



Massachusetts 201 CMR 17 Compliance for File Transfer

Trusted Strategies Whitepaper for Ipswitch

Massachusetts 201 CMR 17 Compliance for File Transfer

Abstract:

The Commonwealth of Massachusetts recently enacted a bill to protect the private information of Massachusetts residents even if that information is held by organizations outside the state. All U.S. organizations who have customers, clients, or employees who are Massachusetts residents are required to review current security practices, create and enact a plan to protect subject information and continuously monitor for breaches. Managing the transfer of files in compliance with the new law will require organizations to utilize a combination of identity checks, encryption, and reporting that can be found only in advanced file transfer solutions.

MA 201 CMR 17 is the Next Generation Regulation for Protecting Private Personal Information

The most recent and stringent state regulation to protect private information is attracting attention from commercial and public organizations across the United States. Known as “*Massachusetts State Law “201 CMR 17.00 - Standards for the Protection of Personal Information of Residents of the Commonwealth”*” this far-reaching law pertains to any individual or organization, commercial or public, that stores or utilizes private personal data of any Massachusetts resident, regardless of whether the organization is actually in Massachusetts. In general, the law requires protection consistent with applicable federal and industry security laws, such as the Gramm-Leach-Bliley Act (GLBA) and Payment Card Industry Data Security Standards (PCI-DSS).

The stated intent of the Massachusetts Privacy Law is to establish a minimum standard for the protection of Massachusetts resident’s personal information (PI) contained in both paper and electronic records. This baseline obviously provides a basis for lawsuits claiming negligence on the part of offending parties. Violators are required to notify both the Office of Consumer Affairs and Business Regulation (OCABR) and the Attorney General of breaches of private information, and may additionally be faced with a civil penalty of \$5,000 for each violation. Further, guilty parties are required to pay the reasonable costs of investigation and litigation of each such violation, including reasonable attorney’s fees.

MA 201 CMR 17 defines PI as a 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 the resident:

- Social Security number;
- driver’s license number or Massachusetts identification card number;

Massachusetts 201 CMR 17 Compliance for File Transfer

- 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; or
- a biometric indicator such as a fingerprint or retina scan file

Many believed initially that the law pertains only to companies that utilize private information relating to Massachusetts customers, clients, or patients such as credit files or medical records. However, because the law also applies to employee and 1099 contractors, most Massachusetts companies, and outside companies that do business in Massachusetts, will be subject to the requirements of MA 201 CMR 17. Despite allowing some latitude in how compliance is achieved according to the size of the organization and the amount of PI involved, the law makes no distinction about types of devices where private information is located – mainframe databases, laptops, servers, cloud applications, smart phones, and USB drives must all provide adequate protection. The law also applies equally to data at rest or in transit.

Electronic File Transfer and Compliance with MA 201 CMR 17

Although the law applies to information stored or transmitted on paper as well as electronically, this whitepaper will focus on the privacy issues associated with electronic file transfer. Electronic file transfer presents special compliance issues because:

1. Data is being moved from one source to potentially many other locations and different machines
2. Data flows are inherently harder to protect and control than data at rest
3. Not only must the data be fully protected while in transit, but the sender must ensure that the recipients are also in compliance with the regulations.
4. Complexities for compliance rapidly mount for organizations that routinely transfer hundreds or thousands of files daily both internally and externally.
5. Encryption and control technologies for data at rest are often very different from protection systems for data in transit; this can cause security gaps, performance problems, and management complexity
6. Keeping track of when files were transferred and to whom is by itself a daunting process, but the law also requires the ability to compile auditable reports of all file transfer activity

Massachusetts 201 CMR 17 Compliance for File Transfer

To address the issues for compliance that are associated with file transfers, we must first address the general requirements of the law and then look at the specific technical requirements:

Risk Assessment

The compliance process begins with a risk assessment to determine when personal information is collected, where it is stored, who has access to it, and how it is transferred for operational or archive purposes. This investigation process is frequently more difficult than it might seem at the outset because private information is often found in both structured and unstructured forms. For example, large organizations are almost certain to have multiple instances of structured private information on servers, databases, backup tapes, and off-site storage. But PI is also likely to be found in desktop PCs, notebooks, USB drives, CDs or DVDs, individual USB backup drives, and even employee's home PCs. Consequently, many organizations will find that unstructured PI frequently leaves the facility in the form of email or ad hoc ftp transfers. Further, small professional organizations frequently store private information that lies in unprotected devices and may be casually transmitted internally or externally with no controls or protection.

Restructuring Processes and Establishing Policies

Obviously, it is almost impossible to attain compliance with the Massachusetts privacy laws if personal information has been allowed to proliferate on many different devices and customarily moves around without adequate controls. So the risk review provides a good opportunity to fully reconsider how information flows within the organization and to then restructure the process for both greater efficiency and regulatory compliance. In fact, the regulation specifically requires "developing security policies for employees relating to the storage, access and transportation of records containing personal information outside of business premises."

All too often, however, written policies mandating complex procedures are routinely ignored as the emphasis inevitably returns to productivity. For example, employees may use email or ad hoc ftp sessions to transfer information if the "approved" file transfer system is too slow and cumbersome. In such cases, the organization should seriously consider updating the file transfer system to streamline production while simultaneously enabling the re-assertion of control according to the established policies.

Documenting the Security Program

Once the risk review has been completed and appropriate changes in policy and procedure instituted, the next step is to document the program. This written plan must document where personal information is used within the organization, who is authorized to use that data, and what procedures and technologies will be used to ensure confidentiality. This is

Massachusetts 201 CMR 17 Compliance for File Transfer

not a one-time effort; the written plan must be updated annually or whenever any material change is made to the program. In very small environments, this task might not be difficult. But in large organizations with sophisticated data flows, multiple locations, and many outside partners, this task could be extremely complex. Again, a comprehensive file transfer system that has already identified the data flows and the policies that are applied to each flow will be an invaluable aid to documenting the system for the purpose of proving compliance.

Monitoring the Security Program

The law further requires ongoing monitoring of the program 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.” Although the appropriate level of monitoring is deliberately left flexible, records must be kept to prove that adequate monitoring occurred. While this will inevitably require some level of administrative attention, the least expensive way to provide evidence of monitoring is to automatically generate log data as the data is accessed and transmitted. However merely collecting log data does not constitute monitoring; to be effective, logs must be consolidated and automatically passed through an analytical process that will generate alerts if anomalies are discovered. The ability to generate status reports that prove ongoing compliance could be crucial in the event of a security breach or regulatory review.

Ensuring compliance by service providers

Many organizations have traditionally outsourced a variety of functions including credit card processing, human resources administration, accounting, data archiving, data destruction, network administration, and network maintenance. More recently, software applications provided as a service (aka “cloud computing”) have become mainstream. The data flows associated with these services may well contain private information. The Massachusetts duty to protect such data includes “software as a service” providers and must become part of the contractual obligations. Unfortunately it is difficult to determine how data is actually processed internally by a service provider. The best technical means for ensuring compliance is to encrypt the data flows at the appropriate level of security which forces the service provider to have complementary security capabilities at the remote end.

Massachusetts 201 CMR 17 Compliance for File Transfer

File Transfer and Specific Security Requirements

Although most of MA 201 CMR 17 is fairly general in nature, section 4 of the legislation imposes specific technical security provisions. This section will identify the requirements which are applicable to the file transfer process and describe how the requirements could be met by a file transfer system.

The first set of specific requirements focuses on secure user authentication. The requirements are:

- a) control of user IDs and other identifiers;

This implies a system which checks the identities of users and prevents access by those without authorization. Further, the method by which user identities are issued and managed must be restricted to authorized administrators.

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

The law accepts passwords as the means of user authentication provided that policies requiring strong passwords are enforced. Such policies would normally specify the minimum length of passwords, their composition (letters, numbers, special symbols etc.), and how long a password can be used before it must be replaced. Obviously more robust forms of authentication using hardware are encouraged.

- c) 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;

Any access control system can be defeated if the passwords are not properly protected. A secure file transfer system must have a module that encrypts and stores passwords in an access-protected file separate from the private data. Further, when remote systems access protected data, only secure hashes of the password are transmitted, not the password itself.

- d) restricting access to active users and active user accounts only; and

This control requires identity authentication against a frequently updated list of authorized users. In addition to strong password policies, it is essential to immediately delete users that are no longer authorized. Maintaining a "whitelist" of approved IP addresses means that all others are considered potentially dangerous.

Massachusetts 201 CMR 17 Compliance for File Transfer

- e) blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

To prevent “brute force” attacks that automate the process of discovering passwords, the system must have the ability to react according to policy when a given number of unsuccessful login attempts occur. Policy options include locking the account until an administrator releases it, or progressively increasing the time interval required between attacks. These measures should be coupled with a secure password reset procedure for authorized persons who forget or mistype the password.

The second set of specific requirements focuses on access control measures that:

- (a) restrict access to records and files containing personal information to those who need such information to perform their job duties; and

This control requires a system that associates users with system privileges and enforces the authorization scheme. Ideally the system would employ an ascending set of privileges to separate people with low levels of responsibility from those with higher levels of trust.

- (b) 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

The intent of this requirement is to clearly identify human users and machines that access confidential data so that accountability is maintained and breaches can be traced. For example, the use of the factory supplied password for a given device is specifically prohibited. Instead, this control requires the use of passwords or ID certificates that are associated with a specific individual, and SSL (“secure sockets layer”) certificates for access by machines.

The third specific requirement is the “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.”

This control mandates the encryption of file transfers of any type that travel across public networks and/or are transmitted wirelessly. Obviously keeping the data encrypted before and after transmission would be the best way to meet the previously stated requirements for access controls.

Massachusetts 201 CMR 17 Compliance for File Transfer

Emails would be an obvious example of transport across public networks. Wireless file transfers such as an SMS text message show how problematic wireless transfers can become. Given the lack of uniform, compliant security methods for email and cell phones, organizations dealing with personal information should provide a suitable alternative system that provides the flexibility that employees need without creating risks and liability.

The fourth specific requirement calls for the continual monitoring of systems, for unauthorized use of, or access to, personal information.

Whatever file transfer system is used, there must be a log of all actions taken that will help administrators identify attempts to break in or take unauthorized actions. It is important that the log itself be protected from tampering so insiders cannot cover their tracks.

The fifth specific requirement is the “encryption of all personal information stored on laptops or other portable devices”.

Although this requirement deals only with data at rest, and not file transfers, it reveals the complexity of attaining full compliance. Data stored on devices can be encrypted at the file level or at the device level (a virtual drive or full hardware disk encryption). Either way, the data will likely need to be decrypted as it leaves the device and then re-encrypted for transit by the file transfer system.

Ipswitch File Transfer solutions enables organizations to move data in compliance with MA 201 CMR 17

The Ipswitch File Transfer portfolio of secure and managed file transfer solutions offers leading-edge security and encryption that is in full compliance with all applicable provisions of MA 201 CMR 17. Ipswitch File Transfer solutions give a global perspective of file transfers that allows management to set and enforce appropriate policies and to monitor the security of the system at all times. The value of Ipswitch File Transfer solutions becomes apparent when managers realize that uncontrolled data transfers are not only risky but frequently extremely inefficient. Using the advanced capabilities and flexibility of Ipswitch, workflow involving file transfers of almost any type of can be safely channeled through a fully compliant process. For example, instead of resorting to vulnerable email or instant messaging, employees can exchange data using the Ipswitch secure messaging service that encrypts everything end to end and logs every transaction.

Massachusetts 201 CMR 17 Compliance for File Transfer

The Ipswitch File Transfer portfolio comprises clients, servers, and workflow, both onsite and with hosted services, that are designed to interoperate securely and seamlessly. They share a host of security features that have already proven compliant with SOX, GLBA, Basel II, HIPAA, and PCI DSS. More specifically, these products collectively meet MA 201 CMR 17 requirements for:

- Encrypted storage of usernames, passwords and scripts, using FIPS-validated 256-bit key AES (Advanced Encryption Standard), the latest and strongest NIST and CSE-approved encryption
- End-to-end encrypted transfer of files via SSL (FTPS/HTTPS), SSH (SFTP) and EDIINT ASx protocols.
- Encrypted file storage using OpenPGP Module that enables unlimited automatic encrypt/decrypt and key management.
- Tamper evident cryptographic logging to a built-in database or Microsoft SQL server.
- File Non-Repudiation ensured by FIPS-validated SHA-1 hashing
- Authentication required for accessing administrative interface to protect tasks from unauthorized changes/usage.
- Secure communications between Ipswitch modules utilize industry-standard 128-bit key SSL encrypted TCP (not SNMP).
- Real-time monitoring of status and activity displays with comprehensive logging of all tasks

Summary

Massachusetts 201 CMR 17 represents one more step in the escalating regulation of private information at the state and Federal level. This law harmonizes state law with applicable Federal regulations but applies the requirements to small as well as large organizations, and extends the required protection outside of the Commonwealth. The complexities of maintaining control and confidentiality of private information during file transfer operations makes compliance with the law daunting without a well conceived security plan and a file transfer system that specifically supports the privacy law requirements. The Ipswitch suite of file transfer products enables organizations to automate and streamline file transfer workflow while simultaneously applying security policies and meeting all relevant Massachusetts 201 CMR 17 requirements.

Massachusetts 201 CMR 17 Compliance for File Transfer

About Ipswitch File Transfer

Ipswitch File Transfer is a global technology provider that builds solutions to securely move your valuable data. We enable companies and people to better manage their data interactions when visibility, management and enforcement matter. Our managed file transfer solutions deliver the control necessary to enable governance and compliance for our more than 40 million global users – including the majority of Fortune 1000 enterprises and government agencies. These organizations trust Ipswitch File Transfer solutions to secure, manage, automate and streamline their critical and highly sensitive file transfers and data workflows. Learn more at www.ipswitchFT.com or to contact us at www.ipswitchFT.com/company/contact.aspx, on [LinkedIn](#) or [Twitter](#).