CONFIDENTIALITY COALITION

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

CONFIDENTIALITY COALITION

Who is Covered by HIPAA Regulations?

Health Care Providers

- That transmit information 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

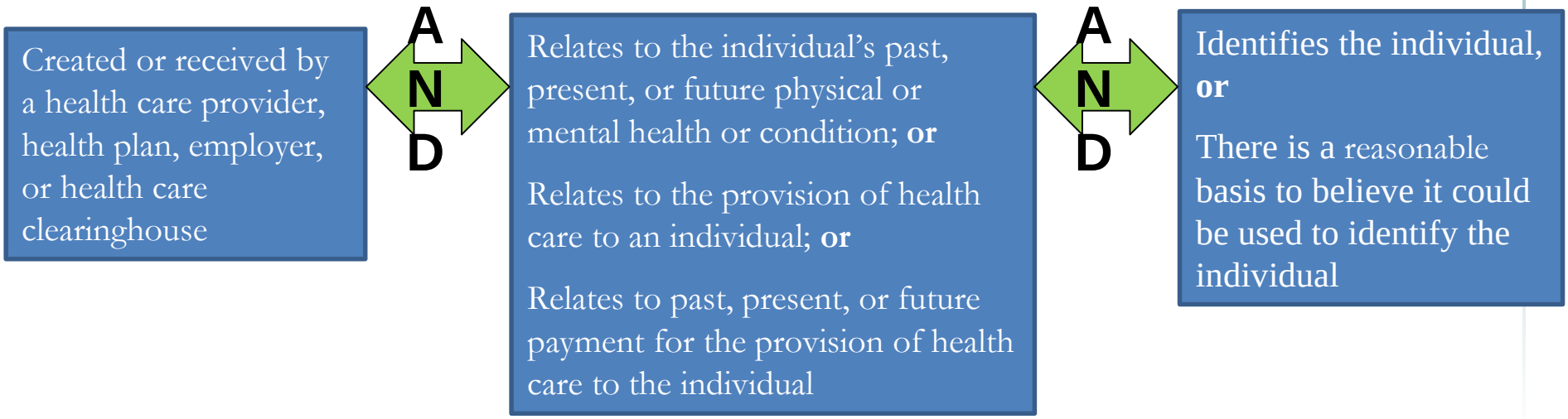
- Process or facilitate the processing of health information to/from nonstandard formats to/from standard formats
- Public or private entities that receive health information from others

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



Examples of Identifying Information

- Demographic information
  - Name
  - Residential Address
  - Phone #, fax # or an email address
- Identifying features or numbers
  - Social Security or Medicaid card numbers
  - Certificate or license numbers
  - License plate numbers
  - Device identifiers and serial numbers
  - Full-face photographic images, comparable images
  - Biometric identifiers, including finger and voice prints
- Dates directly related to an individual
  - Birth, marriage, death, admission, discharge, claim
- Exception: Persons deceased for more than 50 years

HIPAA Privacy Rule

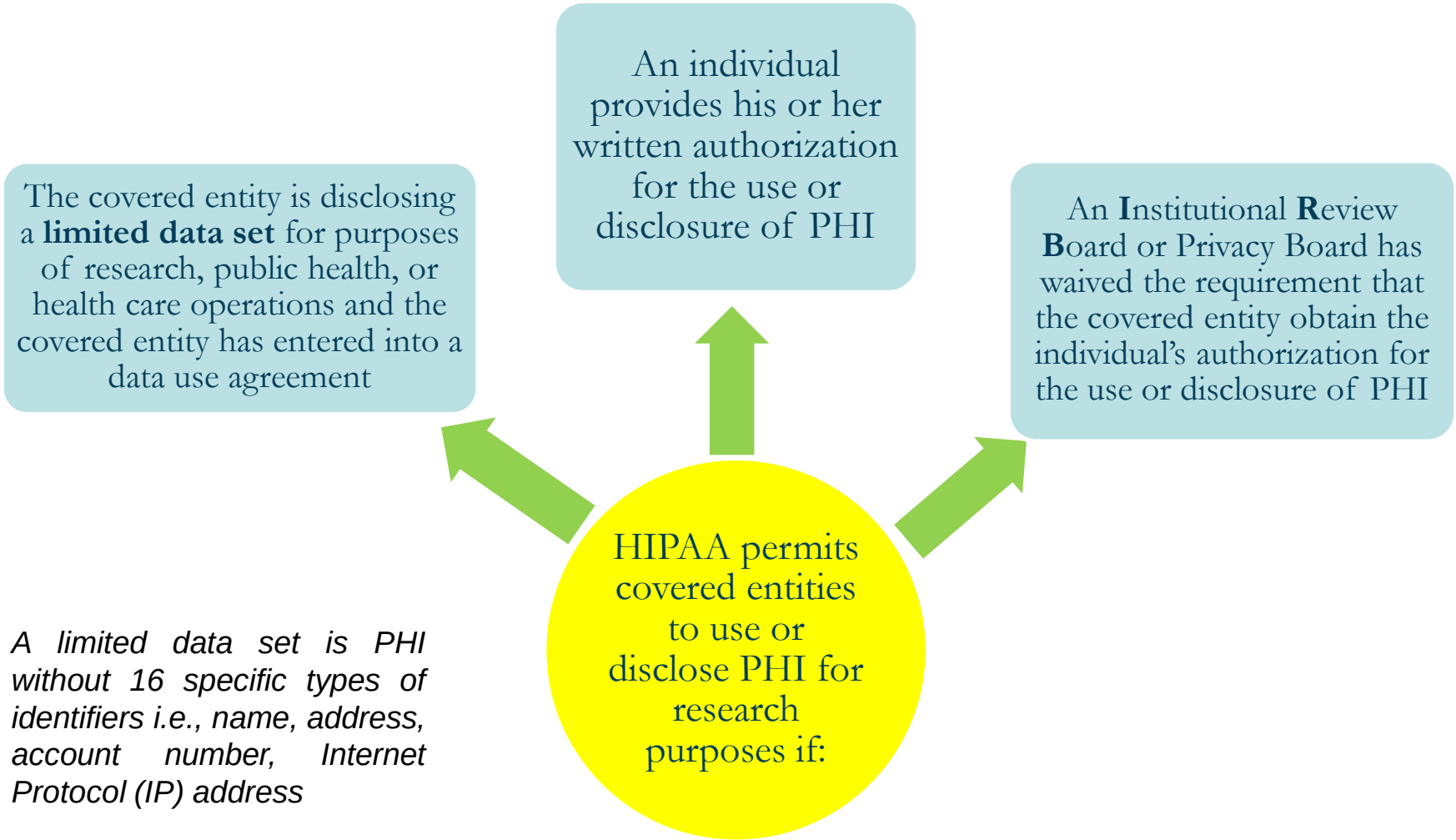
- Limits the use and disclosure of PHI by covered entities and business associates
- Use and disclosure require an individual's authorization or the opportunity to object unless:
  - Disclosure is to the individual
  - Use or disclosure is for treatment, payment, or health care operations
  - Use or disclosure is for one of the specified exceptions and in compliance with the specific rules for each exception:
    - uses and disclosures "required by law"
    - uses and disclosures to avert a serious threat to health or safety
    - uses and disclosures for notification purposes
    - disclosures for disaster relief purposes
    - disclosures for law enforcement purposes
    - uses and disclosures for public health activities
    - uses and disclosures for research purposes

Disclosures for Public Health Activities

HIPAA permits covered entities to use or disclose PHI for public health purposes:

- Public health authorities authorized by law to collect or receive PHI to perform public health activities
  - Preventing or controlling disease, injury, or disability
  - Public health surveillance, investigations, interventions
    - Foodborne illnesses, tuberculosis, HIV
  - Birth, death, and disease reporting
  - Reports of child abuse or neglect
- Food and Drug Administration
  - Adverse event reports related to drugs and medical devices
  - Reports that may lead to product recalls of other FDA-regulated products, such as food and dietary supplements

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

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
- HHS proposed rule to amend the accounting for disclosures provision is still pending

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

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

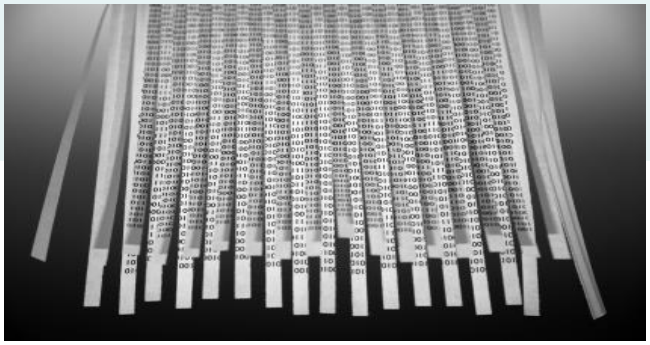
CONFIDENTIALITY COALITION

Breach Notification

- The breach rule applies to covered entities and business associates as of September 23, 2009
- A **breach** is the
  - acquisition, access, use, or disclosure of **unsecured** PHI
  - in a manner not permitted by the HIPAA Privacy Rule (i.e., unauthorized)
  - which compromises the security or privacy of PHI
- Required notifications may include:
  - Individuals
  - HHS Secretary
  - Media
  - State law enforcement or other state entities
    - Almost every state has its own data breach notification law

When is PHI Unsecured for Purposes of a Breach?

Unsecured PHI	Secured PHI
PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified in a HHS guidance document • *i.e.*, PHI can be accessed by unauthorized persons	PHI meets the encryption or destruction standards in the HHS guidance document • Encryption for data in motion and at rest • Based on National Institute of Standards and Technology (NIST) publications • Cross-cut shredding



Breach Notification

- An acquisition, access, use, or disclosure of unsecured PHI in an unauthorized manner is presumed to be a breach
- The covered entity or business associate may demonstrate in a risk assessment that there is a low probability that the PHI has been compromised, based on four factors:
  1. Nature and extent of the PHI involved, including types of identifiers and likelihood of reidentification;
  2. Unauthorized person who used the PHI or to whom the disclosure was made;
  3. Whether the PHI was actually acquired or viewed; and
  4. Extent to which the risk to PHI has been mitigated

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 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

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