

Section 17.03: (2)

DUTY TO PROTECT AND STANDARDS FOR PROTECTING PERSONAL INFORMATION

“Without limiting the generality of the foregoing, every comprehensive information security program (WISP) shall include but not be limited to the following ten (10) elements”

STEP	201CMR17	Regulatory Requirement
1	Section 17.03: (2) (a)	designating one or more employees to maintain your WISP
2	Section 17.03: (2) (b)	performing an internal and external risk assessment of your current information security program’s procedures for safeguarding personal information stored in paper and electronic form, and evaluating and implementing improvements for securing personal information
3	Section 17.03: (2) (c)	developing or amending security policies for storage, access and transportation of records containing PI outside of business premises
4	Section 17.03: (2) (d)	imposing disciplinary measures for violations your WISP’s rules
5	Section 17.03: (2) (e)	preventing terminated employees from accessing PI
6	Section 17.03: (2) (f)	overseeing third-party providers contract(s) for maintaining appropriate security measure for PI consistent with the regulations
7	Section 17.03: (2) (g)	restricting physical access to records containing PI and storage of such PI in locked facilities
8	Section 17.03: (2) (h)	monitoring your WISP to insure that is operating as planned to safeguard your PI
9	Section 17.03: (2) (i)	reviewing the scope of security measures, at least, annually or whenever there has been a material change in your business practices that reasonably impact the security or integrity of records containing PI and making adjustments to your WISP as necessary
10	Section 17.03: (2) (j)	documenting responsive actions taken in connection with any incident involving breach of security

SECTION 17.04:

COMPUTER SYSTEMS SECURITY REQUIREMENTS

“Every person who owns or licenses personal information about a resident of the Commonwealth and electronically stores or transmits such information shall include in its written, comprehensive information security program the establishment and maintenance of a security system covering its computers, including any wireless system, that, at a minimum, and to the extent technically feasible, shall have the following (8) elements”

STEP	201CMR17	Regulatory Requirement
1	Section 17.04: (1)	implementing secure user authentication protocols
2	Section 17.04: (2)	implementing secure user access control measures
3	Section 17.04: (3)	encrypting transmitted records and files containing PI across public networks or wirelessly
4	Section 17.04: (4)	reasonable monitoring of systems for unauthorized use or access to PI
5	Section 17.04: (5)	encrypting all PI stored on laptops or other portable devices
6	Section 17.04: (6)	reasonably up-to-date firewall protection and operating system security patches for maintaining the integrity PI
7	Section 17.04: (7)	reasonably up-to-date version of system security agent software which must include malware and virus protection and set to receive security updates on a regular basis
8	Section 17.04: (8)	educating and training employees in the proper use of the computer security system and the importance of PI security