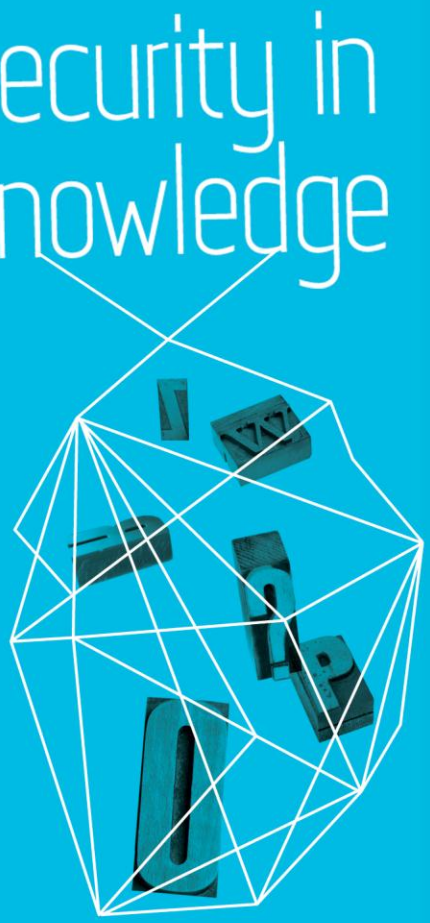
DATA BREACH LAW UPDATE
Global Trends—Legal Complexities



Moderator:

Lucy L. Thomson
Livingston PLLC

Panelists:

Thomas Smedinghoff
Edwards Wildman

Eric Hibbard
Hitachi Data Systems

Robert Thibadeau
Wave Systems

Session ID: **DSP-W23**

Session Classification: **Intermediate**

AGENDA

Data Breach Law Update: Key Developments

- State Laws
- HIPAA-HITECH
- International Laws and Directives
- International Standards

Legal Complexities and Potential Pitfalls

- Law, Technology, and Encryption

Mastering the Complexities

- Action Steps to *Prevent* A Breach

RSA CONFERENCE 2013

DATA BREACH LAW UPDATE— KEY DEVELOPMENTS

MASTERING THE LEGAL AND TECHNICAL COMPLEXITIES

How to Evaluate an Incident/ Possible Breach

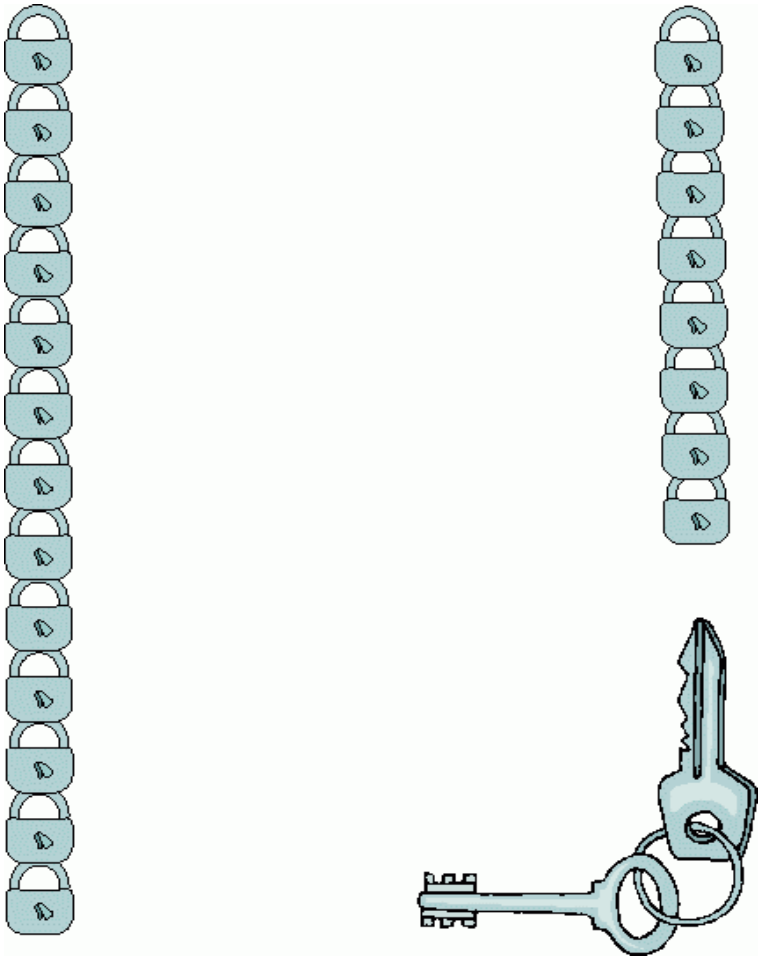
- How did the incident/ possible breach occur? Who is responsible?
- What data were affected? Know (or be able to discover) where the data resides
- Were the data involved in the incident actually encrypted?
  - Was the encryption in accordance with the definitions of "breach" and "encryption" in the applicable statute(s)?
  - What Proof-of-Encryption documentation is available?
  - Were the data compromised? Conduct a Risk Assessment
- Were the Encryption Keys Secure?

How Lawyers and the Courts Evaluate an Incident/ Possible Breach

Read and analyze the elements of each law that applies (state, federal, international)

- "Records Accessed"—What data?
- "Accessed"—Did the perpetrator view the data?
- "Unauthorized"—Was there unauthorized access to PII?
- "Acquisition"—Were the records "acquired" by the perpetrator?
- "Acquisition causes" (has or will cause) identity theft or fraud

When Is Encryption Not a Safe Harbor?



- *Encryption Keys*
  - Inadequate/inappropriate key management can result in data breaches and/or loss of data
  - If the encryption key is compromised the protection is lost
- *Security Lapses*
  - Encryption must be implemented properly
  - When information is encrypted, notification is not required; but all data must be protected

ACTION STEPS TO *PREVENT* A BREACH

Action Steps to *Prevent* a Data Breach

- Use the knowledge gained at RSA to brief your organization on current and emerging laws and encryption requirements
- Develop a comprehensive information security plan specifically designed to prevent data breaches
- Conduct a risk assessment – carefully document how the security controls selected and implemented address all risks identified
- Develop a strategy for implementing and managing encryption consistent with legal requirements; match the encryption solution to the risk; compliance-driven encryption necessitates proof-of-encryption

Action Steps to *Prevent* a Data Breach

- Develop a data retention and destruction plan so personal data is not at risk – sanitize regularly
- Secure your organization's sensitive data using appropriate encryption technology, and technical, administrative, and management controls
- Maintain up-to-date documentation of the encryption solutions implemented throughout the network to protect sensitive personal data; ensure appropriate encryption is utilized on mobile devices
- If you can't prove encryption is operational, why bother?
- Inadequate/inappropriate key management can result in data breaches and/or loss of data

ENCRYPTION DEFINITIONS

Encryption – A Safe Harbor?

>>If personal data are encrypted, individuals do not need to be notified

Almost 50% of the breach notification statutes provide *no definition of encryption whatsoever.*

They simply require notice only if the stolen data is "unencrypted" or "not encrypted"

The other 50% use *varying definitions of encryption—*

- If personal data are encrypted, individuals do not need to be notified
- An algorithmic process that renders the data unreadable or unusable
- An algorithmic process that results in a low probability of assigning meaning to the data
- A 128 bit or greater algorithmic process that results in a low probability of assigning meaning to the data
- Another method that renders data unreadable or unusable
- A method specified by a regulator

HIPAA-HITECH Update

- U.S. Department of Health and Human Services
  - Data Breach defined—

  Unauthorized acquisition, access, use or disclosure of protected health information that compromises the security and privacy of such information.

HHS Mega Final Rule, 78 FR 5566 (January 25, 2013)

Encryption in HITECH

- **HITECH**

U.S. Healthcare Law

- Requires notification in the event of a breach of "unsecured protected health information"

NIST 800-111 for data-at-rest

Requires IT Managed Full Disk Encryption Solutions

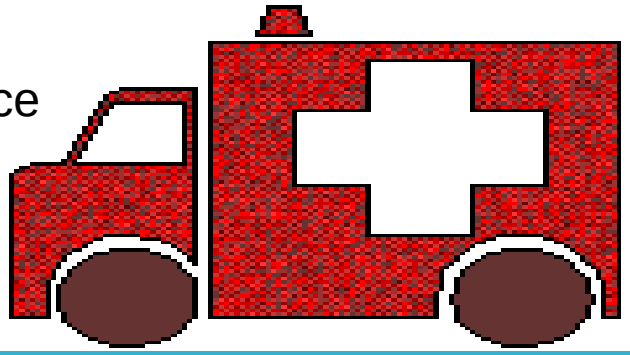
HHS HITECH April 2009 Guidance

June 2010: Now even if a contractor loses PII, you could be responsible unless he meets SP 800-111

Encryption Further Defined in HITECH

- **Electronic PHI** has been encrypted as specified in the HIPAA Security Rule by “the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key” and such confidential process or key that might enable decryption has not been breached.

HHS HITECH April 2009 Guidance

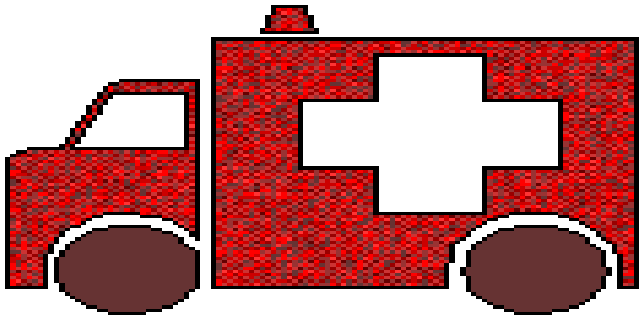


HITECH Guidance Relies on NIST

- HHS HITECH April 2009 Guidance provides:
- "**Encryption processes** identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard:

  (i) Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111, *Guide to Storage Encryption Technologies for End User Devices*."

(more)



HITECH Guidance Focuses on More NIST Standards

HHS HITECH April 2009 Guidance provides:

"(ii) Valid encryption processes for data-in-motion are those that comply, as appropriate, with:

- NIST Special Publications 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TSL) Implementations*
- 800-77, *Guide to IPsec VPNs*
- 800-113, *Guide to SSL VPNs*
- others which are Federal Information Processing Standards (FIPS) 140–2 'validated.'"

✧ **Note: NIST changed these encryption requirements –** *see* **NIST SP 800-131 (January 2010)**