Intersecting State & Federal Data Protection Acts

Richard E. Mackey, Jr.
Vice president
SystemExperts Corporation
dick.mackey@sytemexperts.com

Agenda

- Background
- MA 201 CMR 17
- NV 603a
- HITECH
- The Federal DATA Act
- Red Flag Rules
- Summary

Regulatory Summary

- Forty-five states have enacted legislation requiring notification of security breaches involving personal information
- Many laws only deal with notification after a breach
- Massachusetts and Nevada have passed laws/regulations aimed at *preventing* breaches
- The House of Representatives has passed the DATA Act (HR 2221) – also requiring preventive measures – it's in committee in the Senate now
- HITECH has broadened applicability of HIPAA requirements
- Red Flag Rules require any organization that extends credit to look for "red flags" that indicate identity theft

Comparing Regulations

- Until now, most laws designed to protect information were risk based and rather vague
  - HIPAA, GLB, CA
- New laws (MA and NV) are more prescriptive
- They require specific administrative and technical controls
- The trend is to prescribe controls while taking risk into account

MA 201 CMR 17

- The law is designed to prevent identity theft
- Requires all holders of personal information to implement procedural and technical safeguards to protect the data
- Is consistent with controls required by industry standards (ISO 27000) and other regulations (HIPAA, Red Flag Rules)
- Companies' programs are judged taking into account risk
  - The size, scope, and type of business
  - The resources available
  - The amount of stored data
  - The need for security and confidentiality of information
- This regulation appears to be setting the standard

WISP

- All new regulations require formal programs
- MA 201 CMR 17 requires organizations to have a formal comprehensive **w**ritten **i**nformation **s**ecurity **p**rogram (WISP)
- What is a WISP?
  - Full documentation of your security program
  - Documentation of the specific controls required by the law

MA Administrative Controls

- A designated person or group responsible for managing the security program
- A risk assessment and management program
- A method of assessing the effectiveness of controls protecting personal data
- An employee and contractor training program
- A set of security policies and procedures
- A method of monitoring employee compliance

MA Administrative Controls 2

- A means for detecting and preventing security system failures (monitoring and review)
- Specific policies and procedures relating to the storage, access, transmission, and handling of personal data
- Disciplinary measures for non-compliance
- A reliable method of promptly disabling access of terminated employees

MA Administrative Controls 3

- A program to ensure that third parties with access to personal data are competent and contractually obligated to maintain appropriate safeguards on the information
- A set of physical controls to ensure that systems, media, and paper containing personal data are protected from unauthorized access
- An annual review of security measures and reviews whenever there is a material change in business practices that may affect

MA Technical Controls

- Secure user authentication methods, including secure protocols that do not expose passwords on the network, strong passwords, secure password storage, unique user identifiers, and optional two-factor authentication technologies
- Access control mechanisms that restrict access to only active users
- Automatic lockout after multiple failed access attempts
- Tight access controls on files and records containing personal information
- Restriction of access to those with a business need
- Removal of all vendor default accounts

MA Technical Controls 2

- Encryption of personal records when transmitted across public and wireless networks
- Monitoring of systems for unauthorized use and access to personal information
- Encryption of all personal information stored on laptops or other portable devices
- An Internet firewall protecting systems and files containing personal information
- A vulnerability and management program that keeps software and virus definitions up-to-date

Nevada 603a

- Requires “data collectors” to:
- Implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure of personal data
- Comply with current PCI DSS (if a merchant)
- Encrypt personal information transmitted outside the secure system of the data collector
- Encrypt data on storage devices moved outside the physical controls of the data collector
- Contract with business associates to maintain reasonable measures …

NV 603a (continued)

- Requires notification in event of breach
- Allows civil action against those who profit from breach
- Provides for restitution by perpetrator to data collector for damages
- Attorney General may bring injunction against violator
- Organizations are not liable if they are compliant
- Does not apply to communications providers

HITECH

- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Part of the American Recovery and Reinvestment Act of 2009
- Government will encourage nationwide electronic exchange and use of health information to improve quality and coordination of care.
- Investing $20 billion in incentives to deploy health technology
- Goal to improve quality of care and care coordination and reduce medical errors and duplicative care
- Strengthening Federal privacy and security law to protect identifiable health information from misuse as the health care sector increases use of Health IT

HITECH Act

- Establishes a Federal breach notification requirement for health information that is not encrypted
- Requires notification of unauthorized disclosure
- Expands compliance requirements to all organizations with access to health information
- Allows individuals to request audit trail
- Shuts down secondary information mining market
- Requires patient authorization to use EPHI for marketing and fundraising
- Strengthens enforcement of Federal privacy and security laws by increasing penalties for violations
- Provides greater resources for enforcement and oversight activities

HITECH Impact

- Growing market for electronic interchange with incentives
- More risk
- Broader HIPAA compliance applicability
- Greater need for compliance methods and metrics

HIPAA/HITECH Challenges

- Measuring Security Rule compliance has always been a challenge
  - Lack of detailed specification
  - Difficulty in deriving controls from risks
  - No set of established controls
  - No standard to judge business associates
- Problem compounded with HITECH
  - More legal responsibility
  - Greater funding for enforcement
  - Greater requirements for auditability

Data Accountability and Trust Act of 2009

- Passed in the House of Representatives
- Supersedes state notification laws
- Considers bank account information personal information only with PIN
- Places strong requirements on information brokers
  - Accuracy
  - Policy audits
  - Individual access to data
  - Post breach audits
- Requires a program of administrative and technical controls

DATA Bill Controls

- Responsible officer
- Formal security policy for personal information
- Vulnerability management
  - Assessment
  - Monitoring
  - Corrective actions
- Secure data destruction procedures
- Notification procedures

Red Flag Rules

- Identity theft prevention/detection regulation
- Enforced by the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration
- Requires all organizations that extend credit to implement a program to look for “red flags” indicating identity theft attempts
- Example red flags:
  - Mismatches of name and SSN
  - Mismatches of SSN and age or location
  - Known stolen identities
  - Suspicious documents (forgeries, mismatch of signer)

Red Flag Requirements

- Governance
  - Formal program with assignment of responsibility
  - Board of Director approval of program
- Assessment of risk of identity theft in the context the business
- Specification of red flags
- Policies and procedures to effectively recognize red flags
- Policies and procedures to respond to red flags (notification, law enforcement)
- Training
- Service provider oversight

Summary

- Trend is toward laws that are more prescriptive while still being risk based
- Most regulations require
  - Governance
  - Policy
  - Data controls (identification, isolation, encryption)
  - Identity management and access controls
  - Vulnerability management
  - Incident response (and breach notification)
  - Monitoring and assessment of effectiveness
- Your best path is to establish a security program that meets these needs as the trend of stricter regulations and threats to information will only intensify