



HUMAN RESOURCES
LAW AND ADVOCACY

A Model for Achieving Reasonable Data Security through Information and Instruction

The provision of reasonable information and instruction to an organization's employees and other agents is an important part of a robust data security program.

The following checklist provides organizations with "best practices" guidelines for the information and instruction component of a complete data security program.

1. **Maintain a comprehensive training program and policy that features:**

- Mandatory pre-access training
- Mandatory annual re-training
- Assigned responsibility for:
 - content development
 - content delivery
 - documentation of attendance
 - enforcing compliance with the attendance requirement
- Training content that encompasses:
 - relevant orders guidelines, fact sheets and best practices issued by privacy regulators
 - evolving industry standards and best practices
 - the implementation of new technologies
 - any amendments to applicable legislation
 - new or amended privacy policies, procedures and practices

- recommendations arising from privacy and security audits, privacy impact assessments and investigation into privacy complaints, privacy breaches and information security breaches
- Training materials that include detailed information in relation to the following:
- the purposes for which employees and agents are permitted to collect, use and disclose personal health information and any limitations imposed
 - the privacy policies, procedures and practices and the obligations imposed on agents by these policies, procedures and practices
 - the obligations, if any, of employees and other agents, including for example the duty to report “incidents”
 - the potential consequences that may be imposed with respect to the collection, use or disclosure of personal information in contravention of applicable legislation and/or privacy policies, procedures and practices
 - the potential organizational consequences for the same
- 2. Maintain a communications program that is detailed in a privacy awareness program policy that features:**
- A commitment to maintaining a communication program to periodically remind agents of relevant security policies, procedures and practices as well as their obligations under applicable legislation
 - A commitment regarding the frequency, method and nature of the awareness communications to be delivered
 - Assigned responsibility for implementation of the program
 - A pledge of confidentiality policy applicable to all employees and other agents, requiring compliance with legislation and the company's policies with respect to information management
- 3. Administer a system login notice that:**
- Makes clear that certain uses are not permitted (and not merely that certain uses are permitted)
 - Features a pre-access acknowledgement

For additional information, contact: Daniel Michaluk, Partner, Hicks Morley LLP at daniel-michaluk@hicksmorley.com or 416.864.7253.