

**Understanding Massachusetts Law 201 CMR 17.00  
and  
How SkyView Partners' Products can Help**  
*by Carol Woodbury*

A data protection law out of Massachusetts has far-reaching affects - even if your organization doesn't reside in Massachusetts. Like the original breach notification law out of California, you only have to have one database entry containing personal information for a Massachusetts resident for your organization to be required to comply with this data protection law.

This law is unique because, unlike most data protection laws which are fairly vague about how the data is protected, this U. S. state law outlines specific protection requirements. Europe has been ahead of the United States with their data protection laws. But even the EU Data Protection Directive does not list how or dictate the methods for protecting personal data. While not as detailed as the Payment Card Industry's Data Security Standard (PCI DSS), this law has specific protection requirements with which organization's must comply. In addition, the state's breach notification law (Massachusetts General Law 93H) allows for civil penalties – up to \$5,000 for each violation and up to \$50,000 for each instance of improper disposal of personal data. These civil penalties can also be applied to this law. It is anticipated that other states and or a federal law will be passed. The deadline for compliance is January 1, 2010.

Let's take a closer look at 201 CMR 17.00

First we need to understand how the law defines personal information. Personal information is defined as:

“a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such resident:

- 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 resident's financial account”

With the caveat that:

- “personal information” does not include information that is “lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.”

Point one of 201 CMR 17.03 states:

“Every person that owns, licenses, stores or maintains personal information about a resident of the Commonwealth shall develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information. Such comprehensive information security program shall be reasonably consistent with industry standards, and shall contain administrative, technical, and physical safeguards to ensure the security and confidentiality of such records. “

SkyView Tip:

A once a year effort to clean-up systems to prepare for an audit is not sufficient. A formal security program is required and the issue needs to be addressed in an ongoing fashion. I call this a “compliance lifestyle.”

###

Point two of 201 CMR 17.03 says that there are considerations that should be taken when evaluating compliance with this law:

“...shall be evaluated taking into account:

- the size, scope and type of business of the person obligated to safeguard the personal information under such comprehensive information security program
- the amount of resources available to such person
- the amount of stored data
- and the need for security and confidentiality of both consumer and employee information.”

###

Using the words of the law itself, let's examine the minimum requirements of this information security program. I'm including general compliance tips as well as tips for utilizing the SkyView products to reduce the cost and complexities of complying with this Massachusetts law. Here's a description of the SkyView products:

**[Risk Assessor for IBM i and i5/OS](#)** is an IBM i and i5/OS security diagnostic tool that compares your security configuration against security best practices. Risk Assessor examines more than IBM i and i5/OS 100 "risk points" including system values, user profile settings, object level authorities, TCP/IP configuration, and more. Risk Assessor provides easy-to-read reports that allow you to easily determine where your systems' security configuration deviates from security best practices. In addition, Risk Assessor provides a comprehensive analysis guide which includes an explanation of the best practices settings and recommendations for IBM i

**[Policy Minder for IBM i and i5/OS](#)** is an IBM i and i5/OS security compliance tool that compares your systems' current settings against your organization's security policy requirements. Your policy implementation is documented and non-compliant items are identified. Using the FixIt function, non-compliant items can be set back to match policy settings. Policy Minder automates the process of keeping your IBM i and i5/OS security configuration in compliance with your security policy.

Point three of 201 CMR 17.03 states:

“...every comprehensive information security program shall include, but shall not be limited to:”

1. Designating one or more employees to maintain the comprehensive information security program

SkyView Partners' (SVP) Tip: Someone within the organization must be the owner of the security program. In other words, one would expect them to see this security program as part of someone's job description and results as a part of their performance review.

2. Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to:

- ongoing employee (including temporary and contract employee) training

- employee compliance with policies and procedures
- means for detecting and preventing security system failures

SVP Tip: At a minimum, a recurring risk assessment across the entire organization is required. Note that the assessment includes paper records containing personal data. Many laws just cover electronic information. In addition, an employee awareness program is not only required by this and other laws and regulations, it makes business sense to mobilize your entire workforce, making security everyone's responsibility.

Use SkyView Risk Assessor to perform the risk assessment on your IBM i (i5/OS) systems.

3. Developing security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises.

SVP Tip: Simply put, this requirement mandates that data be classified and, as part of the classification, that the appropriate use of the data be defined. In other words, organizations need a definition of personal data, along with the definition of how and by whom the data can be used. All employees then need to be educated so that there's a clear understanding of the requirements for use and handling of this type of data.

4. Imposing disciplinary measures for violations of the comprehensive information security program rules.

SVP Tip: Part of a security policy defines the ramifications of not following the policy. This is a reminder to make sure your policies have clear ramifications defined, that everyone to which the policy applies understands the ramifications and that the organization is willing to carry out the ramifications when necessary. If the ramifications are defined but are not carried out when a violation occurs, then there is no motivation for employees to comply with the policies.

5. Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.

SVP Tip: Immediate removal of access from terminated employees is probably something you've already implemented as this is clearly a case of following security best practices. Make sure that you handle, not just electronic access, but that you also revoke physical access to your facilities.

Use SkyView Policy Minder to easily set multiple profiles to status of \*DISABLED, remove their password, remove group assignments and/or set special authorities to \*NONE. Policy Minder will keep records of these changes so you have the proof these changes were made in a timely manner.

6. Taking all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such personal information in the manner provided for in 201 CMR 17.00; and taking all reasonable steps to ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required to be applied to personal information under 201 CMR 17.00.

SVP: Outsourcing is a fact of life in today's world. If your organization is using outsourced services and they have access to personal data, you will want to make sure they are (at least) complying with these requirements or have even more stringent data protection measures in place. You don't want your service provider to be the "weak link" in protecting your organization's data.

7. Limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limiting the time such information is retained to that reasonably necessary to accomplish such purpose; and limiting access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.

SVP Tip: While this requirement makes sense, many organizations fail to implement it. For example, I see organizations continue to ask for a social security number when they have no business requirement simply because they have always asked for it. In addition, I consistently see organizations retain information long after it's required to do so. Finally, many organizations do not limit access to data to only those users with a business justification.

Use SkyView Policy Minder to implement a policy that limits access to personal data as well to perform regular compliance checks to ensure it remains secured appropriately.

8. Identifying paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information.

SVP Tip: Without a doubt I believe that most organizations will be shocked at how far the use of personal data has spread. Many – perhaps even most – of the time, the data has been spread because it's in a file with other data that is required. Rather than subset the information, the entire file is copied to another file, saved, printed with the rest of the file contents, sent to a file server, propagated to a data warehouse, etc. It's been my experience that the scope of a project to secure data can be greatly reduced if unnecessary use or propagation of the data is stopped.

9. Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers.

SVP Tip: The emphasis of protecting data in recent years has centered around electronic storage of personal information. While this has been necessary, one cannot forget the plethora of places where the information is physically viewable – employment applications, insurance forms, printed reports, faxes, copies and even old microfiche!

10. Regular monitoring to ensure that the comprehensive information security program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information; and upgrading information safeguards as necessary to limit risks.

SVP Tip: As an advocate of a security compliance "lifestyle" this requirement makes total sense. Unless you are regularly checking whether you are in compliance, it is my experience that organizations quickly slide out of compliance.

This is specifically what SkyView Policy Minder was created to do – perform regular compliance checks to ensure your organization remains in compliance with the security requirements for your IBM i and i5/OS systems.

11. 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.

SVP Tip: An annual assessment to make sure your policies and procedures continue to match your organization's requirements is essential. Otherwise, your organization or technology may have moved in a different direction and your policies will be missing key aspects, leaving your organization exposed.

This is specifically what SkyView Risk Assessor was created to do – perform a regular, unbiased, thorough security assessment of your IBM i (i5/OS) systems.

12. Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

SVP Tip: A security incident response plan is a vital part of all organization's security procedures. And many other laws and regulations including PCI DSS require that an organization have a formal security incident response plan. The last thing you want to be doing should a breach occur, is trying to determine who should be involved in the investigation and what information needs to be gathered. The team and a formal plan of action needs to be formulated *before* a breach occurs.

###

Now let's take a look at the Computer System Security Requirements of this law, providing translation into IBM i and i5/OS terms.

(1) Secure user authentication protocols including:

- control of user IDs and other identifiers

SVP Tip: Ensure your policy requires that users not share their passwords and that shared profiles are not used anywhere in your organization.

- a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices

SVP Tip: Create user profiles with out a password (i.e., PASSWORD(\*NONE)) so that users must be assigned a password before then can sign on the system. When assigning the password, be sure to set the password to expired so that the user will have to change the password at first use.

- control of data security passwords to ensure that such passwords are kept in a location and/or format that does not compromise the security of the data they protect

SVP Tip: IBM i (i5/OS) stored user profile passwords in a one-way encrypted format, so you don't have to worry about the operating system. You main concern will be where

users keep their passwords. The key is to make the password composition rules complex enough to require strong passwords but not so complex that users are required to write down their passwords to remember them. You'll also want to make sure your employee policy states that passwords are not to be written down.

- restricting access to active users and active user accounts only  
SVP Tip: I find that many organizations lack an automated process for dealing with inactive users. Many i5/OS shops have, in the past, disabled profiles that were actually active. Therefore, they are hesitant to disable any profile. Other organizations do this process manually and have no automated process. SkyView's Policy Minder product looks at the right dates so that only profiles that are truly inactive are identified. In addition, it is quite simple to set up a process to automate dealing with inactive profiles. [Click here](#) to find out more.
- blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system

SVP Tip: Use the IBM i system value QMAXSIGN to control how many times a user is allowed to attempt to sign on the system before some action (controlled by the QMAXSGNACN system value) is taken. Best practices says that you allow 3-5 attempts for a user to come up with the right user profile / password combination and that you set QMAXSGNACN to 2 or 3 to ensure that the profile is set to status \*DISABLED.

(2) Secure access control measures that:

- restrict access to records and files containing personal information to those who need such information to perform their job duties; and  
SVP Tip: Restricting access to only those users with a business need demands that you implement object level security. This is the only method to ensure access is blocked to the general public (that is, \*PUBLIC authority is set to \*EXCLUDE) and the only users with access are granted authority. This method ensures that, regardless of the method that the data is accessed, the access controls are in place to appropriately secure the data.

Once you determine who should have access to the personal data, use SkyView Policy Minder to regularly monitor the access control settings to ensure access controls remain in compliance.

- assign unique identifications plus passwords, which are not vendor supplied default passwords, to each person with computer access, that are reasonably designed to maintain the integrity of the security of the access controls;

SVP Tip: User SkyView Risk Assessor or Policy Minder to regularly check for users with default passwords.

(3) To the extent technically feasible, encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly.

SVP Tip: IBM i and i5/OS has integrated capabilities to encrypt transmitted data via SSL. In addition, there are a number of vendors that provide encryption solutions to aide in this requirement.

(4) Reasonable monitoring of systems, for unauthorized use of or access to personal information

SVP Tip: IBM i and i5/OS has integrated auditing features that allow you to audit the access or attempted access of files containing personal information.

(5) Encryption of all personal information stored on laptops or other portable devices

SVP Tip: This requirement dictates the classification of data; otherwise, you will have to assume that all data downloaded or copied to a laptop must be encrypted.

(6) For files containing personal information on a system that is connected to the Internet, there must be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information.

SVP Tip: For data integrity, i5/OS must be running at QSECURITY level 40 or higher. While security patches are not prevalent on i5/OS, they do occasionally occur. Integrity PTFs should be loaded onto your system as soon as feasible after their release.

(7) Reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date patches and virus definitions, or a version of such 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.

SVP Tip: Malware and viruses are not typically an IBM i or i5/OS issue. (See the whitepaper Virus Got you Down?) However, you do want to ensure that you control what is restored onto your system. Setting the QALWOBJRST system value to \*ALWPTF, the QVfyOBJRST system value to '3' and QFRCCVNRST to '3' will help control what is restored onto your system.

Run SkyView Risk Assessor to understand the ramifications of setting these system values as well as other recommendations for ensuring a properly secured system.

(8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

SVP Tip: It's been my opinion that you should engage your entire workforce in battling the data protection war. An employee awareness program does this.

These are just some of the ways SkyView Partners' products can reduce the cost and complexities of maintaining your compliance requirements. For more information on SkyView Partners' solutions, please visit the SkyView Partners website at [www.skyviewpartners.com](http://www.skyviewpartners.com).

**Who is SkyView Partners?** SkyView Partners Inc. is a firm specializing in policy-based security compliance management and assessment software as well as security services for IBM i (AS/400 and iSeries) customers.

**Carol Woodbury** is President and co-founder. Carol has over 19 years experience in the area of security, 10 of which were as Chief Engineering Manager for Security for AS/40 (iSeries.) Carol is a world-renown speaker and writer on the topic of security.

*Disclaimer: Other steps may be necessary than what are described here to be in compliance with this law and/or to fully and appropriately secure personal and other information throughout your organization.*