Resource ID: 7-523-1520

Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation

MELISSA J. KRASNOW, VLP LAW GROUP LLP

Search the Resource ID numbers in blue on Practical Law for more.

A Note discussing written information security programs (WISPs) under the Massachusetts data security regulation (Mass. Regs. Code tit. 201 § 17.00). The Note also discusses reasons for adopting a WISP, preliminary considerations, and enforcement actions by the Massachusetts Attorney General.

The Massachusetts data security regulation (Mass. Regs. Code tit. 201 § 17.01-05) (Massachusetts Regulation) contains some of the most stringent and detailed data security requirements for organizations by a state to date. Massachusetts was the first and is one of the few states to require covered organizations to adopt a comprehensive written information security program (WISP) incorporating specific security measures. Effective since March 1, 2010, the regulation has extensive reach, purporting to cover every organization, wherever located, that owns or licenses Massachusetts residents' personal information.

This Note focuses on developing and implementing WISPs based on the Massachusetts Regulation's requirements. It discusses:

- Preliminary considerations and steps when developing a WISP.
- The Massachusetts Regulation's requirements.
- Massachusetts enforcement actions.

For an example of a WISP that complies with the Massachusetts Regulation and other similar laws, see Standard Document, Written Information Security Program (WISP) (w-001-0073).

REASONS FOR ADOPTING A WISP

In addition to the Massachusetts Regulation, organizations may be subject to other laws and industry standards requiring them to develop written information security programs and implement reasonable security measures (see Box, Additional Relevant US Laws, Guidance, and Industry Standards). However, even where WISPs are not legally required, they are a good business practice for any organization that collects, uses, stores, transfers, or disposes of personal information.

In February 2012, the Obama administration issued Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (w-005-5093). The White House report includes a Consumer Privacy Bill of Rights that sets out the principle that consumers have the right to secure and responsible handling of their personal data.

The consumer privacy framework in the Federal Trade Commission's (FTC) March 2012 final privacy report, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, describes best practices for organizations to protect consumer privacy, including building privacy protections into everyday business practices (privacy by design). These protections include providing reasonable security for consumer data. Recent FTC enforcement actions demonstrate similar expectations (see Practice Note, FTC Data Security Standards and Enforcement (8-617-7036)).

Because of the ongoing threat of data breaches and incidents, and the potential for significant associated legal, business, and reputational costs, organizations increasingly take steps to ensure their third-party service providers and other business partners have comprehensive written information security programs (see Third-Party Service Providers). These steps include requiring contractual protections in relevant agreements (such as purchase agreements or cloud computing services agreements).

Organizations are also increasingly seeking cyber liability insurance and therefore may need to provide information about their information security programs to insurers (see Practice Note, Cyber Insurance: Insuring for Data Breach Risk (2-588-8785)).

PRELIMINARY CONSIDERATIONS

Preliminary steps in developing and implementing a WISP include:

- Identifying reasons for adopting the WISP and its objectives (see Reasons for Adopting a WISP).
- Determining and evaluating the requirements of the Massachusetts Regulation and all other applicable laws, guidance from

governmental authorities, enforcement actions, and industry standards, including identifying any conflicting requirements.

- Gathering all relevant information concerning the personal information the organization collects, uses, stores, and shares. This includes identifying:
  - the categories and types of personal information;
  - how the organization collects, uses, stores, transfers, and destroys the personal information, and the systems and technologies the organization uses for these purposes;
  - the state (and if not the US, country) residences of the individuals whose personal information the organization holds;
  - the organization's third-party service providers and other business partners that have or may have access to personal information the organization holds or controls;
  - the organization's current information security procedures, practices, and policies; and
  - the employees within the organization who are responsible for developing, implementing, maintaining, and enforcing the WISP.

SCOPE OF THE WISP

The scope and complexity of a WISP will vary depending on the organization's specific circumstances. However, two threshold issues include whether to:

- Adopt a WISP that applies to personal information of:
  - only Massachusetts residents; or
  - all personal information the organization holds.

  (See Personal Information Covered by the WISP.)
- Combine the WISP with other information security compliance program documents or maintain separate resources (see Combining with Other Privacy and Information Security Compliance Program Documents).

PERSONAL INFORMATION COVERED BY THE WISP

The organization must initially decide whether the WISP will be created to:

- Specifically comply with the Massachusetts Regulation and only apply to Massachusetts residents' personal information.
- Broadly apply to the collection of personal information from residents of other states.

Adopting a WISP that applies to all personal information the organization holds can provide administrative ease. Although not currently required by most states, a comprehensive WISP reflects best practices and can help reduce the organization's risks. The organization may choose to use the Massachusetts Regulation as a baseline, but it should ensure the WISP takes into account all relevant states' privacy and data security laws, including the various definitions of personal information each state has adopted. For more details on state-specific definitions of personal information, especially as applied in state data breach notification laws, see Practice Note, State Data Breach Laws Protected Personal Information Chart: Overview (4-609-2845).

However, the organization may want to limit the scope of the WISP to the Massachusetts Regulation to narrow its compliance obligations. For example, where only one business unit of an organization collects Massachusetts residents' personal information, the organization may seek to keep that unit's compliance obligations separate from its other business units' obligations.

COMBINING WITH OTHER PRIVACY AND INFORMATION SECURITY COMPLIANCE PROGRAM DOCUMENTS

Where an organization is subject to more than one set of privacy and information security requirements, it can be administratively simpler to consolidate its programs and related policies and procedures into one comprehensive compliance program document. However, the organization may need to consider conflicting legal requirements. For example, organizations subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Gramm-Leach-Bliley Act (GLBA) must also comply with the Massachusetts Regulation.

Like the Massachusetts Regulation, the GLBA Safeguards Rule requires that financial institutions develop comprehensive written information security programs to protect customer information (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules: Information Security Program (4-578-2212)). However, the GLBA Safeguards Rule and Massachusetts Regulation differ in their specific requirements, for example:

- The Safeguards Rule applies only to customer information while the Massachusetts Regulation applies to Massachusetts residents' personal information, including both customer and employee information.
- The Safeguards Rule's requirements are broader and less precise than the Massachusetts Regulation's requirements.

One advantage in keeping a WISP developed specifically for the Massachusetts Regulation separate from the organization's other information security policies is that if the Massachusetts Attorney General or another state attorney general or regulator requests a copy of the Massachusetts WISP, the organization may be able to limit its disclosure to the Massachusetts WISP and not its other policies.

For an example of a WISP that addresses multiple federal and state requirements in one program document, including the Massachusetts Regulation and the Safeguards Rule, see Standard Document, Written Information Security Program (WISP) (w-001-0073).

MASSACHUSETTS REGULATION: GENERAL WISP REQUIREMENTS

The Massachusetts Regulation requires every person that owns or licenses personal information about a Massachusetts resident to develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards that are appropriate to:

- The size, scope, and type of the person's business.
- The person's available resources.
- The amount of stored data.
- The need for security and confidentiality of both consumer and employee information.

In addition, the safeguards must be consistent with safeguards for protection of personal information and similar information set out in any state or federal regulations that apply to that person.

(Mass. Regs. Code tit. 201 § 17.03(1)).

The Massachusetts Regulation also includes a set of:

- Specific WISP requirements (see Massachusetts Regulation: Specific WISP Requirements).
- Computer system security requirements for organizations that electronically store or transmit personal information (see Massachusetts Regulation: Computer System Security Requirements).

WHO MUST COMPLY?

Covered Persons

The Massachusetts Regulation applies to any person (including, for example, a corporation, association, partnership, or other legal entity as well as a natural person) that owns or licenses personal information, which includes any organization that receives, stores, maintains, processes, or otherwise has access to personal information either for:

- The provision of goods or services.
- Employment.

(Mass. Regs. Code tit. 201 § 17.02.)

The Massachusetts Regulation applies to any person regardless of whether that person is located in Massachusetts or even the US.

Persons Covered by HIPAA and GLBA

A person who must comply with HIPAA or GLBA also must comply with the Massachusetts Regulation.

DEFINITION OF PERSONAL INFORMATION

The Massachusetts Regulation defines personal information as a Massachusetts resident's first and last name or first initial and last name combined with one or more of that resident's:

- Social Security number.
- Driver's license number or state-issued identification card number.
- Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password, that would permit access to a Massachusetts resident's financial account.

The definition excludes any information lawfully obtained from either:

- Publicly available information.
- Federal, state, or local government records lawfully made available to the public.

(Mass. Regs. Code tit. 201 § 17.02.)

MASSACHUSETTS REGULATION: SPECIFIC WISP REQUIREMENTS

The Massachusetts Regulation requires that every WISP include:

- Designating one or more employees to maintain the WISP (see Program Oversight).
- Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of electronic, paper, or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of current safeguards for limiting these risks, including:
  - ongoing employee training, including training for temporary and contract employees;
  - employee compliance with policies and procedures; and
  - means for detecting and preventing security system failures.

  (See Identifying and Minimizing Reasonably Foreseeable Internal and External Risks.)
- Developing security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises.
- Imposing disciplinary measures for violations of the WISP's rules.
- Preventing terminated employees from accessing records containing personal information.
- Overseeing service providers by:
  - taking reasonable steps to select and retain third-party service providers capable of maintaining appropriate security measures to protect personal information consistent with the Massachusetts Regulation and any applicable federal regulations; and
  - contractually requiring them to implement and maintain these security measures.

  (See Third-Party Service Providers.)
- Reasonable restrictions on physical access to records containing personal information, and storage of those records in locked facilities, storage areas, or containers.
- Regular monitoring to ensure that the WISP is operated in a way reasonably calculated to prevent unauthorized access to or unauthorized use of personal information.
- Upgrading information safeguards as necessary to limit risks.
- Reviewing the scope of the security measures:
  - at least annually; or
  - whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information.
- Documenting:
  - responsive actions taken in connection with an incident involving a security breach;
  - mandatory post-incident review of events; and
  - any actions taken to make changes in business practices related to protecting personal information.

  (Mass. Regs. Code tit. 201 § 17.03(2).)

PROGRAM OVERSIGHT

The Massachusetts Regulation specifically requires the covered person to designate one or more employees as the data security coordinator or coordinators to maintain the WISP. The data security coordinators are responsible for ensuring that the WISP's specific requirements are carried out, whether by them or others (see Massachusetts Regulation: Specific WISP Requirements). The considerations in designating data security coordinators and assigning their specific responsibilities depend on the organization's specific circumstances and may include:

- The organization's:
  - size;
  - industry; and
  - regulators.

- The types of personal information that the organization owns or maintains on behalf of another organization.
- The employees responsible for the organization's compliance with security requirements, including compliance with:
  - internal policies;
  - contracts; and
  - relevant laws and industry standards.

The organization should also consider the appropriate business units to involve in program oversight, which may include:

- Legal.
- Information technology.
- Privacy or a broader compliance unit.

IDENTIFYING AND MINIMIZING REASONABLY FORESEEABLE INTERNAL AND EXTERNAL RISKS

A key requirement of the Massachusetts Regulation is identifying reasonably foreseeable internal and external risks and adopting steps to mitigate those risks. Risks vary depending on the organization's specific circumstances. Examples of common risks include:

- Inadequate personnel training (see Inadequate Personnel Training).
- Unencrypted personal information (see Unencrypted Personal Information).
- Personal information in paper format (see Personal Information in Paper Format).
- Lack of control over portable devices (see Lack of Control Over Portable Devices).

Inadequate Personnel Training

Inadequate training and education of an organization's personnel creates a reasonably foreseeable internal risk to the protection of personal information. To minimize risk, organizations should ensure that:

- Personnel actually receive the training and have access to information about the requirements.
- The organization has the means to identify when personnel miss or fail to complete the training.
- The training and information provided sufficiently convey the data security requirements so that personnel can comprehend them.
- They periodically assess compliance.

The organization should provide ongoing training and information and update them as necessary or appropriate. For example, after a data breach or incident, the organization should:

- Update training and information to include lessons learned.
- Consider additional or interim training.

Unencrypted Personal Information

Unencrypted personal information is another reasonably foreseeable external risk. The Massachusetts Regulation requires, to the extent technically feasible, encryption of all:

- Transmitted records and files containing personal information that will travel across public networks.
- Data containing personal information to be transmitted wirelessly.
- Personal information stored on laptops or other portable devices.

(See Massachusetts Regulation: Computer System Security Requirements.)

To reduce risks caused by unencrypted personal information, an organization can, for example:

- Conduct an initial inventory of all laptops and other portable devices and continuously maintain the inventory. The inventory should identify whether each device is owned by the organization or the individual.
- Determine whether personal information is stored on the laptops and other portable devices and, if so, whether and how the information is encrypted.
- Where technically feasible, implement encryption of personal information when it is stored on portable devices or transmitted over public or wireless networks.
- Implement tools such as data loss prevention software that flag e-mails containing designated personal information.
- Conduct ongoing training, make regular assessments, and follow up on unsatisfactory results.

The Massachusetts Office of Consumer Affairs and Business Regulation advises against sending unencrypted personal information through e-mail. It suggests instead using alternative methods to conduct transactions involving personal information, for example, by setting up a secure website that requires safeguards like user names and passwords.

Personal Information in Paper Format

Creating, maintaining, transferring, and disposing of personal information in paper format creates reasonably foreseeable internal and external risks to the organization's protection of personal information. Examples of records containing personal information often maintained in paper format include:

- Employment-related documents.
- Customer credit card information.
- Tax, employee benefit, and transaction-related documents for the organization's security holders (for example, stockholders or bondholders).

Organizations that handle personal information in paper format must follow appropriate safeguards, which may differ from those for personal information stored in electronic form. These safeguards may include, for example, requiring:

- Storage of paper records containing personal information in a secure location, for example, in locked filing cabinets, and limiting access to these records to specified individuals.
- Using envelopes or mailing covers without transparent windows for mailings that involve content containing personal information.
- Using a cross-cut shredder on paper records before disposal and ensuring disposal is made in accordance with applicable law,

internal policies, and procedures (for example, records retention policies) and any contractual requirements.

Lack of Control Over Portable Devices

An organization's lack of control over portable devices creates reasonably foreseeable internal and external risks to the organization's protection of personal information. Examples of lack of control over portable devices include:

- The failure to inventory and account for portable devices, whether owned by the organization or individually-owned and used for business purposes (see Standard Document, Bring Your Own Device to Work (BYOD) Policy (1-521-3920)).
- Lack of policies and procedures regarding use of portable devices for business purposes.
- The failure to properly implement and enforce policies and procedures concerning portable devices.

The Massachusetts Regulation specifically requires:

- Developing security policies for employees relating to the storage, access, and transportation of records containing personal information outside of business premises (see Massachusetts Regulation: Specific WISP Requirements).
- Creating and maintaining a security system covering the organization's computers (including any wireless system) (see Massachusetts Regulation: Computer System Security Requirements).

For additional examples of common information security gaps that may create risk, see Common Gaps in Information Security Compliance Checklist (3-501-5491).

THIRD-PARTY SERVICE PROVIDERS

The Massachusetts Regulation requires that the WISP include oversight of third-party service providers, including contractually requiring third-party service providers to implement and maintain appropriate measures for protecting personal information. Organizations should:

- Identify their applicable existing third-party service providers and, if necessary, amend their contracts to ensure compliance (see Amending Existing Contracts).
- Conduct data security due diligence on their third-party service providers (see Due Diligence).
- Include specific requirements in third-party service provider agreements involving personal information that address the Massachusetts Regulation and other data security matters (see Key Contract Requirements).

The organization should conduct ongoing training for personnel with responsibility for the organization's third-party service provider contracts to ensure that they are aware of and comply with the Massachusetts Regulation.

Amending Existing Contracts

The organization may need to amend its existing contracts to ensure compliance with the Massachusetts Regulation.

The organization should closely monitor responses to its requests to amend existing contracts to determine which contracts have been amended and track the status of third-party service provider contracts.

Due Diligence

Organizations should conduct due diligence on their third-party service providers' information security practices. Due diligence should include requesting and reviewing information on:

- The third-party service provider's data security and disaster recovery policies and procedures.
- Data security audit reports concerning the third-party service provider's information security program.
- Details of any actual or potential security breaches or incidents impacting the third-party service provider.

The organization should also consider speaking with existing clients of the third-party service provider.

Key Contract Requirements

The Massachusetts Regulation requires organizations to contractually obligate their third-party service providers to implement and maintain appropriate measures for protecting personal information. Generally, the organization should consider contract provisions that address:

- General and specific security requirements and procedures that the third-party service provider must maintain.
- The third-party service provider's ongoing compliance with applicable privacy and data security laws, including the Massachusetts Regulation.
- The organization's right to audit the third-party service provider's security procedures and policies.
- The organization's right to:
  - terminate the contract for material breaches; and
  - other remedies, for example, indemnification for losses arising out of the third-party service provider's failure to comply with its data security obligations.
- Secure disposal or return of the personal information to the organization on the agreement's termination or expiration.
- Requirements if the third-party service provider suspects or experiences a breach or an incident, such as immediately notifying the organization.

For sample contract clauses, see Standard Clauses, Data Security Contract Clauses for Service Provider Arrangements (Pro-Customer) (2-505-9027).

MASSACHUSETTS REGULATION: COMPUTER SYSTEM SECURITY REQUIREMENTS

The Massachusetts Regulation sets out additional requirements for computer security that, as a practical matter, apply to most organizations. If the organization stores or transmits personal information electronically, the WISP must include the establishment and maintenance of a security system covering

its computers (including any wireless system) that at a minimum includes, to the extent technically feasible:

- Secure user authentication protocols, including:
  - control of user IDs and other identifiers;
  - a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, like biometrics or token devices;
  - control of data security passwords to ensure they are kept in a location or format that does not compromise the security of the data they protect;
  - restricting access to active users and active user accounts only; and
  - blocking access to user accounts after multiple unsuccessful attempts to gain access or limiting access for the particular system.
- Secure access control measures that:
  - restrict access to records and files containing personal information to those who need the information to perform their jobs; and
  - assign unique identifications and passwords that are not vendor-supplied default passwords to each person with computer access and that are reasonably designed to maintain the integrity and security of the access controls.
- Encryption of all:
  - transmitted records and files containing personal information that will travel across public networks;
  - data containing personal information to be transmitted wirelessly; and
  - personal information stored on laptops or other portable devices.
- Reasonable monitoring of systems for unauthorized use of or access to personal information.
- Reasonably up-to-date firewall protection and operating system security patches for files containing personal information on systems that are connected to the internet, reasonably designed to maintain the integrity of the personal information.
- Reasonably up-to-date versions of system security agent software that includes malicious software (malware) protection and reasonably up-to-date patches and virus definitions, or a version of this software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis.
- Employee education and training on the proper use of the organization's computer system security and the importance of personal information security.

(Mass. Regs. Code tit. 201 § 17.04.)

MEANING OF TECHNICALLY FEASIBLE

The Massachusetts Regulation requires implementation of its computer system security requirements only if they are technically feasible. According to guidance from the Massachusetts Office of Consumer Affairs and Business Regulation, technically feasible means that if there is a reasonable means through technology to accomplish a required result, the organization must use it.

ENCRYPTION

Under the Massachusetts Regulation, encryption means the transformation of data into a form where meaning cannot be assigned without the use of a confidential process or key. The data must be altered into an unreadable form. Password protection that does not alter the condition of the data is not encryption. The definition of encryption is intended to be technology neutral and take into account new developments in encryption technology.

ADDITIONAL RELEVANT US LAWS, GUIDANCE, AND INDUSTRY STANDARDS

Other relevant US laws, guidance, enforcement actions, and industry requirements include:

- **GLBA.** The GLBA Safeguards Rule requires financial institutions to develop a comprehensive written information security program to protect customer information (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules (4-578-2212)).
- **HIPAA.** The Security Rule establishes standards to protect electronic protected health information that is created, received, used, or maintained by a covered entity or a business associate.
- **State security procedures laws.** In addition to Massachusetts, several other states (for example, California and Texas) have laws requiring organizations to develop, implement, and maintain reasonable security practices and procedures regarding personal information. Similar data security laws in other states include:
  - Oregon's statute that requires organizations to implement and maintain an information security program that includes specific safeguards (Or. Rev. Stat. § 646A.622);
  - Information security program requirements in Rhode Island's Identity Theft Protection Act of 2015 (R.I. Gen. Laws § 11-49.3.1); and
  - Illinois's Personal Information Protection Act, as amended in January 2017, calls for implementation and maintenance of reasonable security measures (815 Ill. Comp. Stat. Ann. 530/1).
- **State guidance.** In February 2016, the California Attorney General issued Data Breach Report 2012-2015 with recommendations defining a baseline level of information security. Specifically, the California Attorney General will deem failing to implement minimum information security controls, as defined by the 20 controls in the Center for Internet Security's Critical Security Controls, as a lack of reasonable security.
- **FTC enforcement actions.** The FTC has brought data security enforcement actions under Section 5 of the FTC Act against organizations for failing to take reasonable security measures. As part of its settlements of these enforcement actions, the FTC has required the organizations to implement comprehensive information security programs.

- **FTC guidance.** The FTC guidance entitled Protecting Personal Information: A Guide for Business describes steps organizations can take to protect personal information and principles for sound data security plans. The FTC's report, Start with Security: A Guide for Business, provides organizations with practical lessons gleaned from its data security enforcement actions. The FTC's report Internet of Things: Privacy & Security in a Connected World also describes security best practices for companies developing connected devices.
- **National Institute of Standards and Technology (NIST) Guidance.** The NIST cybersecurity framework, Framework for Improving Critical Infrastructure Cybersecurity, developed under Executive Order 13636 is a voluntary risk-based set of industry standards and best practices that organizations can use in managing cybersecurity risks (see Practice Note, The NIST Cybersecurity Framework (5-599-6825)).
- **Payment Card Industry Data Security Standard (PCI DSS).** These data security standards apply to organizations that process, store, or transmit cardholder data. The requirements include protecting cardholder data and maintaining an information security policy (see Practice Note, PCI DSS Compliance (8-608-7192)).

For more information on the additional laws, guidance, and industry standards, see Practice Note: US Privacy and Data Security Law: Overview (6-501-4555).

MASSACHUSETTS ATTORNEY GENERAL ENFORCEMENT ACTIONS

If an organization experiences a data breach involving a Massachusetts resident's personal information, it must provide written notification of the data breach to:

- The Massachusetts Attorney General.
- The Massachusetts Office of Consumer Affairs and Business Regulation.
- The affected Massachusetts resident.

The Massachusetts Attorney General can request a copy of the organization's WISP.

The Massachusetts Attorney General has brought a number of enforcement actions relating to data breaches. The enforcement actions show the importance of having a WISP in place and ensuring compliance. Typically, the actions have alleged that organizations violated one or more of the following laws by failing to institute security measures, such as encrypting personal information, failing to properly oversee third-party service providers, or failing to follow their own WISPs:

- The Massachusetts Regulation.
- The Massachusetts Security Breach Act.
- The Massachusetts Consumer Protection Act.
- HIPAA.

Many enforcement actions have resulted in settlement agreements. The settlement agreements have typically required the organizations to take actions such as:

- Institute or comply with a WISP that meets the Massachusetts Regulation's requirements.
- Institute specific security measures, such as:
  - encryption;
  - workforce training; or
  - overseeing third-party service providers.
- Review or audit their security programs.
- Implement specific corrective actions.
- Report to the Massachusetts Attorney General.
- Pay a civil penalty.

(See, for example, *In the Matter of Zappos.com, Inc.*, CIF. No. 15-0039, Assurance of Discontinuance (Mass. Sup. Ct. Jan. 7, 2015); *Commonwealth v. The Children's Hospital Corp.*, CIF No. 14-3955, Consent Judgment (Mass. Sup. Ct. Dec. 19, 2014); *In the Matter of TD Bank, N.A.*, CIF. No. 14-3832, Assurance of Discontinuance (Mass. Sup. Ct. Dec. 8, 2014); *Commonwealth v. Beth Israel Deaconess Med. Ctr.*, CIF No. 14-3627, Consent Judgment (Mass. Sup. Ct. Nov. 20, 2014); *In the Matter of Belmont Sav. Bank*, CIF. No. 11-2774, Assurance of Discontinuance (Mass. Sup. Ct. July 28, 2011).)

WOMEN AND INFANTS HOSPITAL

For example, in 2014, the Massachusetts Attorney General brought an enforcement action against The Women and Infants Hospital in Rhode Island (WIH). This enforcement action is a significant example of the Massachusetts Attorney General's enforcement actions because it demonstrates the intent to pursue cross-border enforcement of the Massachusetts Regulation and to enforce HIPAA.

In this enforcement action, the Massachusetts Attorney General alleged that WIH failed to secure and then report the loss of personal information and protected health information of over 12,000 Massachusetts residents contained on 19 lost unencrypted backup tapes.

As part of its settlement, WIH agreed to, among other things:

- Take certain steps to comply with the Massachusetts Regulation and HIPAA, including encrypting, erasing, or destroying all personal information or protected health information on unencrypted portable devices to the extent technically feasible.
- Continue to develop, implement, maintain, and adhere to a WISP under the Massachusetts Regulation.
- Maintain an inventory of all paper and unencrypted electronic media containing personal information and protected health information.
- Obtain certain assurances when using a third party to dispose of electronic media containing personal information or protected health information.

- Engage in an independent third-party audit of its compliance with HIPAA and the Massachusetts Regulation and to take certain recommended corrective measures.
- Pay $150,000, including $110,000 in civil penalties, $25,000 for attorney's fees and costs, and $15,000 for an education fund for use by the Massachusetts Attorney General to promote education about protecting personal information and protected health information and a fund for future data security litigation.

(*Commonwealth v. Women and Infants Hospital*, CIF No. 14-2332G, Consent Judgment (Mass. Sup. Ct. Jul. 22, 2014).)

01-17