Automation Suite for 201 CMR 17.00 Compliance

201 CMR 17.00 Compliance Assurance with LogRhythm

The Massachusetts General Law Chapter 93H regulation 201 CMR 17.00 was enacted on March 1, 2010. The regulation was developed to safeguard personal information of residents of the commonwealth of Massachusetts. The regulation applies to all organizations (companies or persons) that own or license personal information about Massachusetts residents. All affected organizations must develop, implement and maintain an auditable comprehensive written information security program containing administrative, technical and physical safeguards. The security program must meet industry standards for confidentiality and security to protect Massachusetts residents' personal information in both paper and electronic form from threats to security, integrity and unauthorized access.

The organization's security program must designate specific employees to oversee and manage the security procedures in the organization and perform continuous monitoring to address security issues. The program should include access policies to address specific employee access to and the transportation of personal information, along with the disciplinary actions for employees who do not conform to the requirements. The plan must also limit the collection of personal information to the minimum required based on appropriate intended use.

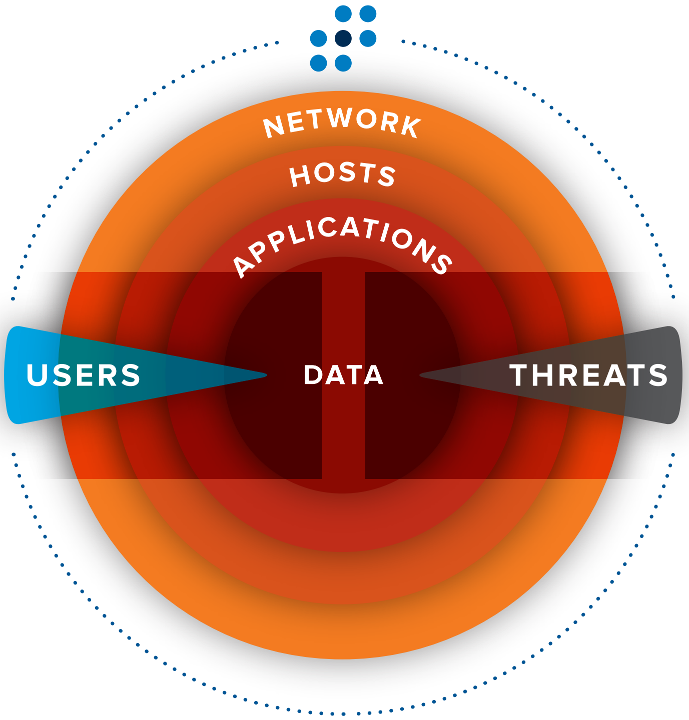
The collection, management and analysis of log data are integral to meeting 201 CMR 17.00 audit requirements. IT environments include many heterogeneous devices, systems and applications that all report log data. Millions of individual log entries can be generated daily, if not hourly. The task of simply assembling this information can be overwhelming in itself. The additional requirements of analyzing and reporting on log data render manual processes or homegrown remedies inadequate and costly.

LogRhythm has extensive experience in helping organizations improve their overall security and compliance posture while reducing costs. Log collection, archive and recovery are fully-automated across the entire IT infrastructure. LogRhythm automatically performs log data categorization, identification and normalization to facilitate easy analysis and reporting. LogRhythm's best-of-breed log management capabilities enable automatic identification of the most critical events and notification of relevant personnel through its powerful alarming capabilities.

LogRhythm provides out-of-the-box 201 CMR compliance support. As part of the 201 CMR 17 Compliance Module, enterprise assets are divided into three categories: access control, file integrity monitoring and security systems. LogRhythm's extensive support for both commercial and custom applications enables comprehensive and efficient collection, processing, review and reporting of all log sources specified in 201 CMR security program requirements.

To ensure compliance with 201 CMR 17 requirements, information systems and applications are monitored in real-time. AI Engine Rules, Alarms, Investigations, Reports, reporting packages, and tails are provided. They allow for immediate notification and analysis of conditions that impact the integrity of the organization's customer data. Areas of non-compliance can be identified in real time. Reports can be generated as needed or scheduled to run at pre-determined intervals via reporting packages. Additionally, the 201 CMR package elements are provided as part of LogRhythm's standard Knowledge Base to further augment the usefulness of the log data.

Protecting Critical Information



The following table outlines the 201 CMR 17 requirements LogRhythm either directly meets or provides support for the testing process. The requirements listed come directly from the 201 CMR 17 documents located at the Commonwealth of Massachusetts Government web site (http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf).

201 CMR Control Requirement	Directly Meets Requirements	Augments Control Process
17.03: Duty to Protect and Standards for Protecting Personal Information	17.03.2.b, 17.03.2.b.3, 17.03.2.h, , 17.03.2.j	17.03.2.e
17.04: Computer System Security Requirements	17.04.4	17.04.1.d, 17.04.1.e, 17.04.2.a, 17.04.2.b, 17.04.3, 17.04.6, 17.04.7

The tables on the subsequent pages outline how LogRhythm specifically supports requirements of the 201 CMR sections. The "How LogRhythm Supports Compliance" column describes the capabilities LogRhythm provides that will meet, support or augment 201 CMR 17 compliance.

17.03: Duty to Protect and Standards for Protecting Personal Information

LogRhythm provides monitoring of critical resources for security related events, critical errors, and unauthorized access.

Compliance Requirements		How LogRhythm Supports Compliance
17.03.2.b	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.	LogRhythm provides direct support for 201 CMR 17 control requirement 17.03.2.b by centrally collecting, monitoring, and analyzing security events from IDS/IPS systems, A/V systems, firewalls, and other security devices across the organization. LogRhythm reports provide evidence of security events (activity, attack, compromise, denial of service, malware, misuse, reconnaissance, suspicious, and vulnerability) and system critical/error conditions.
17.03.2.b.3	Means for detecting and preventing security system failures.	LogRhythm provides direct support for 201 CMR 17 control requirement 17.03.2.3.b by centrally collecting, monitoring, and analyzing system error conditions from devices across the organization. LogRhythm reports provide evidence of system critical/error conditions.
17.03.2.e	Preventing terminated employees from accessing records containing personal information.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.03.2.e by collecting access control log messages. LogRhythm reports provide evidence of unauthorized access, access granting/revocation, account enabling/disabling, and account locking/unlocking for terminated/disabled accounts.
17.03.2.h	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.	LogRhythm provides direct support for 201 CMR 17 control requirement 17.03.2.h by collecting logical access control log messages. LogRhythm reports provide evidence of authorized/unauthorized logical access such as access/authentication successes/failures.
17.03.2.j	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.	LogRhythm provides direct support for 201 CMR 17 control requirement 17.03.2.j by completely automating the process of recording responsive actions taken. LogRhythm reports provide details of all alarms affecting selected systems, lists events, notifications, and response activity associated with each alarm.

17.04: Computer System Security Requirements

LogRhythm provides monitoring of critical systems for unauthorized access, unencrypted communication, software updates, antivirus activity, and signature updates.

Compliance Requirements		How LogRhythm Supports Compliance
17.04.1.d:	Restricting access to active users and active user accounts only.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.1.d by collecting access control log messages. LogRhythm reports provide evidence of unauthorized access, access granting/revocation, account enabling/disabling, account locking/unlocking, and account creation/deletion.
17.04.1.e	Blocking access to user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.1.d by collecting access control log messages. LogRhythm reports provide evidence of account enabling/disabling and account locking/unlocking.
17.04.2.a	Restrict access to records and files containing personal information to those who need such information to perform their job duties.	LogRhythm provide direct support for 201 CMR 17 control requirement 17.04.2.a by providing details of file integrity activity via LogRhythm's File Integrity Monitor Agent. LogRhythm's File Integrity Monitor can be configured to monitor key file or directory activity, deletions, modification, and permission changes. The file integrity capability is completely automated, the agent can be configured to either scan for files/directory changes on a schedule or the kernel level driver can automatically detect file integrity activity in real-time.
17.04.2.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.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.2.b by collecting access control log messages. LogRhythm reports provide evidence of unauthorized access, access granting/revocation, account enabling/disabling, and account locking/unlocking for vendor default accounts.
17.04.3	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.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.3 by collecting electronic access point device log messages (firewalls, VPN servers, networking devices, etc.). LogRhythm reports provide evidence of allowed/denied ingress/egress network communications including source/destination IP/port.
17.04.4	Reasonable monitoring of systems, for unauthorized use of or access to personal information.	LogRhythm provides direct support for 201 CMR 17 control requirement 17.04.4 by collecting logical access control log messages. LogRhythm reports provide evidence of authorized/unauthorized logical access such as access/authentication successes/failures.
17.04.6	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.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.6 by collecting system log messages related to firewall configuration and software updates. LogRhythm reports provide evidence of software patch failures/successes and host firewall critical/error/information conditions.
17.04.7	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.	LogRhythm provides supplemental support for 201 CMR 17 control requirement 17.04.7 by collecting log messages from antivirus software and other anti-malware tools. LogRhythm reports provide evidence of antivirus activity, malware infections, and signature update failures/successes.