Massachusetts Business PII Security Program Requirement

The Commonwealth of Massachusetts has a **Comprehensive Written Information Security Program** also known as **WISP**. This program seeks to address the management of **Personally Identifiable information** in your organization.

SaviorLabs wants you to know that in Massachusetts is it important for organizations to understand their legal responsibility to managing the security of information. It is **critical that you have developed written policies to ensure your organization can meet these regulations** (201 CMR 17.00). Additionally, you need to have written policies that outline how you will validate your compliance with these policies. We can help!

Key point: Create a written policy right now!

Handling "personally identifiable information"

- ☐ Do you have a **comprehensive, written policy applicable to all records containing personally identifiable information** ("PII") about a Massachusetts resident?
- ☐ Does your policy include **administrative, technical, and physical safeguards** for PII protection?
- ☐ Have you **designated employees** to maintain and supervise your policy implementation and performance?
- ☐ Have you **identified** paper, **electronic and other records**, computing systems, and storage media, including laptops and portable devices that **contain personal information**?
- ☐ Maybe just **treat all your records as if they all contained PII?**
- ☐ Have you **identified** and evaluated **reasonably foreseeable** internal and external **risks** to paper and electronic records containing PII?
- ☐ Have you **evaluated** the **effectiveness of current safeguards**?
- ☐ Does your policy include **regular ongoing employee training**, and procedures for **monitoring** employee **compliance**?
- ☐ Does your policy include policies and procedures for when and **how records** containing PII should be kept, accessed or **transported off** your business **premises**?
- ☐ Does your policy provide for **immediately blocking terminated employees**, physical and electronic access to PII records (including deactivating their passwords and user names)?
- ☐ Have you taken **reasonable steps to** select and **retain a third-party service provider** capable of **maintaining appropriate security measures** consistent with 201 CMR 17.00?
- ☐ Have you **contracted with third-party service providers to implement and maintain such appropriate security measures**?
- ☐ Is the amount of **PII** that you have collected **limited to the amount reasonably necessary** to accomplish your legitimate purposes, or to comply with state or federal regulations?
- ☐ Does your policy **specify restrictions for physical access to PII** records?
- ☐ Do you **store your records** and data containing PII **in locked facilities**, storage areas or containers?

- ☐ Is access to PII records **limited to those persons who have a need to know** in connection with your legitimate business purpose, or to comply with regulations?
- ☐ Is the **length of time that you are storing PII records** limited to the time reasonably necessary to accomplish your legitimate business purpose or to comply with regulations?
- ☐ Do you have a process for **regularly monitoring** to ensure that your policy is operating in a reasonably calculated manner to prevent unauthorized access to or unauthorized use of PII; and for upgrading it as necessary?
- ☐ Are your **security measures reviewed at least annually**, and whenever there is a material change in business practices that may affect the security or integrity of PII records?
- ☐ Do you have in place a **procedure for documenting any actions taken in connection with any breach of security**; does that procedure require post-incident review of events and actions taken to improve security?
- ☐ Does your policy include **disciplinary measures for violators**?

Additional Requirements for Electronic Records

So, did you just read the previous checklist and thought you were all set? Not so, electronic records have even more specific requirements!

- ☐ Do you have in place **secure authentication protocols** that provide for:
  - ☐ **Control** of **user IDs** and other identifiers?
  - ☐ A reasonably **secure** method of assigning/selecting **passwords**, or use biometrics or token devices?
  - ☐ **Controlling passwords** such that they are kept in a location and format that does not compromise the security of the data they protect?
  - ☐ **Restricting access** to PII to active users and active user accounts?
  - ☐ **Blocking** access **after multiple** unsuccessful access **attempts**?
- ☐ Do you have **secure access control measures** that restrict access, on a **need-to-know basis**, to PII records and files?
- ☐ Do you, to the extent technically feasible, **encrypt all PII** and files that are transmitted across public networks or wirelessly?
- ☐ Do you **assign unique identifications plus passwords** (not default passwords) to each person with computer access; are those IDs and passwords reasonably complex to maintain the security of those access controls?
- ☐ Do you, to the extent technically feasible, **encrypt all PII stored on laptops or other portable devices**?
- ☐ Do you have **monitoring** in place to **alert** you to the occurrence of **unauthorized use** or access to PII?
- ☐ On any system that is connected to the Internet, do you have **up-to-date firewall protection**; and **operating system security patches**?
- ☐ Do you have up-to-date versions of **system security agent software** (including malware protection) and **up-to-date security patches and virus definitions**?
- ☐ Do you have in place **training for employees** on the proper use of computer system security, and the importance of PII security?

Call SaviorLabs
978-223-2959
We can help!