Designing a Privacy Policy and Incident Response Program for Employee Personal Information

Business Law Institute CLE
Hamline University School of Law
September 27, 2013

Melissa Rosenbaum
Senior Attorney and
Deputy System Privacy Coordinator
Federal Reserve Bank of Minneapolis

Overview

- Legal Framework
  - Minnesota Breach Notification Statute
- Design Issues to Consider
  - Defining Employee Personal Information
  - Protecting Employee Personal Information
  - Responding to Potential Breaches
- Key Considerations for Successful Implementation

Legal Framework

- U.S. legal privacy framework is sector based
  - No comprehensive federal requirements
  - Laws based largely on potential for identity theft or fraud

- Employee personal information generally considered confidential
  - Protected by mix of sector laws, such as HIPAA, state laws, codes of conduct, and policies and procedures

- State laws instrumental in informing policies
  - 46 states have breach notification laws
  - Exceptions: Alabama, Kentucky, New Mexico, South Dakota

Legal Framework:
State Breach Notification Laws

- Most include some form of these elements:
  - Entities subject to the law
  - Definition of personal information
  - Definition of “breach in the security of the system”
  - Who must be notified and when
  - Exceptions to notification
  - Requirements for the communication

Legal Framework:
Minnesota Breach Notification Law

"Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the needs of law enforcement …"*

*Minn. Stat. §325E.61(1)(2013).

Issues to Consider:
How Will Policy Define Personal Information?

- MN breach notification statute defines personal information as a name or first initial and last name in combination with:
  - Social security number;
  - Driver’s license number or MN ID card number; or
  - Account number or credit or debit card number, in combination with any required code/password that would permit access to a financial account.*
- Definition applies if one or more data elements is not encrypted

*Minn. Stat. §325E.61(1)(e).

Issues to Consider:
How will Policy Define Personal Information?

- Consider other state or international laws
- Consider whether to define more broadly than legal requirements
  - Personnel information such as compensation, performance reviews, disciplinary action, contact information
  - Trends and definition in other contexts
- Consider whether to create subsets of personal information, classified by risk

Issues to Consider:

How will the Policy Protect Personal Information?

- MN breach notification statute does not impose specific security requirements
    - But, exempts encrypted data from personal information
- Minnesota social security shield law*
    - Requires affirmative steps to protect against disclosure
- Other legal and policy considerations
    - Additional sector specific requirements
    - Other state laws
        - Massachusetts requires a "comprehensive information security program," including encryption, access control, monitoring, and training **

*Minn. Stat. §325E.59 (2013).

**201 CMR 17.04 (2013).

Issues to Consider:

How will the Policy Protect Personal Information?

- Consider conducting an inventory of personally identifiable information (PII)
- Benefits of PII inventory
  - Raise awareness and encourage minimization of data
  - Provide starting point for risk assessment
  - Identify vendors with access to PII
    - Implement contract provisions
- Work closely with information security
  - Ensure appropriate technical and physical safeguards

Issues to Consider:
Responding to Potential Breaches

- Contain and control the incident
- Conduct analysis of notification requirements
- MN breach notification statute
  - “Breach of the security of the system” is “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.”
    - No risk of harm requirement
    - Good faith exception
  - Form of notice may be written, electronic or substitute, depending on circumstances
  - No notice content requirements

Issues to Consider:
Responding to Potential Breaches

- Assess policy considerations
- Notify affected and relevant individuals as needed/ appropriate
- Consider providing credit monitoring
- Conduct post-incident review

Key Considerations for Successful Implementation

- Top-down support
- Employee communication and awareness
  - Encourage reporting
  - Conduct training – ongoing and annual basis
- Vendor management
- Designated individual/ committee responsible for process
- Relationship with stakeholders
  - Information Security
  - Legal
  - Human Resources
  - Enterprise Risk
  - Public Affairs
  - Business Areas

Additional Resources and Information

- International Association of Privacy Professionals (IAPP), Resources (some resources require membership for access)
  - https://www.privacyassociation.org/resource_center
- Federal Trade Commission, Bureau of Consumer Protection Business Center, Privacy and Security: compliance and legal resources
  - http://business.ftc.gov/privacy-and-security
- Minnesota Legislative Reference Library: links to privacy resources and legislative tracker for MN
  - http://www.leg.state.mn.us/lrl/issues/issues.aspx?issue=Privacy
- California Office of the Attorney General, Privacy Enforcement and Protection: business and legal resources, consumer topics, reports
  - http://oag.ca.gov/privacy
- Privacy Rights Clearinghouse: consumer-oriented resources, breach database
  - www.privacyrights.org