## Mass 201 CMR 17.00

|  |  |  |  |
| --- | --- | --- | --- |
| Section | Control Description | Control Effectiveness | Notes |
| 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. |  |  |
| 17.03(3)(a) | Designate one or more employees 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 3. means for detecting and preventing security system failures. |  |  |
| 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. |  |  |
| 17.03(3)(d) | 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 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. |  |  |
| 17.04(2)(a) | Restrict access to records and files containing personal information to those who need such information to perform their job duties. |  |  |
| 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. |  |  |
| 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. |  |  |
| 17.04(4) | Reasonably monitor systems, for unauthorized user of or access to personal information. |  |  |
| 17.04(5) | Encrypt all personal information stored on laptops or other portable devices. |  |  |
| 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. |  |  |
| 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. |  |  |
| 17.04(8) | Educate and train all employees on the proper use of the computer security system and the importance of personal information security. |  |  |