CONFIDENTIALITY COALITION

Our Presentation

- Provide some basic background on the development and scope of the HIPAA Privacy and Security Rules
- Identify some of the key developments from the new HITECH rules that went into effect in 2013
- Identify some additional "hot topics" for health care privacy and security

CONFIDENTIALITY COALITION

HIPAA History

- The HIPAA Statute was passed in 1996
- Health Insurance Portability and Accountability Act
- Focused on "portability" of health care coverage
- Additional elements added to statute, including "administrative simplification"

CONFIDENTIALITY COALITION

HIPAA History

- Combination of administrative simplification (including standardized electronic claims) and portability led to development of HIPAA Privacy (2003) and Security (2005) Rules
- Applied to "covered entities" (e.g., health care providers, health plans and clearinghouses) and now (as of 2013) business associates (service providers to covered entities)

CONFIDENTIALITY COALITION

HIPAA History

- Congress amended HIPAA rules in the HITECH Act (Health Information Technology for Economic and Clinical Health Act of 2009) (part of economic stimulus legislation)
- Provided incentives to implement electronic health records and then modified privacy/security rules

CONFIDENTIALITY COALITION

The Omnibus HIPAA Regulation

- Final rules implementing HITECH changes published in the Federal Register on January 25, 2013
- Effective on March 26, 2013
- Required compliance by September 23, 2013
- Includes changes to privacy and security rules, enforcement, breach notification rule and GINA provisions

CONFIDENTIALITY COALITION

Key HIPAA Components

- Privacy Rule
- Security Rule
- Breach Notification
- Enforcement

CONFIDENTIALITY COALITION

The HIPAA Privacy Rule

- Sets a national baseline standard on privacy and security for the health care industry
- Creates general principles for the use and disclosure of "protected health information"
- Creates various individual rights, including amendment, access and accounting
- Provides privacy notices
- Requires training, policies and procedures

CONFIDENTIALITY COALITION

HIPAA Applies to "PHI"

- "Protected Health Information" or "PHI"
- Individually identifiable health information created or received by or on behalf of a covered entity
- Identifies an individual (or could be used to reasonably identify an individual)
- Relates to an individual's past, present, future health care treatment or payment for health care
- Not an overall medical privacy rule

CONFIDENTIALITY COALITION

Uses and Disclosures

- HIPAA approach – uses and disclosures are made with "presumed" patient consent (for Treatment, Payment and Health Care Operations – TPO - purposes)
- Disclosures can be made for certain "public purposes" without the need for patient consent or in defined situations
- Otherwise, patient "authorization" is needed.

CONFIDENTIALITY COALITION

Public Policy Disclosures

- Specific identified purposes for disclosure.
- Required by Law
- Public Health activities
- Litigation and health care Oversight
- Law Enforcement
- Research

CONFIDENTIALITY COALITION

Additional principles

- Disclosures generally must be limited to the minimum amount of information necessary to accomplish the purpose of the disclosure
- Contracts required between covered entities and their "business associates"
- Significant restrictions on "marketing" activities

CONFIDENTIALITY COALITION

The 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

Breach Notification

- HITECH law and new HIPAA Rules impose standards for notification of individuals in the event of a security breach
- Additional notification to media and/or HHS in certain circumstances

CONFIDENTIALITY COALITION

The Breach Basics

- A breach is the acquisition, access, use, or disclosure of protected health information in a manner not permitted under [HIPAA] which compromises the security or privacy of the protected health information.

CONFIDENTIALITY COALITION

Notification Standard

- Notification is required to the affected individuals unless the covered entity "demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment."

CONFIDENTIALITY COALITION

The 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.

CONFIDENTIALITY COALITION

Enforcement

- Primary enforcement is through HHS Office for Civil Rights (fines, penalties ($100-$1.5 million), settlements, corrective action, etc)
- Specific additional enforcement authority for State Attorneys general
- Department of Justice has criminal authority

CONFIDENTIALITY COALITION

Next Issues - Regulatory

- The HIPAA Accounting Rule
- Ongoing debate about how this rule will change, whether this is what patients want, and how much burden will be imposed
- Initial proposal from HHS has been largely withdrawn, but significant open issues remain

CONFIDENTIALITY COALITION

The FTC and Health Care

- FTC has been exploring "gaps" in the HIPAA structure – where HIPAA does not apply to medical information (e.g., mobile applications)
- FTC also has undertaken some enforcement against health care entities for security breaches – raising questions about jurisdiction.

CONFIDENTIALITY COALITION

Questions?

Tina Olson Grande
Sr. Vice President, Policy
Healthcare Leadership Council
(on behalf of the Confidentiality Coalition)
750 9th Street, NW, Suite 500
Washington, DC 20001

www.confidentialitycoalition.org