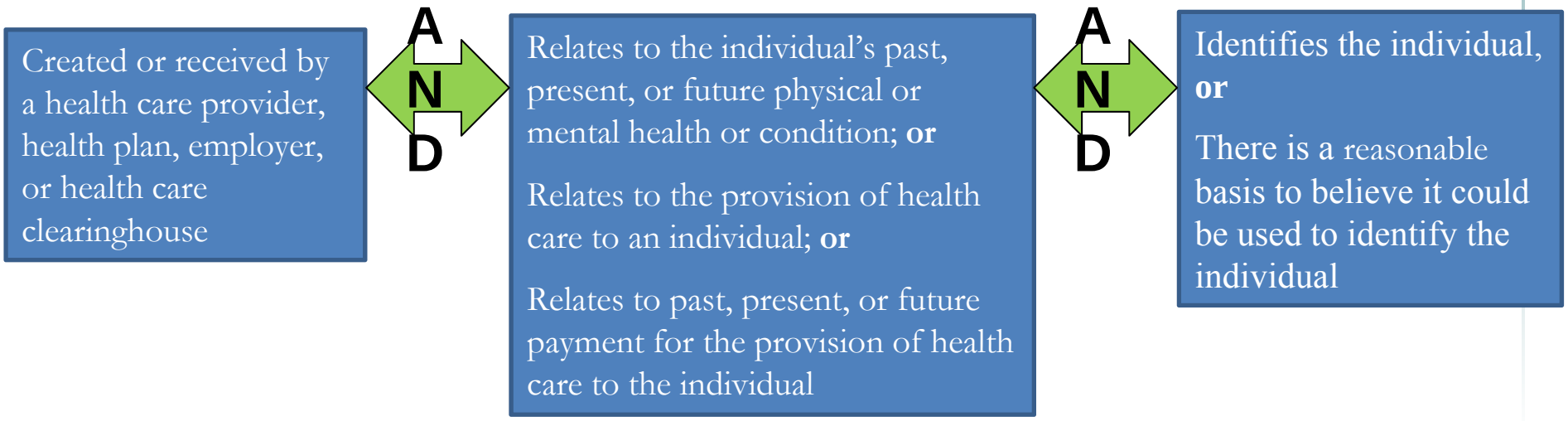
- Process or facilitate the processing of health information to/from nonstandard formats to/from standard formats
- Public or private entities that receive health information from others

Business Associates

- Perform certain functions or activities that involve the use or disclosure of PHI on behalf of the covered entity

Protected Health Information (PHI)

- Protected Health Information
  - Defined as individually identifiable health information that is transmitted by or maintained in any form or medium (oral, paper, electronic media)
  - Excludes educational records covered by FERPA, employment records held by a covered entity, and records of a person deceased for more than 50 years
- Individually Identifiable Health Information



Identifiable Information

Identifiers include:

- Names
- Geographic subdivisions smaller than a state (first 3 digits of zip code)
- Dates (except year)
- Ages over 89
- Telephone numbers
- Fax numbers
- E-mail addresses
- SSNs
- Medical record numbers
- Health plan numbers
- Account numbers
- Certification/License numbers
- License plate numbers
- Device identifiers/serial numbers
- URLs
- IP address numbers
- Biometric identifiers
- Photographic images

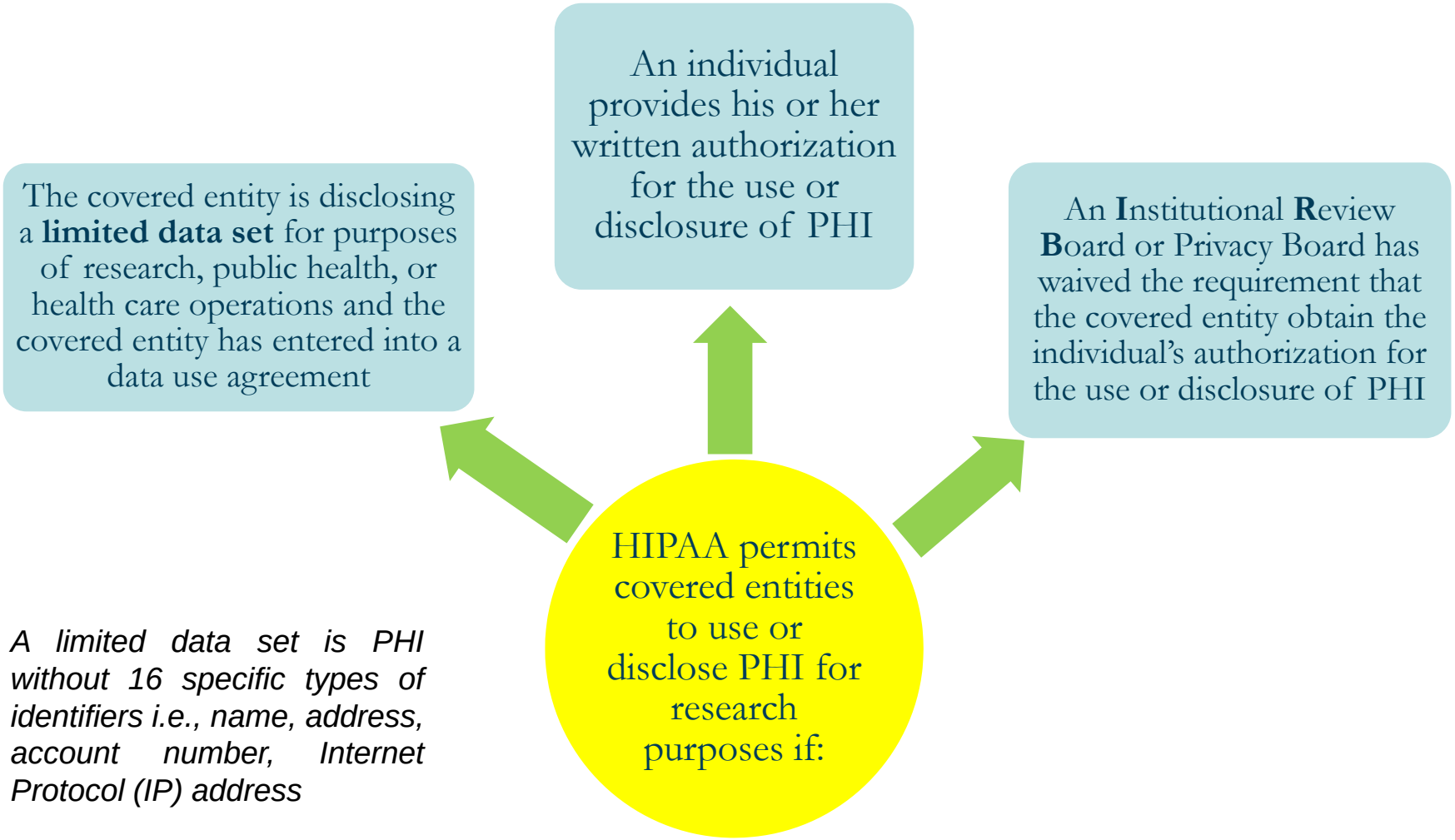
Privacy Rule Basics

- CEs may use and disclose Protected Health Information (PHI)
  - Pursuant to patient authorization
  - For Treatment of a patient
  - For Payment, and
  - For Health Care Operations, such as training employees or conducting audits

HIPAA Privacy Rule

- Other permitted disclosures without authorization:
  - "required by law"
  - to avert a serious threat to health or safety
  - for notification purposes
  - for disaster relief purposes
  - for law enforcement purposes
  - for public health activities
    - Preventing or controlling disease, injury, or disability
    - Public health surveillance, investigations, interventions
    - Birth, death, and disease reporting
    - Reports of child abuse or neglect
  - To FDA-regulated entities for reporting or other postmarket obligations
  - For research purposes

Disclosures for Research



A limited data set is PHI without 16 specific types of identifiers i.e., name, address, account number, Internet Protocol (IP) address

Access to PHI

- Access to PHI must be limited to personnel who need it to do their jobs
- Access should not be granted to outside groups

Minimum Necessary Use Requirements

- HIPAA requires covered entities and business associates, to limit use and disclosure of PHI to the minimum amount necessary to accomplish the permitted purpose
- Exception for uses related to treatment

HIPAA Obligations to Patients

- Covered entities, and their business associates, must have procedures in place to:
  - respond to patients' requests to access or amend their records
  - respond to patients' requests to limit manner in which PHI is used, even for treatment, payment or operations or how we contact them (need not agree to the request)
  - provide an accounting of all disclosures of a patient's PHI, upon request

Accounting of Disclosures

- Individuals have the right to receive an accounting of disclosures of PHI made by a covered entity in the past 6 years
- HITECH required covered entities and business associates to account for disclosure of PHI for treatment, payment, and health care operations if the disclosures are made via an electronic health record

Exceptions:

- Disclosures to carry out treatment, payment, and health care operations
- Disclosures to the individual
- Disclosures incident to a use or disclosure otherwise permitted or required
- Disclosures pursuant to an authorization
- Disclosures for national security or intelligence purposes
- Disclosures as part of a limited data set
- Disclosures to correctional institutions or law enforcement officials
- Disclosures to persons involved in the individual's care or notification purposes

Notice of Privacy Practices

- Covered Entities that have a direct treatment relationship with patients must make available to them a notice of privacy practices describing how the Covered Entity will use their information
- This is not an authorization

Privacy Rule Basics for Business Associates

- Business Associates can only use PHI for the purposes for which it was received, i.e., to perform the contracted services
  - Limited exceptions for compliance with law, product safety and performance analysis, and limited activities necessary for administration (e.g., audits)
- Business Associates may not use PHI for:
  - Marketing
  - Fundraising
  - In exchange for remuneration

The Privacy Rule's Limited Reach

The Privacy Rule does not restrict uses and disclosures of:

- Health and wellness mobile apps that are not created by covered entities or business associates (for example, most step and calorie counters)
- Consumer health information that is not PHI
- Employment records (sick leave, fitness for duty)
- Records of persons deceased for 50+ years
- Education records (Family Educational Rights and Privacy Act - FERPA)
- De-identified information
  - Does not identify an individual
  - No reasonable basis to believe that the information could be used to identify an individual from de-identified information

Major Omnibus Rule Provisions

- Mandated new provisions in Business Associate Agreements and made business associates directly liable for HIPAA/HITECH compliance
- Strengthened limits on the use and disclosure of PHI for marketing and fundraising purposes
- Expanded individual rights to receive electronic copies of PHI
- Allowed individuals to restrict disclosures to a health plan if they pay out of pocket, in full, for treatment
- Facilitated disclosures of proof of a child's immunization to schools
- Required revisions to a covered entity's Notice of Privacy Practices
- Compliance with the new rule was required by September 23, 2013 or September 22, 2014

How is HIPAA Related to Other Laws?

- HIPAA preempts state laws that are contrary to HIPAA *unless*:
  - The HHS Secretary makes a determination that the law is necessary for certain purposes, such as the prevention of fraud and abuse;
  - The state law is more stringent than HIPAA's Privacy Rule;
  - The state law provides for the reporting of disease or injury, child abuse, birth, death, or the conduct of public health activities; or
  - The state law requires a health plan to report or provide access to information for audit, program monitoring, licensure, or other purposes

How is HIPAA Related to Other Laws? (continued)

- HIPAA does not overrule more restrictive federal law and needs to be understood in context with a number of other federal laws, including:
  - Federal Privacy Act of 1974
  - Genetic Information Nondiscrimination Act of 2008 (GINA)
  - Americans with Disabilities Act
  - Federal confidentiality laws and regulations for substance abuse patient records
  - Public Health Service Act, section 543 (42 U.S.C. § 290dd-2); 42 C.F.R. Part 2
- Proposals for the consumer privacy bill of rights incorporate HIPAA by reference

How are HIPAA and HITECH Enforced?

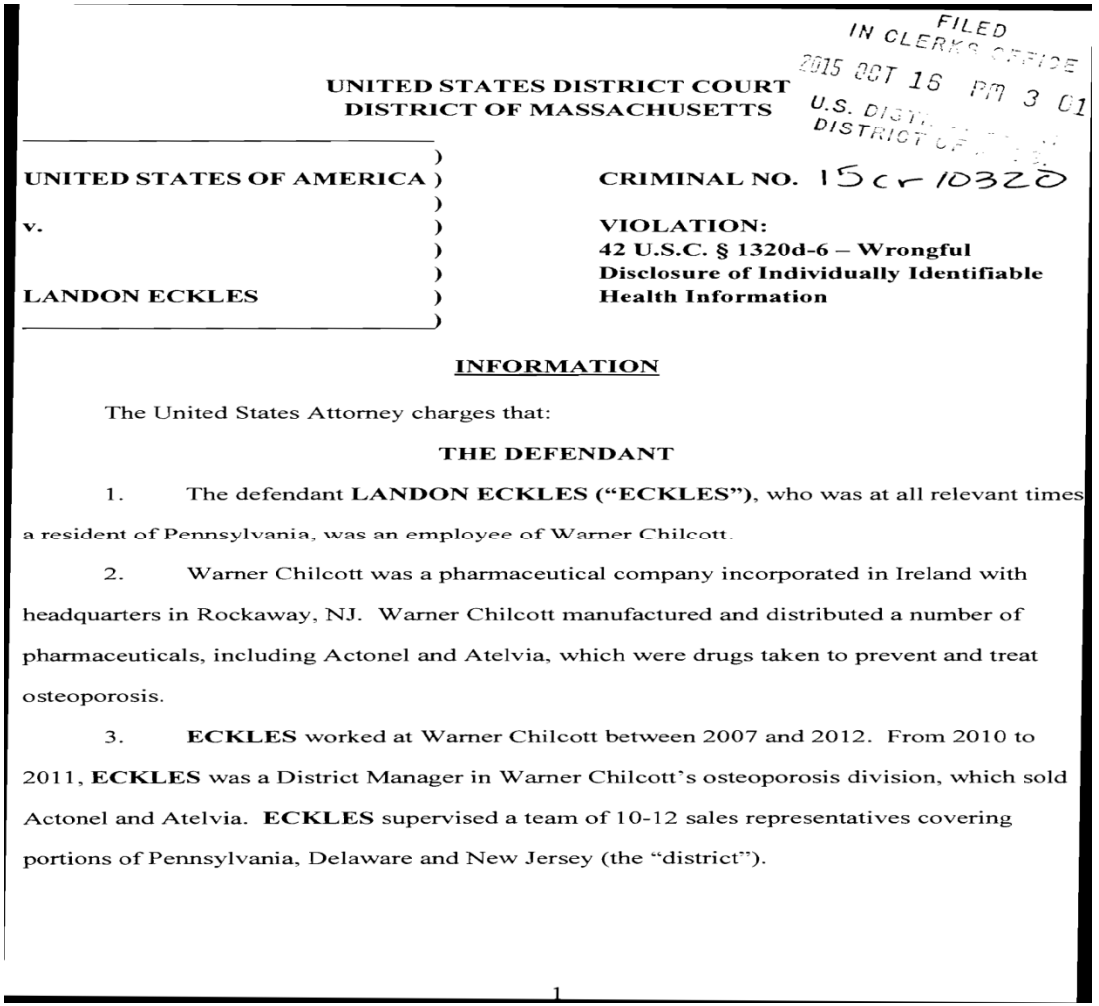
- Enforced by HHS and the US Department of Justice
  - Individuals may face civil and/or criminal penalties for HIPAA violations
  - Covered entities and business associates may face large fines for HIPAA violations
    - Up to $1.5 million for all identical violations in a calendar year

- HITECH required HHS to perform periodic audits of covered entities and business associates
  - Any covered entity or business associate can be audited
  - Audits review compliance with the HIPAA Privacy, Security, and Breach rules
- HITECH permitted state Attorneys General to bring civil actions on behalf of state residents
- No federal private right of action for individuals

Privacy Enforcement Activity in 2016

- HHS Office of Civil Rights has stepped up enforcement:
  - $2.2 million settlement with a hospital for allowing filming of a documentary in the ER
  - $750,000 settlement with Raleigh Orthopedic Clinic for not having HIPAA business associate agreements in place with contractors
  - $3.9 million settlement with Feinstein Institute of Medical Research for not having proper privacy and security controls in place
  - $1.5 million settlement with North Memorial Health Care System for disclosing patient information to a contractor without a HIPAA business associate agreement

Privacy Enforcement Activity in 2016



FILED
IN CLERK'S OFFICE
2015 OCT 16 PM 3 01
U.S. DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

LANDON ECKLES

CRIMINAL NO. 15cr10320

VIOLATION:
42 U.S.C. § 1320d-6 – Wrongful Disclosure of Individually Identifiable Health Information

INFORMATION

The United States Attorney charges that:

THE DEFENDANT

1. The defendant **LANDON ECKLES ("ECKLES")**, who was at all relevant times a resident of Pennsylvania, was an employee of Warner Chilcott.

2. Warner Chilcott was a pharmaceutical company incorporated in Ireland with headquarters in Rockaway, NJ. Warner Chilcott manufactured and distributed a number of pharmaceuticals, including Actonel and Atelvia, which were drugs taken to prevent and treat osteoporosis.

3. **ECKLES** worked at Warner Chilcott between 2007 and 2012. From 2010 to 2011, **ECKLES** was a District Manager in Warner Chilcott's osteoporosis division, which sold Actonel and Atelvia. **ECKLES** supervised a team of 10-12 sales representatives covering portions of Pennsylvania, Delaware and New Jersey (the "district").

1

OCR Audits

- In 2011 OCR conducted audits of 115 covered entities
  - Did not treat it as an enforcement exercise.
  - Stated that only 11% of auditees had no findings
- OCR is currently conducting another round of audits, of both covered entities and business associates.
  - Estimate 200 desk audits will be done. Approximately 50 onsite reviews.

CONFIDENTIALITY COALITION

Confidentiality Coalition: HIPAA 101

HIPAA Security Rule

Kimberly S. Gray, J.D., CIPP/US

Global Chief Privacy Officer, IMS Health

July 21, 2016 – Rayburn Office Building, Washington DC

imshealth™
INTELLIGENCE APPLIED.

Security as a legal and compliance issue

Uptick in concerns

- Security is now a separate legal requirement in the US – connected to privacy but with different rules and issues
- Security is a top issue today, with almost daily news stories about security breaches and a tie to identity theft
- Security has moved from a business-driven "best practice" to a legal requirement in all industries
- Security problems are generating most relevant enforcement actions and litigation

HIPAA Statute

Each Covered Entity who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical and physical safeguards:

- To ensure the **integrity** and **confidentiality** of the information;
- To protect against any *reasonably anticipated* threats or hazards to the security or integrity of the information; and unauthorized uses or disclosures of the information; and
- Otherwise to ensure compliance with this part by the officers and employees of such Covered Entity.

HIPAA Statute

Requires HHS Secretary to prepare rule addressing:

- Technical capabilities of record systems used to maintain health information;
- The costs of security measures;
- The need for training persons who have access to health information;
- The value of audit trails in computerized record systems; and
- The needs and capabilities of small health care providers and rural health care providers.

HIPAA Security Rule

Specifically, covered entities must:

- Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
- Identify and protect against reasonably anticipated threats to the security or integrity of the information;
- Protect against reasonably anticipated, impermissible uses or disclosures; and
- Ensure compliance by their workforce.

HIPAA Security Rule (scope)

- All electronic protected health information (EPHI)
- In motion AND at rest
- All covered entities (Now all business associates as well)
- Privacy Rule is all PHI

Security Standards

- *Flexible, scalable* - Permits standards to be interpreted and implemented appropriately from the smallest provider to the largest plan
- *Comprehensive* - Cover all aspects of security-behavioral as well as technical
- *Technology neutral* - Can utilize future technology advances in this fast-changing field

HIPAA Security Rule

"The most appropriate means of compliance for any covered entity can only be determined by that entity assessing its own risks and deciding upon the measures that would best mitigate those risks"

- Does not imply that organizations are given complete discretion to make their own rules
- Organizations determine their own technology choices to mitigate their risks

Covered entities must assess if an implementation specification is reasonable and appropriate based upon factors such as:

- Risk analysis and mitigation strategy
- Current security controls in place
- Costs of implementation

Key concept: "reasonable and appropriate"

Cost is not meant to free covered entities from their security responsibilities

HIPAA Security Rule

Security Official

Responsibility must rest with one individual to ensure accountability:

"More than one individual may be given specific security responsibilities, especially within a large organization, but a single individual must be designated as having the overall final responsibility for the security of the entity's electronic protected health information."

HIPAA Security Rule

Most of the Security Rule describes an appropriate "process" that covered entities must go through in evaluating security options, broken down into technical, physical and administrative safeguards.

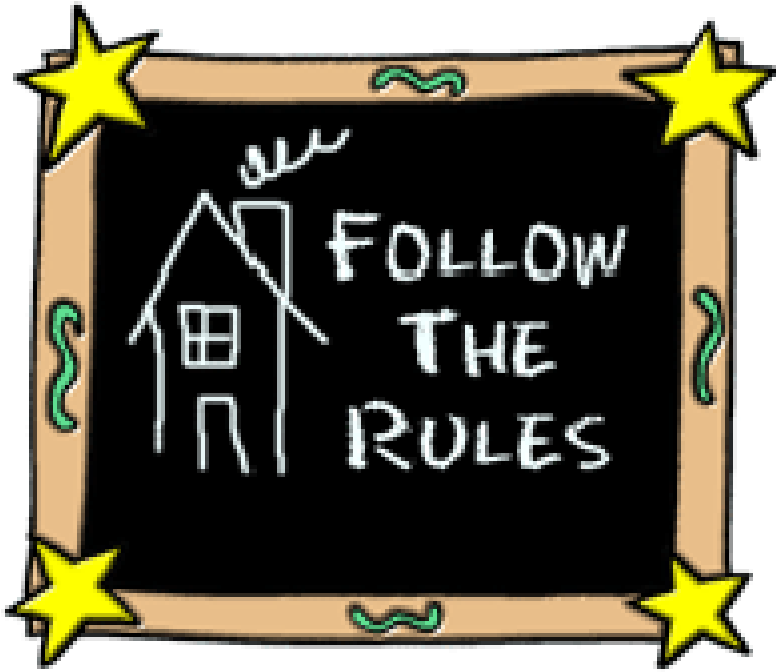
"Risk analysis" means to Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity

"Risk management" involves an obligation to:
Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule.

Administrative safeguards

Examples

- Sanction policy
- Assigned responsibility for security activities
- Security awareness and training
- Contingency planning
- "Security incident" procedures (a "security incident" is an "attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system")



Technical safeguards

Examples

- Access controls (such as unique user identification automatic log-off and emergency access procedures)
- Audit controls integrity (protection against improper alteration or destruction of PHI)
- Person/entity authentication and transmission security

Physical safeguards

Examples

- Facility access controls (limiting physical access to information systems)
- Workstation use policies
- Workstation security, and
- Device and media controls (such as procedures for disposal of computer hardware in light of recent reports of privacy violations involving discarded computers that still retained PHI)

Security Breaches

- Information security practices are designed to reduce the risks of privacy and security breaches
- These rules have been built up in connection with specific laws (HIPAA, GLB for financial services) or general "best practice" requirements (FTC)
- An entirely separate set of laws has built up over requirements to notify individuals in the event of a privacy or security breach
- State laws now exist in nearly all states
- Federal law/rule for health care industry from the HIPAA/HITECH statute

HIPAA/HITECH Breach

- Section 13402 of the Act requires HIPAA covered entities to notify affected individuals, and requires business associates to notify covered entities, following the discovery of a breach of unsecured protected health information.
- Breach means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.
- Must perform a "risk assessment" to determine if there is a low probability of a "compromise" of the PHI. If the risk assessment reveals a low probability of compromise, notification is not required.
- Covered entity can provide notice without a risk assessment.

Breach reporting

Elements of the breach risk assessment

- The nature and extent of the protected health information involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Cyberthreats and HIPAA security

Do the basics! And monitor threats…

- Comply with HIPAA Security Rule requirements
- Security controls in place
- Assess controls regularly
- Monitor threats
- Adjust controls accordingly

Summary: HIPAA Security Rule

- Protects electronic PHI
- Requires the adoption of administrative, physical, technical safeguards
- Flexibility of approach
- Requires risk analysis and risk management, along with specific list of standards

CONFIDENTIALITY COALITION

Questions?

Tina Olson Grande
Chair, Confidentiality Coalition
750 9th Street, NW, Suite 500
Washington, DC 20001
tgrande@hlc.org

www.confidentialitycoalition.org