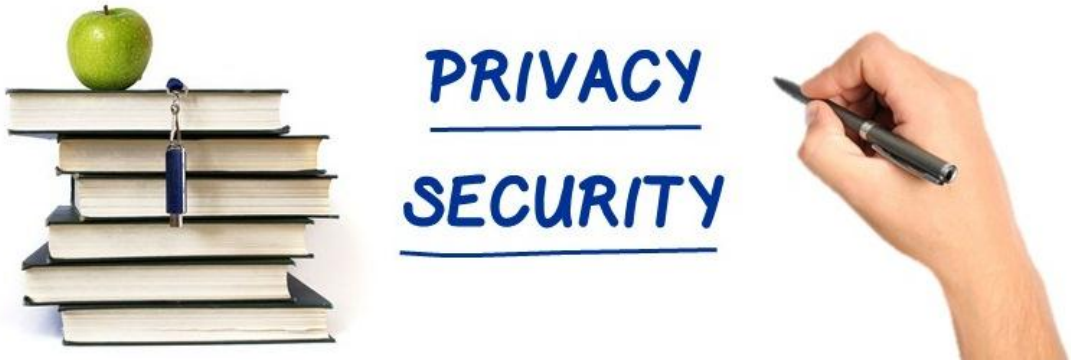

A LIST OF PRIVACY AND DATA SECURITY TRAINING REQUIREMENTS

HIPAA Privacy and Security Rules

HIPAA's Privacy and Security Rules have extensive training requirements. HIPAA requires a covered entity to train all workforce members on its policies and procedures with respect to PHI. Each new workforce member must be trained within a reasonable period of time after hiring. Thereafter, training must be given whenever there is a material change in policies or procedures. Covered entities and business associates must provide a security awareness and training program for all workforce members. This program must include periodic security updates.

Policies and Procedures Training Requirements
45 CFR § 164.530(b)(1)

45 CFR § 164.530 Administrative requirements.

(b) (1) *Standard: Training.* A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information required by this subpart and subpart D of this part, as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity.

(2) *Implementation specifications: Training.*

(i) A covered entity must provide training that meets the requirements of paragraph (b)(1) of this section, as follows:

(A) To each member of the covered entity's workforce by no later than the compliance date for the covered entity;

(B) Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the covered entity's workforce; and

(C) To each member of the covered entity's workforce whose functions are affected by a material change in the policies or procedures required by this subpart or subpart D of this part, within a reasonable period of time after the material change becomes effective in accordance with paragraph (i) of this section.

(ii) A covered entity must document that the training as described in paragraph (b)(2)(i) of this section has been provided, as required by paragraph (j) of this section.

Security Awareness Training Requirements
45 CFR § 164.308(a)(5)

45 CFR § 164.308 Administrative safeguards

(a) A covered entity or business associate must, in accordance with § 164.306:

(1)(i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations. . . .

(5)(i) Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).

(ii) Implementation specifications. Implement . . . (A) Security reminders (Addressable). Periodic security updates.

Gramm-Leach-Bliley Act (GLBA)

Training under GLBA is required via its Safeguards Rule, 16 CFR 314.4. The training requirement is rather vague, but interagency guidance recommends that organizations should: "Train staff to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling; Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about computer security; and Train staff to properly dispose of customer information."[1]

GLBA Safeguards Rule, 16 CFR 314.4

(b) Identify reasonably foreseeable internal and external risks . . . including (1) Employee training and management.

[1] http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm.

Payment Card Industry Data Security Standard (PCI-DSS)

PCI-DSS is a code developed by the credit card industry's PCI council. It has a number of requirements regarding privacy training.

PCI-DSS 12.6 – Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

PCI-DSS 12.6.1 – Educate personnel upon hire and at least annually.

PCI-DSS 12.6.1.a – Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web based training, meetings, and promotions).

PCI-DSS 12.6.1.b – Verify that personnel attend awareness training upon hire and at least annually.

PCI-DSS 12.6.2 – Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually that they have read and understand the information security policy.

PCI-DSS 12.9.4 – Verify through observation and review of policies that staff with responsibilities for security breach response are periodically trained.

FACTA – FTC Red Flags Rule

Under the FACTA, which amended the Fair Credit Reporting Act, the FTC established the Red Flags Rule, which requires training as part of an Identity Theft Prevention Program. See 16 CFR 681.1(d)-(e). Staff should be trained about the various red flags to look out for, and/or any other relevant aspect of the organization's Identity Theft Prevention Program.

16 CFR 681.1 - Duties regarding the detection, prevention, and mitigation of identity theft

(d) Establishment of an Identity Theft Prevention Program—

> (1) Program requirement. Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

(e) Administration of the Program. Each financial institution or creditor that is required to implement a Program must provide for the continued administration of the Program and must:

. . .

(3) Train staff, as necessary, to effectively implement the Program . . . .

Texas Health Privacy Law

Section 181.101 of the Health and Safety Code, as amended by HB 1609 and effective June 14, 2013, requires training about both the state's law and HIPAA. This law is one of the few state health laws that mandates training about the state's own health privacy law. Additionally, it mandates training about HIPAA. Penalties for violating the Texas law are equivalent to HIPAA's, so they are quite high.

Section 181.101. Training Required

(a) Each covered entity shall provide training to employees of the covered entity regarding the state and federal law concerning protected health information as necessary and appropriate for the employees to carry out their duties for the covered entity.

(b) An employee of a covered entity must complete training described by Subsection (a) not later than the 180th day after the date the employee is hired by the covered entity.

(c) If the duties of an employee of a covered entity are affected by a material change in state or federal law concerning protected health information, the employee shall receive training described by Subsection (a) within a reasonable period, not to exceed one year, after the material change becomes effective.

(d) A covered entity shall require an employee of the entity who is trained as described by Subsection (a) to sign, electronically or in writing, a statement verifying the employee's completion of training. The covered entity shall maintain the signed statement for six years.

Massachusetts Data Security Law

Massachusetts's Data Security Law, at 201 CMR 17.03, requires training as mandatory for maintaining a comprehensive information security program. Training should focus on reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information. Training must be "ongoing" and must be given for not only permanent employees but also temporary and contract employees.

201 CMR 17.03: Duty to Protect and Standards for Protecting Personal Information

(1) Every person that owns or licenses personal information about a resident of the Commonwealth shall develop, implement, and maintain a comprehensive information security program. . . .

(2) Without limiting the generality of the foregoing, every comprehensive information security program shall include, but shall not be limited to:

> (b) Identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and evaluating and improving, where necessary, the effectiveness of the current safeguards for limiting such risks, including but not limited to: 1. ongoing employee (including temporary and contract employee) training . . . .

17.04: Computer System Security Requirements

Every person that 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 elements: . . .

> (8) Education and training of employees on the proper use of the computer security system and the importance of personal information security.

Federal Information Security Management Act (FISMA)

FISMA, 4 U.S.C. § 3544, requires federal agencies to establish a security awareness training program. The program must include contractors and "other uses of information systems" that support the agency. The program must address information security risks and each employee's responsibilities in complying with agency policies and procedures to minimize security risks.

(b) Agency program.--Each agency shall develop, document, and implement an agencywide information security program . . . to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

> (4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of—
>
> (A) information security risks associated with their activities; and
>
> (B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

EU-US Safe Harbor Arrangement

Proper training is necessary for a company to self-certify compliance with the Safe Harbor requirements to the Department of Commerce. There isn't much guidance about the specifics of such training, but it should logically focus on ensuring compliance with the Safe Harbor principles.

The US DOC states in its Safe Harbor Workbook that:

> Under the self-assessment approach, verification would indicate that an organization's published Safe Harbor privacy policy is accurate, comprehensive, prominently displayed, completely implemented, accessible, and conforms to the Safe Harbor Privacy Principles. It would also need to indicate that appropriate employee training, as well as internal procedures for periodic, objective reviews of compliance are in place.

The DOC guide to self-certification echoes this requirement:

> Under the self-assessment approach, such verification would have to indicate that an organization's published privacy policy regarding personal information received from the EU is accurate, comprehensive, prominently displayed, completely implemented and accessible. It would also need to indicate that its privacy policy conforms to the Safe Harbor Principles; that individuals are informed of any in-house arrangements for handling complaints and of the independent mechanisms through which they may pursue complaints; that it has in place

procedures for training employees in its implementation, and disciplining them for failure to follow it; and that it has in place internal procedures for periodically conducting objective reviews of compliance with the above.

ISO/IEC 27002

The International Standards Organization (ISO)'s Information Security standard ISO/IEC 27002:2005 is one of the most frequently followed standards by organizations throughout the world. The standard provides guidance on information security management in organizations, and it contains a requirement that all employees receive data security awareness training.

Section 8.2.2 Information Security Awareness, Education, and Training

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

Personal Information Protection and Electronic Document Act (PIPEDA)

Principle 4.1.4 of PIPEDA, Canada's broadly-applicable privacy law, requires training about the "organization's policies and practices" related to complying with PIPEDA.

Principle 4.1.4

Organizations shall implement policies and practices to give effect to the principles, including . . . (c) Training staff and communicating to staff information about the organization's policies and practices.