

Comprehensive Written Information Security Program (WISP)

Gap Analysis

- Do you have a comprehensive, written information security program (WISP) applicable to all records containing personal information (PI) about a resident of Massachusetts?
- Does the WISP include administrative, technical and physical safeguards for PI protection?
- Have you designated one or more employees to maintain and supervise WISP implementation and performance?
- Have you identified the paper, electronic and other records, computing systems, and storage media, including laptops and portable devices, that contain personal information?
- Have you identified and evaluated reasonably foreseeable internal and external risks to paper and electronic records containing PI?
- Have you evaluated the effectiveness of current safeguards?
- Does the WISP include regular ongoing employee training, and procedures for monitoring employee compliance?
- Does the WISP include disciplinary measures for violators?
- Does the WISP include policies and procedures for when and how records containing PI should be kept, access or transported off your business premises?
- Does the WISP provide for immediately blocking terminated employees' physical and electronic access to PI records (including deactivating their passwords and user names)?
- Do you have in place a procedure for documenting any actions taken in connection with any breach of security; and does that procedure require post-incident review of events and actions taken to improve security?