The Top 10 Things to Know About Information Security Programs

By Steven J. O'Neill, Attorney at Law (September 1, 2009)

10 **Got PI?** According to a new Massachusetts security breach law, if your organization owns, licenses, stores or maintains any Personal Information ("PI") concerning a Massachusetts resident in paper or electronic form, you must implement a comprehensive Written Information Security Program ("WISP") by January 1, 2010.

9 **What is PI?** PI exists in nearly every organization. In fact, it takes only three ingredients to make PI in Massachusetts: 1) first and last name or first initial and last name; 2) of a Massachusetts resident; PLUS 3) some identifying information such as a credit card number, a social security number, a drivers license ID number, a state-issued ID card, a credit/debit card number, a financial account number or similar identity information. This definition does not require that the PI holder have any password or security code associated with the financial account in order for the information to qualify as PI. Even a simple personal check or employee information could constitute PI.

8 **What else does the new law require?** Massachusetts and Nevada now have the two most comprehensive state laws concerning identity theft. Previously, identity theft laws merely required notifications after security breaches. In addition to the new requirement of a WISP, Massachusetts already requires that when a holder of PI knows or has reason to know of a security breach, the holder must notify the resident, the Attorney General and the Director of the Office of Consumer Affairs and Business Regulations ("OCABR") in writing. Another section of the new law regulates the destruction of electronic and paper documents containing PI. This article is focused on the substantial new WISP regulations contaned in 201 CMR 17.00.

7 **Who is required to create a WISP?** The new Massachusetts law is national in scope and impact. Ostensibly the law applies to all legal entities holding Massachusetts PI, whether located in Massachusetts or not; most state entities are covered by Executive Order 504.

6 **What should be in a WISP?** The new Massachusetts regulations (201 CMR 17.00) dictate compliance standards for a comprehensive Written Information Security Program. Although creation of a WISP is mandatory for all persons and entities holding PI, the regulations recognize that different organizations present different risk profiles. The regulations provide a flexible basis for evaluating whether a covered entity is in compliance with the standards. The evaluation takes into account, "(i) the size, scope and type of business of the person obligated to safeguard the personal information under such [a] comprehensive information security program, (ii) the amount of resources available to such person, (iii) the amount of stored data, and (iv) the need for security and confidentiality of both consumer and employee information." The high profile security breaches at TJX (2007 approx. 94,000,000 records) and Hannaford Supermarkets (2008 approx. 4,200,000 records) were not avoided by a simple data breach notification law. See http://datalossdb.org for updated listings. It is logical that larger holders present greater risk to the public and will be held to higher standards.

5 **Compliance Standards.** Notwithstanding the flexibility allowed in evaluating compliance, the regulations mandate 12 compliance standards:

1) designating one or more employees to maintain and supervise WISP implementation and performance;

2) identifying and assessing reasonably foreseeable internal and external risks to paper and electronic records; evaluating and improving current safeguards for limiting such risks including ongoing training, developing employee procedures and means for detecting and preventing security breaches;

3) developing security policies for employees (including temporary and contract employees) that take into account when and whether PI should be transported;

4) imposing disciplinary measures for the violation of the comprehensive WISP;

(continued)

About the Author

Steven J. O'Neill is an experienced litigator with extensive knowledge of computer data systems architecture, electronic records issues and eDiscovery law. He has presented numerous seminars on these topics throughout the U.S. His practice areas include business law, litigation and technology law focusing on eDiscovery, Document Retention Compliance and Information Security Compliance. He is admitted to practice in state and federal court in MA and CT and available to serve clients nationally.

Law Offices of Steven J O'Neill

888.766.3455 Phone
888.766.6040 Fax

soneill@attorneyoneill.com

attorneyoneill.com

5) preventing terminated employees from accessing PI immediately upon separation;

6) taking all reasonable steps to verify that third party service providers with access to PI have the capacity to comply with the regulations; and taking all reasonable steps to ensure that third party service providers actually apply protective security measures at least as stringent as the regulations;

7) limiting the amount of PI collected to that reasonably necessary to accomplish legitimate purposes; limiting the time that PI is held; and limiting access, "to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements";

8) identifying paper, electronic and other records/documents, computer systems, data storage systems and portable devices containing PI unless the WISP provides that all information shall be treated as if it contained PI;

9) imposing restrictions on physical access to records including, "a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data in locked facilities, storage areas or containers;"

10) regular monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of PI; and upgrading information safeguards as necessary to limit risks;

11) reviewing 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 PI; and

12) documenting responsive actions taken in connection with any incident involving a breach of security; mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of PI.

4 **Encryption Requirements.** The regulations expressly require the, encryption of, "all personal information stored on laptops or other portable devices," and reasonable levels of encryption in other circumstances. See e.g., 201 CMR 17.04(5). The risk of a security breach related to PI stored on portable computer devices is very high. For example, on February 6, 2009 Kaiser Permanente reported that 29,500 records in a computer file were lost or stolen. This breach followed a July 27, 2006 incident where Kaiser Permanente reported that 160,000 records containing PI were on a stolen laptop. The regulations state only that encryption is, "the transformation of data through the use of an algorithmic process, or an alternative method at least as secure, into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation by the Office of Consumer Affairs and Business Regulation." Until specific standards are issued by OCABR, such technology decisions should reference industry technical standards and best practices.

3 **Legal Standards and Best Practices.** The Massachusetts Office for Consumer Affairs and Business Regulation ("OCABR") provides information to guide the creation of a WISP. In addition to official publications, professional legal and technical guidance is advisable. For example, instituting new employee disciplinary or termination measures will require advice concerning employment law together with changes in policies and employment manuals. Contracts with vendors having access to PI should be reviewed. Especially in the event of a data security breach, which requires notification of the Attorney General, you may be required to justify that all steps taken to secure PI were reasonable under the circumstances. The ability to document that the assessment and implementation process followed legal guidelines and best practices will strengthen your defense. In general, an organization actively pursuing the implementation of a standards based Document Retention Policy will not find the development of a WISP to be particularly burdensome.

2 **Technical Standards and Best Practices.** The regulations require that the comprehensive Written Information Security Program (WISP) be developed with reference to technical standards and best practices. Program safeguards should also be consistent with safeguards required by federal and other regulations governing similar classes of Personal Information. For example, the U.S. Department of Commerce National Institute of Standards and Technology ("NIST") publishes a number of guidelines such as the NATIONAL CHECKLIST PROGRAM FOR IT PRODUCTS. NIST Special Publication 800-70 (September 2007 Draft). It states that, "[a]lthough the solutions to IT security are complex, one simple yet effective tool is the security configuration checklist. . . A security configuration checklist (also referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is essentially a document that contains instructions or procedures for configuring an IT product to an operational environment. . . Using well-written, standardized checklists can reduce the vulnerability exposure of IT products and be particularly helpful to small organizations and individuals in securing their systems." (footnote omitted). Additional sources of information include: SANS S.C.O.R.E.; RFC; OWASP; ISSA, Generally Accepted Information Security Principles; ISO 27002; and the PCAOB Auditing Standard No. 2 for SOX compliance. Because of the wide range and complexity of technical configurations, a comprehensive listing of sources of technical guidance is beyond the scope of this article. A qualified IT security consultant will be familiar with the technical options.

1 **Enforcement.** The security breach law is enforced by the Attorney General using the regular remedies provided by the Consumer Protection Act. The available remedies include temporary restraining orders or preliminary or permanent injunctions and a civil penalty of not more than five thousand dollars for each violation. In addition, payment of the reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees may be required. The new law does not provide a private right of action based on violation of its terms. Whether PI security breaches amount to an independent violation of the Consumer Protection Act or other laws is beyond the scope of this article.