



LiveDDM Solutions for PIPEDA Compliance

The Personal Information Protection and Electronic Documents Act (PIPEDA) mandates more electronic information storage and exchange along with innovative e-healthcare technology solutions, leaving healthcare organizations the challenge of securing information and maintaining strict levels of patient confidentiality---all while allowing easy access to authorized users.

This document provides a brief overview of PIPEDA requirements, LiveDDM and LiveChart dental information solutions and how these solutions help dentists meet PIPEDA requirements, while securing their networks for the future.

PIPEDA Overview

"Privacy is a right underpinning healthcare in Canada. The right is addressed in legislation, code of ethics, standards and procedures." (PIPEDA, January 2004)

PIPEDA promotes and enforces a unified privacy principle across Canada for federally regulated organizations (i.e. inter-provincial transport companies, banks, etc.). Based on the Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information and developed in conjunction with businesses and consumer organizations, PIPEDA's approach bridges the complex rules of the European Union and the self-regulatory approach of the United States.

On January 1, 2004 PIPEDA came into full effect, covering all collections, uses and disclosures of personal information in the course of commercial activity by most organizations---including healthcare organizations, defined as: "Any organization engaged in the planning, funding, management, manufacture, or delivery of health services and products."

PIPEDA holds organizations accountable for certain personal information in their custody and under their control, requiring reasonable limits on the collection, use, disclosure and retention of personal information. Access to an organization's policies and practices to regulated personal information.

PIPEDA Impact to Healthcare

PIPEDA provides assurances to the public, patients, and providers that personal health information will continue to be managed and shared confidentially and securely. The Canadian government believes PIPEDA's regulations will not significantly differ from those currently in place in the health sector. To make compliance valid, however, PIPEDA requires institutions to inform patients of their privacy rights.

PIPEDA Scope

PIPEDA does not apply to the entire Canadian health sector.

PIPEDA applies to the information collected, used, and disclosed in the course of commercial activities such as private pharmacies, laboratories, and healthcare providers in private practices.

PIPEDA does not apply to personal information in Provinces and Territories that have substantially similar privacy legislation in place covering commercial activities.

Non-Compliance

Failure to comply with the PIPEDA is risky.

For example, individuals, employees or patients have the ability to file a complaint with the privacy commissioner. If the dispute is not resolved, the individual may take it before the Federal Court, which can order an organization to correct its practices and award damages.

PIPEDA Requirements

The CSA Model Code outlines the following ten internationally recognized principals of fair information practices. They balance the privacy rights of individuals and the information requirements of private organizations.

1. **Accountability:** An organization is responsible for personal information under its control and shall designate an individual(s) accountable for the organization's compliance with the following principles.
2. **Identifying Purposes:** Identify the information's purpose before or while the information is collected.
3. **Consent:** The individual's knowledge and consent are required to collect, use, or disclosure personal information, except where inappropriate.
4. **Limiting Collection:** Personal information collected is limited to that necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention:** Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
6. **Accuracy:** Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.
7. **Safeguards:** Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

8. Openness: An organization shall make readily available specific information about its personal information management policies and practices.
9. Individual Access: Upon request, individuals shall be informed of the existence, use, and disclosure of personal information, and shall be given access to that information. An individual can challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance: An individual can challenge compliance with the above principles, by sending the complaint to the designated individual(s) accountable for the organization's compliance.

PIPEDA - #7. Safeguards

In order to comply with PIPEDA security standards, organizations must assess their current security practices and complete security provisions, including developing and implementing a security policy to protect personal health information. Resources to accomplish this exercise will vary substantially according to the organization size and structure.

For a sole practitioner's office, this could simply be a short document detailing provisions such as:

Physical measures (locked filing cabinets, restricting access to offices, alarm systems)

Technological tools (passwords, encryption, firewalls, anonymizing software)

Organizational controls (security clearances, staff training, confidentiality agreements)

As organizations grow in size and complexity, network security, remote access, access controls and data integrity play a much larger part of adhering to PIPEDA Safeguards. **For more information on PIPEDA, visit <http://www.strategis.ic.gc.ca>**

LiveDDM Dental Security Solutions

LiveDDM offers a broad range of easy-to-use, scalable and cost-effective dental security solutions based on industry standards---keeping your office mobile and productive, while meeting PIPEDA regulations. These robust solutions protect vital dental information on your networks, while allowing confidential information to flow easily and securely.

Software:

Microsoft Server 2003 and Windows XP both Password Protected for access
LiveDDM password protected access

LiveDDM biometric security access using fingerprint ID

LiveDDM Security access levels only allow specified users access only to what they are required to see

LiveDDM Activity Logs / Audit Trail

LiveDDM SQL single file, encrypted-password protected database designed by Microsoft for Accuracy, Speed and Security.

AntiVirus and AntiSpyware Software with AutoUpdates

Hardware:

Firewall/VPN protect the perimeter of your network by acting as a gateway against external attacks and allowing only acceptable traffic through. VPN (Virtual Private Network) provides secure, cost-effective connectivity between remote clinics physician offices, administration and hospitals, enabling confidential information to be accessed only by intended recipients.

Wireless networking solutions can offer unprecedented freedom and flexibility, mobilizing the workforce and bringing productivity applications closer to the point-of-care. LiveDDM solutions can use enhanced IPSec security, making them much more secure than the standard Wired Equivalent Privacy (WEP) encryption.

Anti-Virus (AV) Solutions keep healthcare organizations running while eliminating costly operational disruptions or shutdowns. AV provides client and server protection, blocking attacks and ensuring all users have the latest updates before logging on to the Internet.