201 CMR 17.00 Certification Program

201 CMR 17.03
Duty to Protect PI

- *Develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards.*
- *Designate one or more employees to maintain the comprehensive information security program.*
- *Identify and assess internal and external risks to the security, confidentiality, and integrity of any electronic, paper or other records containing personal information.*
- *Evaluate and improve the effectiveness of current safeguards.*
- *Ongoing employee (including temporary and contract employee) training.*
- *Ensure employee compliance with policies and procedures.*
- *Implement means for detecting and preventing security system failures.*
- *Develop security policies and procedures relating to the handling, storing, accessing and transporting PI.*
- *Requiring third-party service providers by contract to implement and maintain appropriate security measures.*

- ***Information Gathering and Analysis*** – Review of any existing documentation such as internal policies and procedures, provider agreements, and security awareness training programs.
- ***PI Discovery and Data Mapping*** – Discover electronic & paper based personal information within the environment via questionnaires, interviews, operational observations and e-discovery.

- ***Identifying Vulnerable Access Points*** – Identify access points in and out of your environment and determine the security posture of those access points.
- ***GAP Analysis and Remediation Recommendations*** – Prioritize the risks, offer recommendations for remediation, and execute on the implementation of the solution.
- ***Verification of Remediation Recommendations*** – Review of solutions implemented to alleviate against potential risks and ensure their alignment with the 201 CMR 17.00.

- ***Employee Training and Certification Program –*** A comprehensive web based training program focused on personal information protection and overall staff security awareness.
- ***WISP and Digital Framework Implementation*** – Development of your Written Information Security Program and supporting documentation to create a complete digital framework of policies, processes, and procedures to support regulatory compliance.
- ***Executive Review*** – An executive summary of current policies, the gaps identified during our analysis, and strategic recommendations for the continuous improvement of the security program.

- ***Safe Side Certification*** – Letter certifying your organization has implemented security best practice policies, processes, and procedures in compliance with the 201 CMR 17.00.

Why Safe Side Compliance?

Partnering with SSC will provide you with the "industry standard". Our knowledge transfer at project completion imparts Fortune 1000 organizational and security practices utilized by the SSC team. By choosing to work with SSC, you will have the best technologists at your side to meet all of your security, compliance, and assessment challenges.