Security Standards: Mapping Massachusetts Regulations to HIPAA

Massachusetts has recently become the first state to mandate that those storing personal information of residents of Massachusetts comply with specific security practices as required under 201 CMR § 17.00. These standards go into effect on January 1, 2010. The following is an analysis of how the Massachusetts legislation lines up with the existing HIPAA security standards that are described in detail in 45 CFR § 164 as promulgated in 2003 and effective in 2005.

Scope

Section 17.01(2) applies the Massachusetts regulations to any persons that "own, license, store, or maintain personal information about a resident of the Commonwealth." 201 C.M.R. § 17.01(2). The HIPAA security regulations apply to "covered entities," which are health plans, clearinghouses, and health care providers that transmit health information in electronic form. 45 C.F.R. § 164.104. The HIPAA security regulations are national in scope, but limited to health care entities, where the Massachusetts regulations apply to any entity that may store personal information on a resident of Massachusetts. Section 17.02 defines "personal information" as a Massachusetts resident's first and last name, or first initial and last name, in combination with a social security number, driver's license number, or financial account number. 201 C.M.R. § 17.02. The HIPAA security regulations are applicable to "protected health information," which is defined as "individually identifiable health information." This definition has been interpreted to include a patient's name, social security number, date of birth, and other patient identifiers, along with clinical diagnostic information or other data that might be stored in a health care provider's records related to patient care. 45 C.F.R. § 160.103. The information to be protected by the two regulatory schemes is overlapping but distinguishable; the Massachusetts regulations are aimed at protecting financial information like credit card account numbers, where HIPAA is aimed at protecting health information. However, an health care provider that provides services to Massachusetts residents would be obligated to comply with both regulatory programs.

Designee to Maintain Security Program Section 17.03(3)(1) requires that an employee be designated to maintain the security program of the organization. 201 C.M.R. § 17.03(3)(1). The HIPAA security regulations require that a person be designated who is responsible for developing organizational policies to support compliance. 45 C.F.R. § 164.308(a)(2).

Risk Assessment Section 17.03(3)(2) requires a risk assessment of security risks to both paper and electronic systems containing personal information. 201 C.M.R. § 17.03(3)(2). The HIPAA security regulations require that a risk analysis and risk management process be implemented at the covered entity. 45 C.F.R. § 164.308(a)(1)(ii).

Policy on Information Transport Off Business Premises Section 17.03(3)(3) requires the development of an organizational policy on the transport of personal information off business premises. 201 C.M.R. § 17.03(3)(3). There is no specific provision under the HIPAA security regulations that would require a specific policy on transporting protected health information.

Disciplinary Policy Section 17.03(3)(4) requires the imposition of a disciplinary policy for violations of the security program. 201 C.M.R. § 17.03(3)(4). The HIPAA security regulations

require that a sanction policy be developed for violations of the security policies of the covered entity. 45 C.F.R. § 164.308(a)(1)(ii)(C).

Terminated Staff Section 17.03(3)(5) requires that the security access of terminated staff be immediately terminated through a deactivation of the user's account. 201 C.M.R. § 17.03(3)(5). The HIPAA security regulations require that a procedure be implemented to terminate access for separated staff, but the regulation does not require "immediate" termination of access. 45 C.F.R. § 164.308(3)(ii)(C).

Third Party Service Providers Section 17.03(3)(6) requires that entity's that have personal information and relationships with third parties take measures to ensure third party compliance with the security regulations. 201 C.M.R. § 17.03(3)(6). The HIPAA security regulations require that covered entities enter into business associate contracts with third parties that may have access to electronic protected health information of the covered entity. See 45 C.F.R. § 160.103; 45 C.F.R. § 164.314(a). The American Recovery and Reinvestment Act of 2009 (ARRA) went further with regards to business associates; section 13401 requires that business associates specifically comply with the HIPAA security regulations found in 164.308, 164.310 and 164.312. ARRA § 13401.

Limiting Data Sets Section 17.03(3)(7) requires that the minimum data set be collected by an entity that collects personal information. 201 C.M.R. § 17.03(3)(7). The HIPAA security regulations do not specifically address this requirement.

System Identification Section 17.03(3)(8) requires that an entity identify what records or systems contain personal information, so that these records or systems can be handled in compliance with the security policies of the organization. 201 C.M.R. § 17.03(3)(8). The HIPAA security regulations do not specifically address, but such a system by system identification would likely occur within the risk analysis conducted by the covered entity under section 164.308(a)(ii)(A). 45 C.F.R. § 164.308(a)(ii)(A).

Physical Access Section 17.03(3)(9) requires reasonable restrictions on physical access to paper records to prevent unauthorized disclosure of personal information. 201 C.M.R. § 17.03(3)(9). The HIPAA security regulations do address physical access to the covered entity's facilities, but do not address how paper records should be secured. See 45 C.F.R. § 164.310.

Monitoring Section 17.03(3)(10) requires monitoring of the security program to ensure effectiveness. 201 C.M.R. § 17.03(3)(10). The HIPAA security regulations require regular monitoring of the security program to ensure that protected health information remains secure. 45 C.F.R. §§ 164.306(e), 164.316.

Review Section 17.03(3)(11) requires the at least annual review of the security program. 201 C.M.R. § 17.03(3)(11). The Massachusetts rules also contemplate review of the security program when an entity substantially materially changes its business practices. The HIPAA security regulations do not specify a minimum review period for the security programs of

covered entities, however, the typical practice for risk analysis and review is to conduct such a review on an annual basis. See 45 C.F.R. § 164.308(a)(ii)(A).

Documentation and Incident Reporting Section 17.03(3)(12) requires the documentation of an entity's response to security incidents. 201 C.M.R. § 17.03(3)(12). The HIPAA security regulations do require a covered entity to implement a policy for reporting and responding to security incidents, and the regulations provide for a requirement that activities taken under the security program be documented. 45 C.F.R. §§ 164.308(a)(6), 164.316.

Secure User Authentication Section 17.04(1) requires a detailed secure user authentication process that controls user logins, passwords, restricting access to only active users, and locking accounts after a number of unsuccessful login attempts. 201 C.M.R. § 17.04(1). The HIPAA security regulations address the issue of user authentication more generally by requiring that a policy be developed to grant access to users based on prior authorization. See 45 C.F.R. § 164.308(a)(4). In addition, the regulations require a policy on managing passwords, but are not specific on how the details of how passwords are to be managed or created. 45 C.F.R. § 164.308(a)(5)(ii)(D).

Access Control Section 17.04(2) requires a detailed access control process that restricts access to personal information and requires unique usernames and password combinations assigned to each user with access to personal information. 201 C.M.R. § 17.04(2). The HIPAA security regulations require unique user identification under section 164.312(a)(2)(i).

Encryption Section 17.04(3) requires the encryption of all personal information that is transmitted over a wireless or public network. 201 C.M.R. § 17.04(3). Section 17.04(5) specifically requires that personal information on laptops or other portable devices be encrypted. 201 C.M.R. § 17.04(5). The technical safeguards of the HIPAA security regulations address generally the need to encrypt electronic protected health information, but do not address specifically when this information must be encrypted. 45 C.F.R. § 164.312(a)(2)(iv). The transmission security section only requires that security measures be implemented to "guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network." 45 C.F.R. § 164.312(e). Wireless, however, is not specifically addressed in the HIPAA security regulations, as this technology was still nascent when the original regulations were written in the late 1990's. The HIPAA security regulations do not specifically require that the contents of laptops or other portable devices be encrypted.

Monitoring Section 17.04(4) requires monitoring of unauthorized access of systems. 201 C.M.R. § 17.04(4). The HIPAA security regulations also require the recording and examination of activity in information systems. 45 C.F.R. §§ 164.312(b), 164.308(5)(ii)(C).

Systems Connected to the Internet Section 17.04(6) requires a firewall and up-to-date operating system patches for any system connected to the internet that contains personal information. 201 C.M.R. § 17.04(6). The HIPAA security regulations do not address these specifics, though most security experts would agree that a firewall is a minimum security feature for controlling unauthorized access to protected systems from the internet. The issue of

operating system patches is not addressed either, but, at least for Windows systems, the patching of security threats is also now a minimum feature of any organizational network. Other operating systems and applications also regularly release patches that ought to be applied, but most of the game is in securing your Windows systems.

Anti-virus Software Section 17.04(7) requires up-to-date anti-virus software be in use. 201 C.M.R. § 17.04(7). The HIPAA security regulations also require some kind of protection from malicious software. 45 C.F.R. § 164.308(5)(ii)(B).

Education Section 17.04(8) requires education and training on best security practices for all personnel that use information systems. 201 C.M.R. § 17.04(8). The HIPAA security regulations require that covered entities provide security awareness training for all staff in the organization, and require "periodic security updates." 45 C.F.R. § 164.308(a)(5).

Summary

Much of the Massachusetts requirements for personal information correspond to the protections mandated under the HIPAA security regulations, however, there are some specific threats which have occurred more recently that the Massachusetts regulations respond to, particularly laptop and portable device security, and the specific and ongoing threat to Windows-based computer systems. Need help managing your technical security? Give us a call for help.