

September AIM Members Forum

Security and Liability of Mobile Devices

James E. O'Connor
Baird Holm LLP

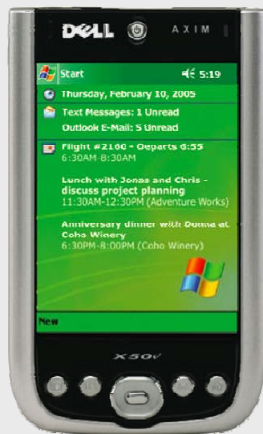
James O'Gorman
Continuum Worldwide Corporation

BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Agenda

- Need to secure portable devices
- Regulatory requirements
 - HIPAA
 - State Data Breach Notification laws
- Securing portable devices
 - Best practices
 - Tips/techniques

Portable Devices and Media



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Inherent Conflicts of Portables

- Need to have data to be useful
- Small, easy to carry, conceal, lose
- High value (relatively)

Portable Device* Data Breaches

- Calendar year 2010
 - As of September 14, 2010, a total of 97 portable device data breaches have been reported.
 - These breaches involve a minimum of 6,452,996 records.**

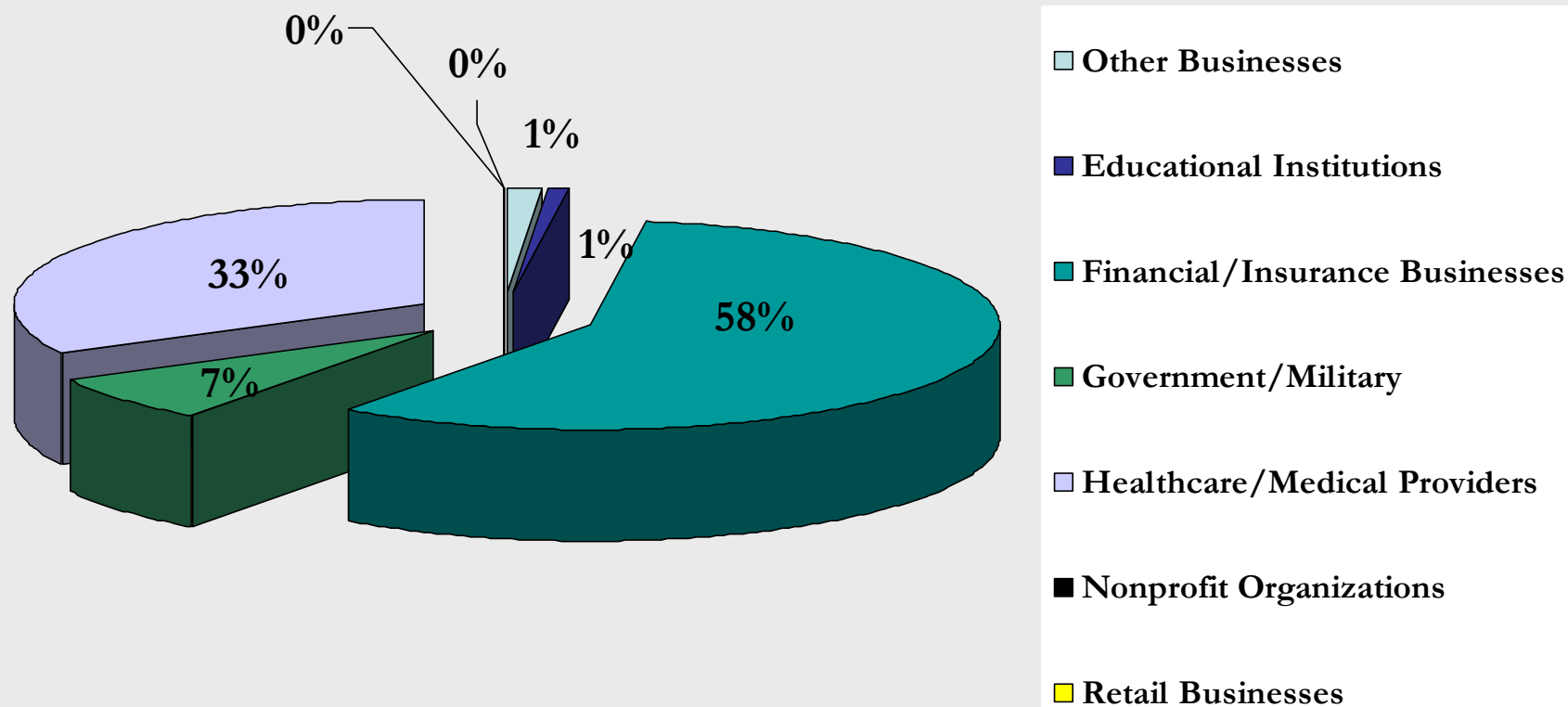
*Portable devices include laptops, PDAs, smartphones, portable memory devices, CDs, hard drives, data tapes, etc.

**Breached records that did not contain any Social Security numbers or financial information are not included in this total.

From Privacy Rights Clearinghouse (<http://www.privacyrights.org>)

BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Data Breach Breakdown by Industry*



*Breached records that did not contain any social security numbers or financial information are not included in this breakdown.

From Privacy Rights Clearinghouse (<http://www.privacyrights.org>)

Largest Breaches*

- **AvMed Health Plans** of Gainesville, FL - February 6, 2010
 - personal information including names, addresses, phone numbers, Social Security numbers, and protected health information
 - 1.1 million individuals may have been compromised
 - theft of two company laptops. It was determined that the data on one of the laptops *may not have been protected properly*.
- **Educational Credit Management Corporation** - March 26, 2010
 - guarantor of federal student loans
 - personally identifiable information including names, addresses, dates of birth, and Social Security numbers
 - 3.3 million individuals
 - theft from its headquarters involving portable media

*Breaches that did not contain any Social Security numbers or financial information are not included.

From Privacy Rights Clearinghouse (<http://www.privacyrights.org>)

Think You're Safe?

- **Cook County Health and Hospital Systems** in Chicago, IL
 - password-protected laptop with patient information including names, dates of birth, and Social Security numbers
 - stolen from a locked office in an administration building
- **Department of Pediatrics Newborn Screening Program** in Lexington, KY
 - password-protected laptop with information including patient dates of birth, names, medical record numbers , and some Social Security numbers
 - stolen from a locked private office

From Privacy Rights Clearinghouse (<http://www.privacyrights.org>)

Current State of the Law: Heart of Most Regulations

- Requirement: Reasonable and appropriate administrative, physical and technical safeguards
- Definitions:
 - System: "an interconnected set of information resources under the same direct management control that shares common functionality...includes hardware, software, information, data, applications, communications, and people."
 - Workstations: "an electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment."

(from HIPAA)

Current State of the Law

Specific Laws

- GLBA
- HIPAA/HITECH
- State Data Breach Notification Laws

What is a Breach?



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

How is Breach Defined?

HIPAA:

- The **acquisition, access, use or disclosure of protected health information** which compromises the security or privacy of the protected health information
- For purposes of this definition, **compromises the security or privacy of the protected health information** means poses a significant risk of financial, reputational, or other harm to the individual

Compromises the Security or Privacy of PHI

- "Poses a significant risk of financial, reputational or other harm to the individual"
- This standard requires some form of risk assessment in the event of a breach
- Based upon the assessment, notification may be necessary

Risk Assessment

As part of the Risk Assessment, consider:

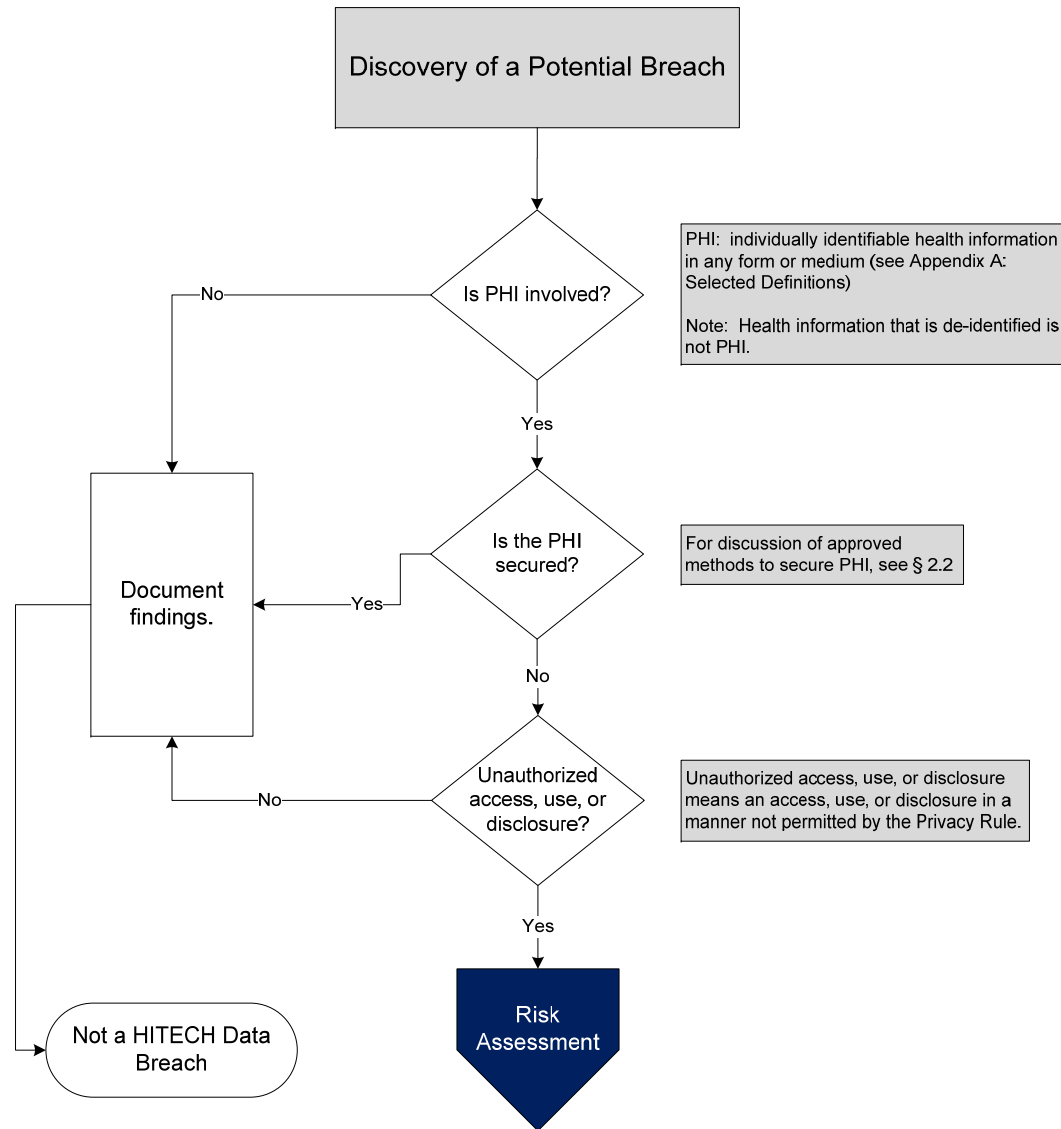
1. Who impermissibly accessed, used, or to whom the information was impermissibly disclosed.
2. Was the information returned prior to being accessed for an improper purpose?
3. The type and amount of PHI involved.

Hypothetical

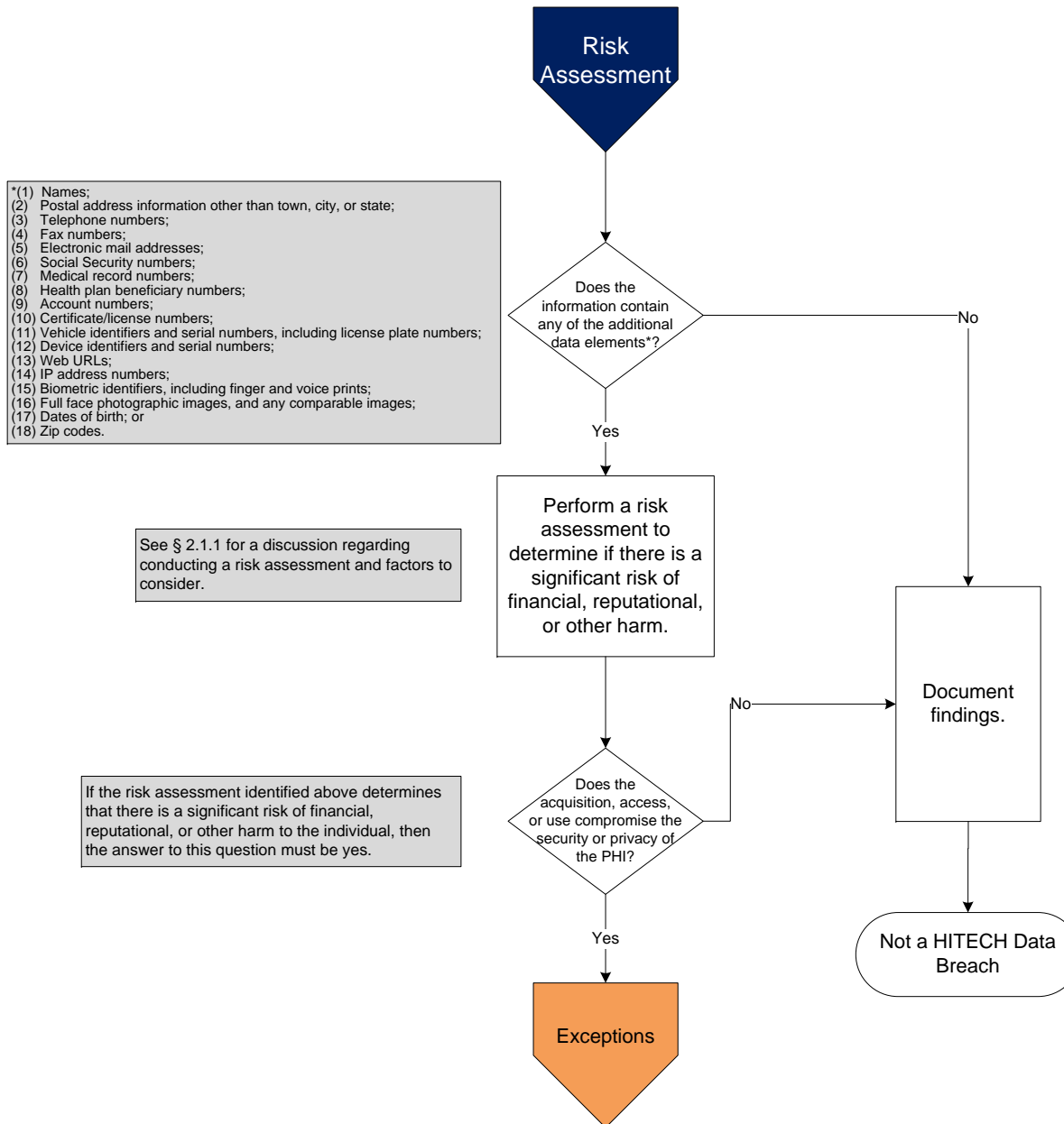
- Doctor loses laptop
 - Patient contact information (with notations)
 - Appointments (with procedures)
 - Ability to log in to billing system
- Situation 1: not encrypted
- Situation 2: encrypted

Situation 1 - Analysis

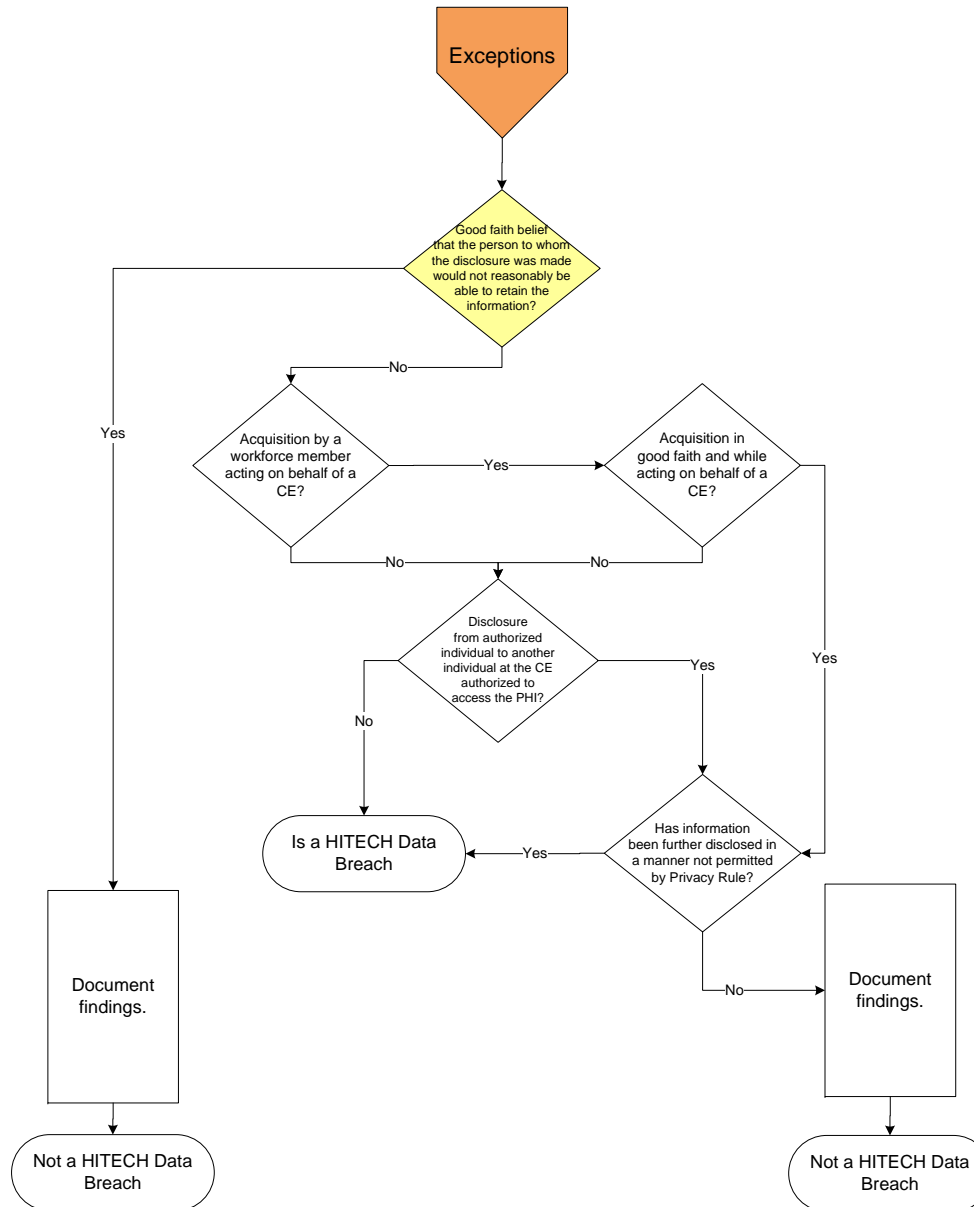
HITECH Definition of Breach Flowchart



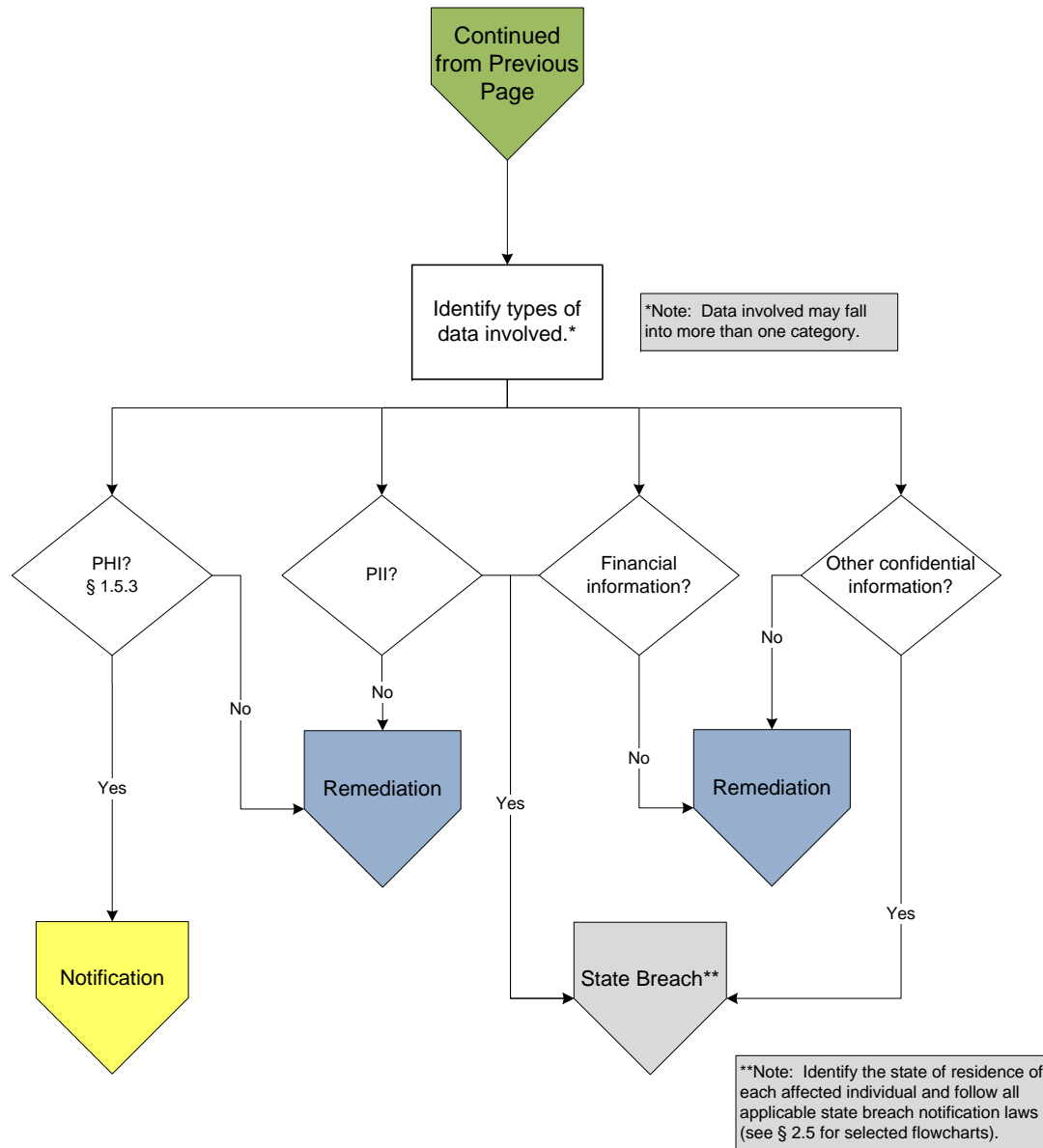
Situation 1 - Analysis (cont.)



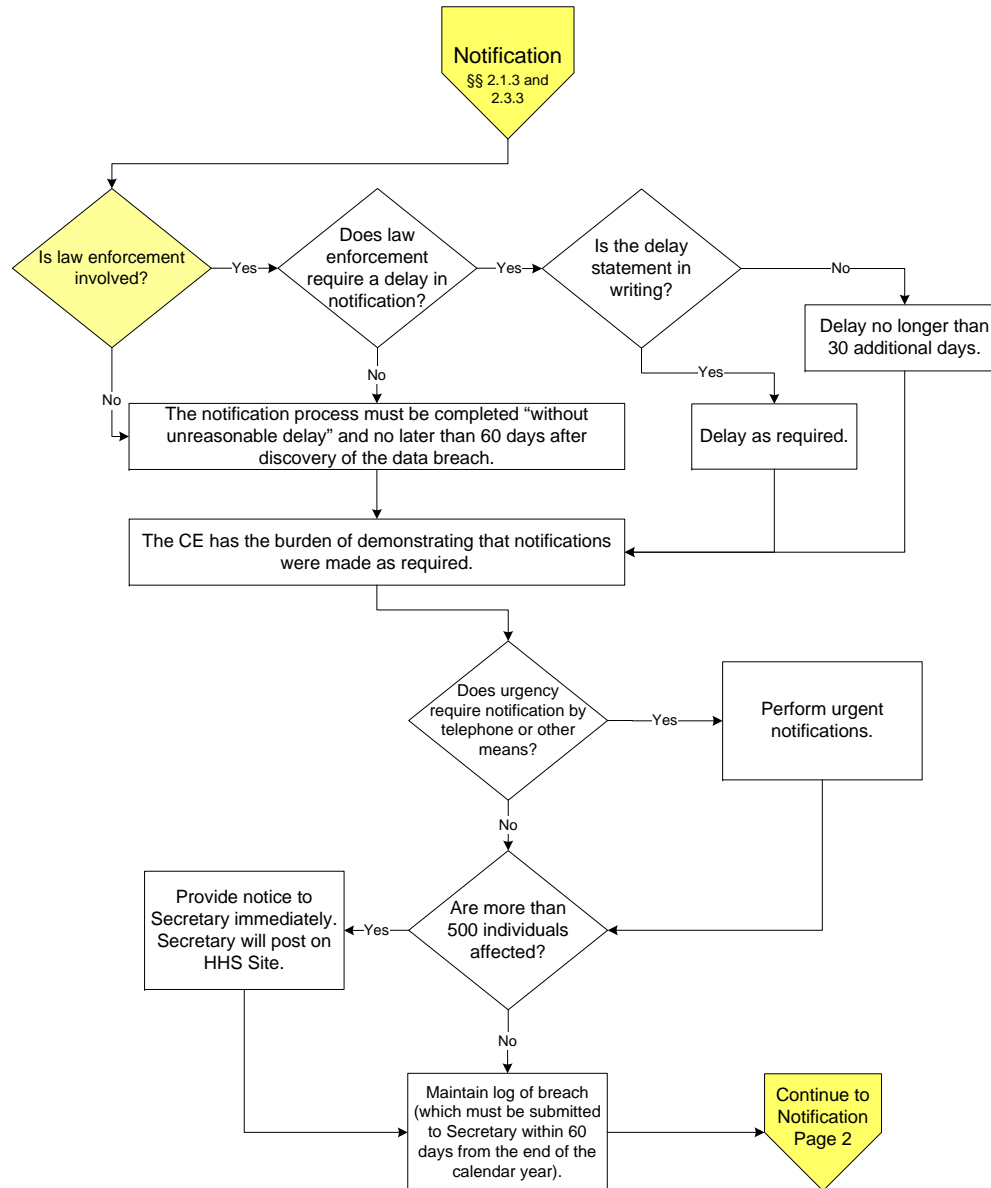
Situation 1 - Analysis (cont.)



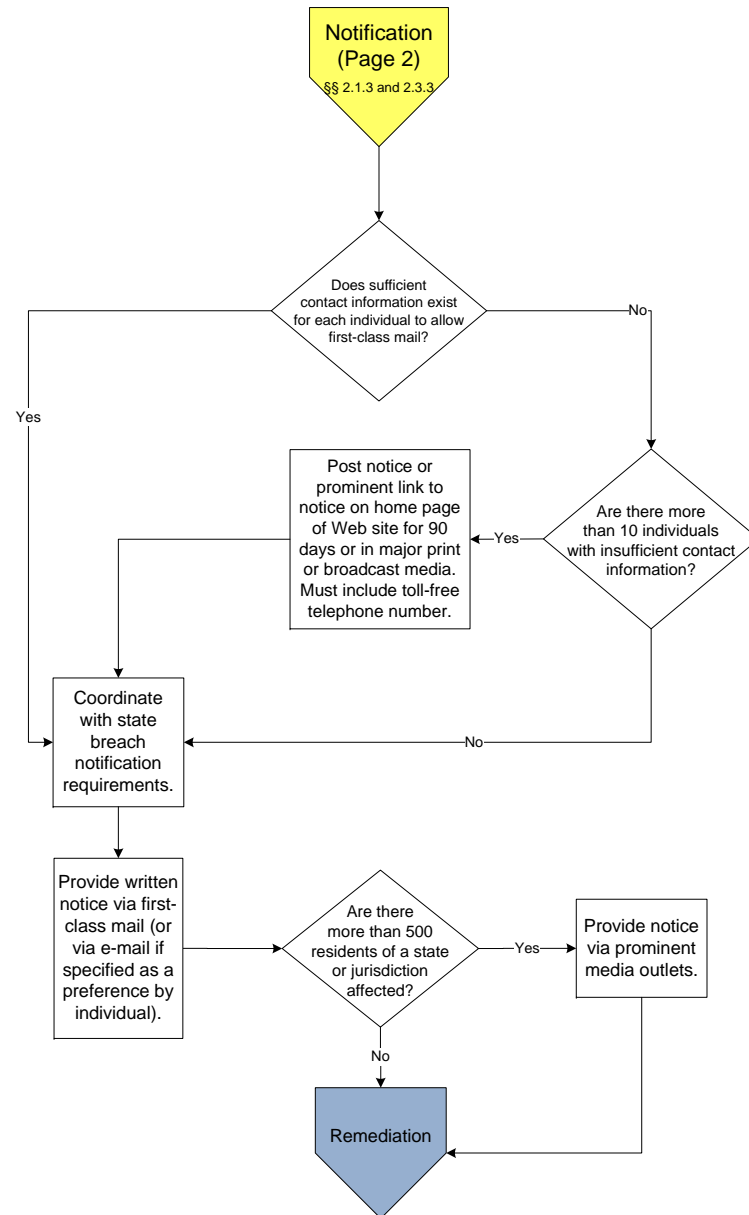
Situation 1 - Analysis (cont.)



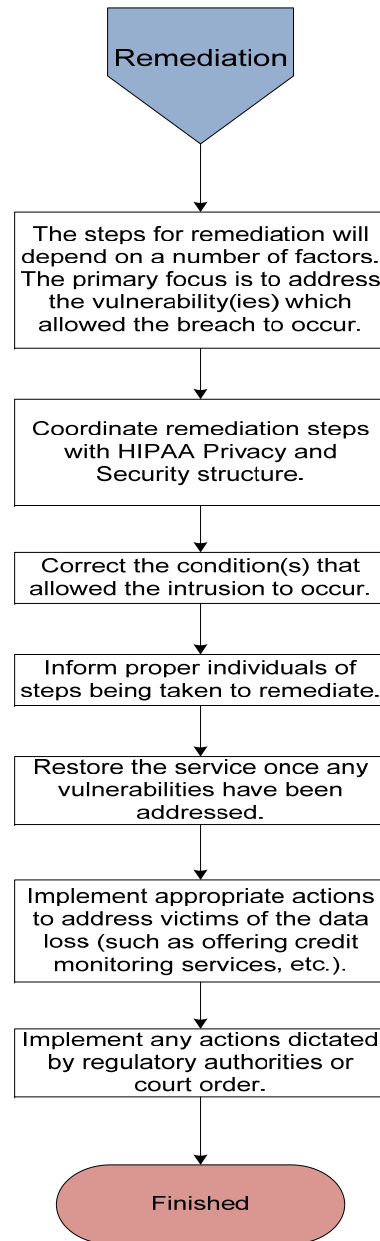
Situation 1 - Analysis (cont.)



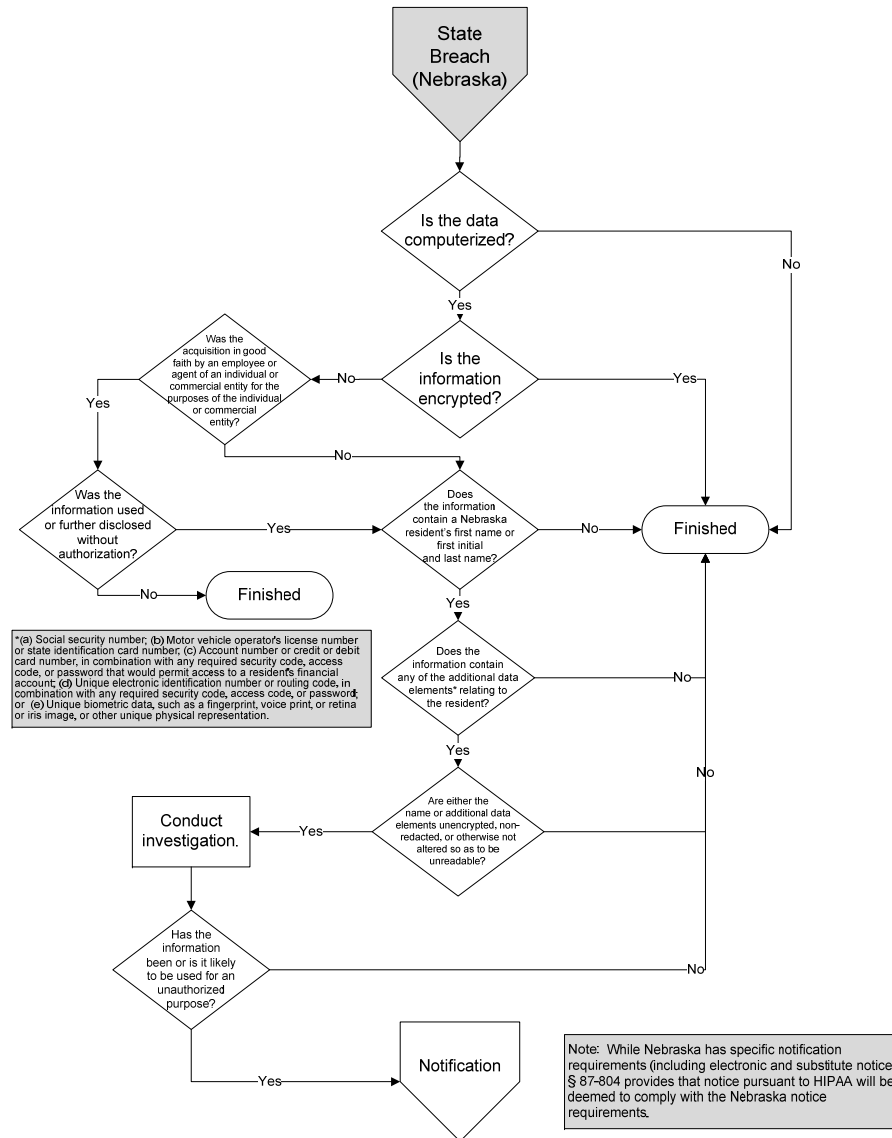
Situation 1 - Analysis (cont.)



Situation 1 - Analysis (cont.)



Situation 1 - Analysis (cont.)

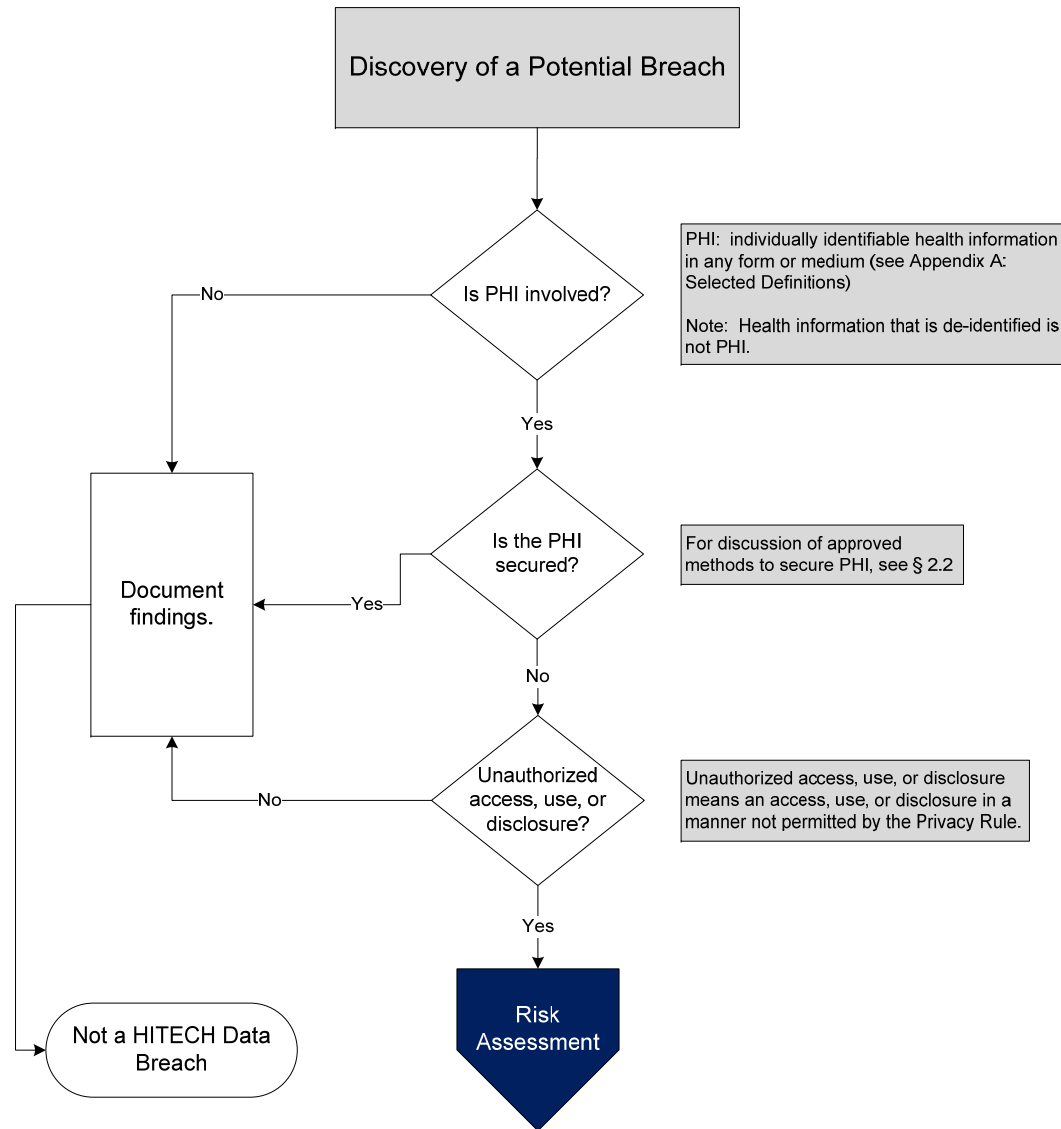


Hypothetical

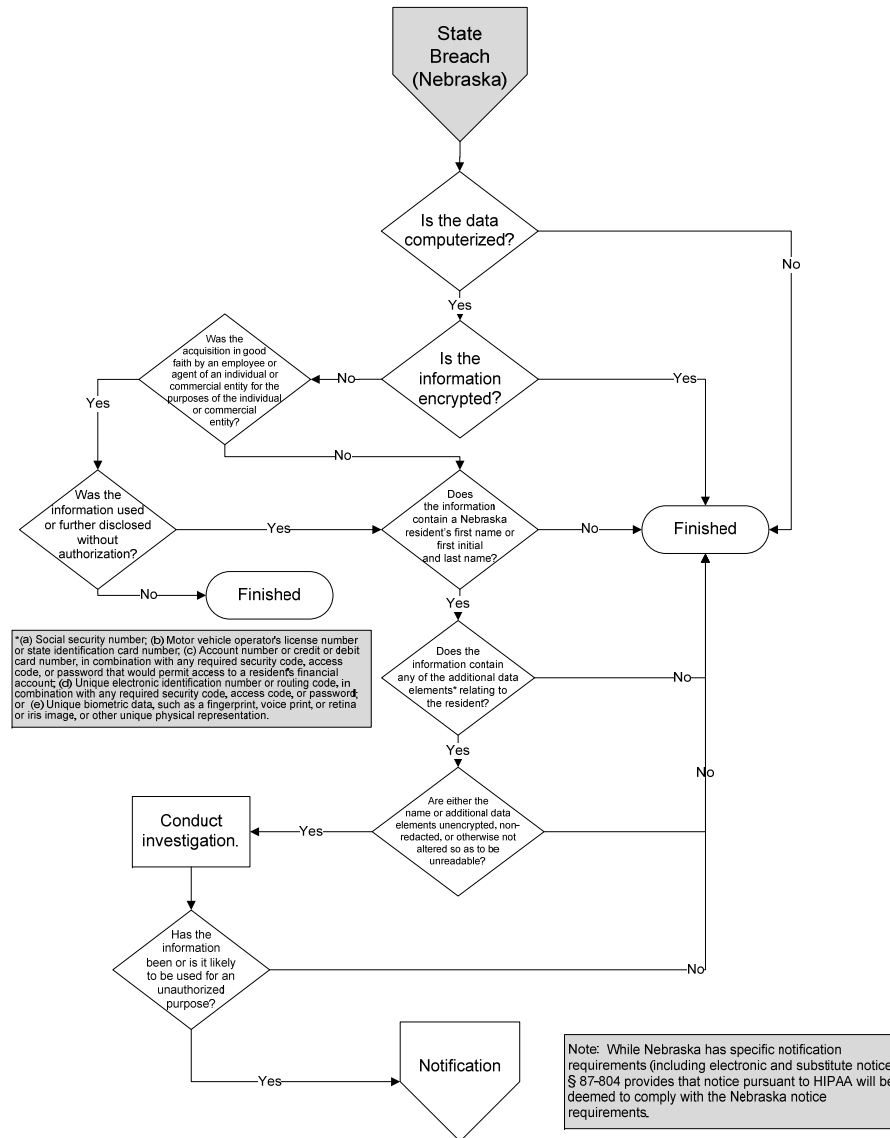
- Doctor loses laptop
 - Patient contact information (with notations)
 - Appointments (with procedures)
 - Ability to log in to billing system
- Situation 1: not encrypted
- Situation 2: encrypted

Situation 2 - Analysis

HITECH Definition of Breach Flowchart



Situation 2 - Analysis



State Data Breach Notification Laws

- As of April 12, 2010, 46 states have security breach laws.
- The following states do not have security breach laws:
 - Alabama
 - Kentucky
 - New Mexico
 - South Dakota
- However, the following territories do have some form of data breach notification laws:
 - District of Columbia
 - Puerto Rico
 - Virgin Islands

State Data Breach Notification Laws (cont.)

- Varying triggers for reporting:
 - Likelihood PII has been or will be used for unauthorized purposes (NE)
 - Any breach (IL)
 - Paper as well as electronic (MA)

State Data Breach Notification Laws (cont.)

- The specific notice requirements vary by state. For example:
 - Florida and Ohio require notice within 45 days of the discovery of the breach; Wisconsin requires notice within 15 days after the company learns of the breach.
 - North Carolina security breach notification law covers both electronic and hard copy documents.
 - Some states require notice only if a certain number of consumers or residents are affected (e.g., more than 1,000).
 - Some states require the company affected by the breach to notify all credit reporting agencies and the state's Attorney General's office.

Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006

- Conduct business in Nebraska and system has personal information about a resident of Nebraska
- Become aware of a breach of the security of the system:
 - conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose
 - If the investigation determines that the use of information has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (cont.)

- Notice shall be made as soon as possible and without unreasonable delay.
- Attorney General may seek direct economic damages for each affected Nebraska resident

Additional State Laws

- Massachusetts *Standards for the Protection of Personal Information of Residents of the Commonwealth* (201 CMR 17.00)
- Comprehensive written information security program including:
 - risk assessment, policies, access controls, monitoring, annual review, user authentication, encryption (transmission, portable devices), etc.

Additional State Laws (cont.)

- Nevada Senate Bill 227 (signed into law May 29, 2009)
 - requires those accepting a payment card in connection with transaction to comply with Payment Card Industry (PCI) Data Security Standards
 - Others collecting or transmitting personal information must encrypt when in "an electronic nonvoice transmission other than a facsimile" or moving the data "beyond the logical or physical controls."

Emerging Trends

- 1.0 Incident based – breach notification
- 2.0 Reasonable requirements (GLB, HIPAA, FTC)
- 2.5 Encryption in transmission
- 3.0 More specific standards (including encryption at rest, user authentication, etc.)

Recommendations

- Comprehensive privacy and security program
- Team: technical and legal
- Focus on culture – educate
- Limit collection of personal information
- Encrypt data at rest and in motion
- **Portable devices**
- Remote access

Questions?