* 1. **Mass 201 CMR 17.00**

|  |  |  |  |
| --- | --- | --- | --- |
| **Mass 201 CMR 17.00 Requirement** | **Reporting Instruction** | **Assessor’s Response** | **Control Effectiveness** |
| **17.03: Duty to Protect and Standards for Protecting Personal Information** | | | | |
| **17.03(1)** | | | | |
| Develop, implement, maintain, and monitor a comprehensive, written information security program applicable to any records containing personal information. Such comprehensive information security program must be reasonably consistent with industry standards, and must contain administrative, technical, and physical safeguards to ensure the security and confidentiality of personal information. | **Identify the documented information security policy** examined. |  |  | |
| **Describe how** the information security policy was examined to verify that it is published and disseminated to: | |  | |
| All relevant personnel. |  |
| All relevant vendors and business partners. |  |
| **17.03(3)(a)** | | | | |
| Designate one or more employees to maintain the comprehensive information security program. | **Identify the personnel** designated to maintain the comprehensive information security program. |  |  | |
| **17.03(3)(b)** | | | | |
| Identify and assess 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:   1. ongoing employee (including temporary and contract employee) training; 2. employee compliance with policies and procedures; and   means for detecting and preventing security system failures. | **Describe how** it was verified that an annual risk-assessment process is documented that: | |  | |
| * Identifies critical assets, threats and vulnerabilities. |  |
| * Results in formal, documented analysis of risk. |  |
| **17.03(3)(c)** | | | | |
| Develop 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. | **Identify** **the documented policy to control distribution of media** that was reviewed to verify the policy covers all distributed media, including that distributed to individuals. |  |  | |
| **Describe how** media distribution is controlled, including distribution to individuals. |  |
| **17.03(3)(d)** | | | | |
| Impose disciplinary measures for violations of the comprehensive information security program rules. | **Identify the policies** and procedures that Impose disciplinary measures for violations of the comprehensive information security program rules. |  |  | |
| **17.03(3)(e)** | | | | |
| Prevent 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. | **Identify** **the sample** of users terminated in the past six months selected. |  |  | |
| **Describe how** the current user access lists for ***local access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **Describe how** the current user access lists for ***remote access*** were reviewed to verify that the sampled user IDs have been deactivated or removed from the access lists. |  |
| **17.03(3)(f)** | | | | |
| Take all reasonable steps to verify that any third-party service provider with access to personal information has the capacity to protect such 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. | **Identify the documented policies and procedures to manage service providers with whom confidential data is shared, or that could affect the security of confidential data**, reviewed to verify policy defines the following:   * Maintain a list of service providers. * Maintain a written agreement that includes an acknowledgement that the service providers will maintain all applicable PCI DSS requirements to the extent the service provider handles, has access to, or otherwise stores, processes, or transmits the customer’s confidential data or sensitive authentication data, or manages the customer's confidential data environment on behalf of a customer. * Ensure there is an established process for engaging service providers including proper due diligence prior to engagement. * Maintain a program to monitor service providers’ PCI DSS compliance status at least annually. * Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity. |  |  | |
| **17.03(3)(g)** | | | | |
| Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected; limit the time such information is retained to that reasonably necessary to accomplish such purpose; and limit access to those persons who are reasonable required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements. | **Identify the document** that gives procedures on limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected |  |  | |
| **17.03(3)(h)** | | | | |
| Identify paper, electronic and other records, computer 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. | **Identify** **the data-flow diagram**(s) examined. |  |  | |
| **Identify** **the responsible personnel** interviewed for this testing procedure. |  |
| For the interview, **summarize the relevant details discussed** to verify the diagram: | |
| * Shows all confidential data flows across systems and networks. |  |
| * Is kept current and updated as needed upon changes to the environment. |  |
| **17.03(3)(i)** | | | | |
| Reasonably restrict 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 store such records and data in locked facilities, storage area or containers. | **Identify the documented procedures for protecting confidential data** reviewed to verify controls for physically securing all media are defined. |  |  | |
| *For all types of media used,* **describe the controls** for physically securing the media used. |  |
| **17.03(3)(j)** | | | | |
| Regularly monitor 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 upgrade information safeguards as necessary to limit risks. | **Identify the documented security policies and procedures** examined to verify that procedures define reviewing the following at least daily, either manually or via log tools:   * All security events * Logs of all system components that store, process, or transmit CHD and/or SAD * Logs of all critical system components * Logs of all servers and system components that perform security functions. |  |  | |
| **17.03(3)(k)** | | | | |
| Review 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. | **Identify** any security measures reviewed or assessed internally or by an auditor. |  |  | |
| **17.03(3)(l)** | | | | |
| Document responsive actions taken in connection with any incident involving a breach of security, and perform a post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information. | **Identify the documented policy** reviewed to verify that processes are defined to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |  | |
| **Identify the sample of responsible personnel** interviewed who confirm that processes are implemented to modify and evolve the incident response plan:   * According to lessons learned. * To incorporate industry developments. |  |
| **Describe how** it was observed that processes are implemented to modify and evolve the incident response plan: | |
| * According to lessons learned. |  |
| * To incorporate industry developments. |  |
| **17.04: Computer System Security Requirements** | | | | |
| **17.04(1)** | | | | |
| Secure user authentication protocols including:  (a) control of user IDs and other identifiers;  (b) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies, such as biometrics or token devices;  (c) control of data security passwords to ensure that such passwords are kept in a safe location and/or format that does not compromise the security of the data they protect;  (d) restrict access to active users and active user accounts only;  (e) block access to user identification after multiple unsuccessful attempts to gain access or the limitation places on access for the particular system. | **Identify** **the written procedures for user identification management** examined to verify processes are defined for each of the items below:   * Assign all users a unique ID before allowing them to access system components or confidential data. * Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. * Immediately revoke access for any terminated users. * Remove/disable inactive user accounts at least every 90 days. * Manage IDs used by vendors to access, support, or maintain system components via remote access as follows: * Enabled only during the time period needed and disabled when not in use. * Monitored when in use. * Limit repeated access attempts by locking out the user ID after not more than six attempts. * Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID. * If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session. |  |  | |
| **17.04(2)(a)** | | | | |
| Restrict access to records and files containing personal information to those who need such information to perform their job duties. | **Identify** **the selected sample** of roles for this testing procedure. |  |  | |
| *For each role in the selected sample***, describe how** the role was examined to verify access needs for each role are defined and include: | |
| * System components and data resources that each role needs to access for their job function. |  |
| * Identification of privilege necessary for each role to perform their job function. |  |
| **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. | **Identify** **the responsible administrative personnel** interviewed for this testing procedure. |  |  | |
| For the interview, **summarize the relevant details discussed** to confirm that all users are assigned a unique ID for access to system components or confidential data. |  |
| **17.04(3)** | | | | |
| To the extent technically feasible, encrypt all transmitted records and files containing personal information that will travel across public networks, and encrypt all data containing personal information to be transmitted wirelessly. | **Identify** all locations where confidential data is transmitted or received over open, public networks. |  |  | |
| **Identify** **the documented standards** examined. |  |
| **Describe how** the documented standards were examined and compared to system configurations to verify the use of: | |
| * Security protocols observed in use |  |
| * Strong cryptography for all locations |  |
| **17.04(4)** | | | | |
| Reasonably monitor systems, for unauthorized user of or access to personal information. | **Identify the responsible personnel** interviewed who confirm the following are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including:   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |  | |
| **Identify the sample of audit logs** observed to verify the following are logged:   * All individual access to confidential data. * All actions taken by any individual with root or administrative privileges. * Access to all audit trails. * Invalid logical access attempts. * Use of and changes to identification and authentication mechanisms, including.   + All elevation of privileges.   + All changes, additions, or deletions to any account with root or administrative privileges. * Initialization of audit logs. * Stopping or pausing of audit logs. * Creation and deletion of system level objects. |  |
| **17.04(5)** | | | | |
| Encrypt all personal information stored on laptops or other portable devices. | **Indicate whether** disk encryption is used. **(yes/no)** |  |  | |
| *If “yes,” complete the remainder.*  *If “no,” mark the remainder as “Not Applicable.’* | |
| **Describe** the disk encryption mechanism(s) in use. |  |
| *For each disk encryption mechanism in use*, **describe how** the configuration was inspected and the authentication process observed to verify that logical access to encrypted file systems is separate from the native operating system’s authentication mechanism. |  |
| **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. | **Identify** **the documented policies and configuration standards** that define the following:   * Firewall software/hardware is required for all devices (containing personal information) that connect to the Internet when outside the network, and which are also used to access the network. |  |  | |
| **17.04(7)** | | | | |
| Implement 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. | **Describe how** anti-virus configurations, including the master installation of the software, were examined to verify anti-virus mechanisms are: | |  | |
| * Configured to perform automatic updates, and |  |
| * Configured to perform periodic scans. |  |
| **17.04(8)** | | | | |
| Educate and train all employees on the proper use of the computer security system and the importance of personal information security. | **Identify the documented security awareness program** reviewed to verify it provides awareness to all personnel about the importance of confidential data security. |  |  | |