



---

**PIPEDA AND THE PRIVACY ACT:  
ACHIEVING COMPLIANCE WITH  
CANADIAN REGULATIONS**

**A WHITE PAPER**

---



*March 31st, 2004*

---

## AUTHORS

This document was prepared by:

**Steve Pasquill, Managing Director**

**BearingPoint**

20 Bay Street, Suite 940

WaterPark Place

Toronto, ON M5J 2X9

Tel: 416-775-6200

E-mail: [steve.pasquill@bearingpoint.com](mailto:steve.pasquill@bearingpoint.com)

**Steve Lough, Senior Manager**

**BearingPoint**

20 Bay Street, Suite 940

WaterPark Place

Toronto, ON M5J 2X9

Tel: 416-775-6267

E-mail: [steve.lough@bearingpoint.com](mailto:steve.lough@bearingpoint.com)

This document is protected under the copyright laws of the Canada and other countries as an unpublished work. This document contains information that is proprietary and confidential to BearingPoint LP or its technical alliance partners, which shall not be disclosed outside or duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate BearingPoint LP. Any use or disclosure in whole or in part of this information without the express written permission of BearingPoint LP is prohibited.

© 2004 BearingPoint LP (Unpublished). All rights reserved.

---

## TABLE OF CONTENTS

<b>1. EXECUTIVE SUMMARY</b>	<b>1</b>
<b>2. CANADIAN PRIVACY LEGISLATION</b>	<b>2</b>
2.1 The Privacy Act of 1983.....	2
2.2 The Personal Information Protection and Electronic Documents Act (PIPEDA) of 2004.....	2
<b>3. BUSINESS IMPLICATIONS AND CHALLENGES</b>	<b>4</b>
<b>4. TECHNOLOGY IMPLICATIONS AND CHALLENGES</b>	<b>5</b>
<b>5. ACHIEVING COMPLIANCE</b>	<b>6</b>
<b>6. THE CENTERA CE SOLUTION FOR RECORDS MANAGEMENT</b>	<b>7</b>
6.1 Centera CE Overview — What it is.....	7
6.2 Centera CE Functionality — What it does .....	7
6.3 How it Works.....	9
<b>7. BEARINGPOINT ASSESSMENT AND ANALYSIS</b>	<b>10</b>
7.1 Analysis.....	10
7.2 The Authors .....	11



## 1. EXECUTIVE SUMMARY

The transition to an information-based economy in Canada requires increasing attention by both the public and private sector to compliance with evolving legislation and best practices related to the management and protection of information. In particular, privacy legislation has placed additional expectations on governments and companies to enhance the systems and solutions that they use for storage, retrieval, retention and management of electronic information about individuals. The Canadian Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA) have raised the level of public accountability significantly and therefore the need for compliance capability in the areas of storing personal information in a private and secure way.

The key implication of these developments is that organizations must now be able to demonstrate that they understand what personal information they have in their possession, that it was appropriately collected, and that it is being managed in accordance with the relevant legislation. In addition to making changes in their business practices, organizations need to establish and maintain information systems that facilitate efficient and effective compliance with the requirements of the legislation.

EMC<sup>2</sup> retained BearingPoint to conduct an independent and objective assessment of the Centera Compliance Edition relative to its ability to meet the evolving electronic records management requirements of these two pieces of legislation. This White Paper presents a brief summary of the legislative requirements, discusses the business and technical challenges that they present and provides comment on the ability of the EMC<sup>2</sup> Centera Compliance Edition to meet these requirements.

Based on our analysis of the requirements of the legislation and the functionality of EMC<sup>2</sup>'s Centera CE solution, it is the opinion of BearingPoint that Centera Compliance Edition, when configured and used in conjunction with a certified RMA application, has the ability to demonstrate legislative compliance for the personal information stored within the solution. It has the functionality and tools to be able to demonstrate and show an auditable history of compliance with the key aspects of the Privacy Act and PIPEDA., and can assist public and private sector organizations to meet the requirements of Canada's privacy legislation.

## 2. CANADIAN PRIVACY LEGISLATION

Over time, a variety of federal and provincial legislation and supporting government policies have defined the requirements for information management<sup>1</sup>, but in recent years two specific pieces of legislation have re-defined privacy requirements. The Privacy Act, which took effect on July 1, 1983 defined how governments must keep personal information private. The Personal Information Protection and Electronic Documents Act (PIPEDA) was enacted January 1st, 2001 and became fully operational on January 1, 2004. PIPEDA defines the personal information privacy requirements for private sector organizations. Both of these acts are based on a similar set of principles and expectations.

It is important to recognize that these acts not only govern personal information about a client or constituent, but also any personal information about individuals in the possession of an organization (e.g. suppliers, partners, employees, etc.).

### 2.1 The Privacy Act of 1983

This Act requires the Government of Canada and provincial governments, unless the individual province's legislation is even more comprehensive than the federal legislation, to manage the privacy of personal information by:

- , Limiting its collection of personal information to the minimum details needed to operate programs or activities;
- , Collecting the information, whenever possible, directly from the person concerned;
- , Informing the person why the information is being collected and how it will be used;
- , Using the information only for purposes specified, unless allowed by law;
- , Keeping the information long enough to allow the person a reasonable opportunity to obtain access;
- , Ensuring the information is as accurate, up-to-date and complete as possible; and
- , Disclosing personal information only when specifically allowed by the Privacy Act or another law.

### 2.2 The Personal Information Protection and Electronic Documents Act (PIPEDA) of 2004

This Act establishes ten principles<sup>2</sup> to govern the collection, use, and disclosure of personal information in both the public and private sectors. These principles were derived in part from the Organization for Economic Cooperation and Development's (OECD) privacy recommendations and they form part of the Canadian Standards Association's (CSA) Model Code for Protection of Personal Information. As such, they represent broad agreement on best practices in addition to specific legal requirements.

---

<sup>1</sup> Access to Information Act, National Archives of Canada Act, National Library of Canada Act, Canada Evidence Act, Financial Administration Act, Copyright Act, Criminal Records Act, Emergency Preparedness Act, Official Languages Act, Official Secrets Act, Security of Information Act, Statistics Act.

<sup>2</sup> Privacy Commissioner of Canada, Summary

*Figure 1: Ten Principles for the Protection Of Personal Information*

1. **Accountability:** An organization is responsible for personal information under its control and must designate an individual who is accountable for the organization's compliance.
2. **Identifying Purposes:** The purposes for which personal information is collected must be identified by the organization at or before the time the information is collected.
3. **Consent:** The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
4. **Limiting Collection:** The collection of personal information must be limited to that which is necessary for the purposes and must be collected by fair and lawful means.
5. **Limiting Use, Disclosure, and Retention:** Personal information must 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, and must be retained only as long as necessary for the fulfillment of those purposes.
6. **Accuracy:** Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. **Safeguards:** Personal information must be protected by security safeguards appropriate to the sensitivity of the information.
8. **Openness:** An organization must make information about its policies and practices relating to the management of personal information readily available to individuals.
9. **Individual Access:** Upon request, an individual must be informed of the existence, use, and disclosure of his or her personal information and must have access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. **Challenging Compliance:** An individual must be able to address a challenge concerning compliance with the above principles to the designated individual accountable for the organization's compliance.

### **3. BUSINESS IMPLICATIONS AND CHALLENGES**

The Privacy Act and PIPEDA raise the bar of accountability for the collection, storage, and protection of personal information. Public and private organizations must be able to clearly demonstrate their compliance with the various aspects of the Act relevant to them. These Acts both require organizations to designate a person or persons that will be held accountable for the management and protection of personal information.

To be able to definitively demonstrate that they are compliant with the relevant Acts, organizations will need to undertake several key initial activities. Firms must take an inventory of all the personal information they have stored to verify and be able to prove the following:

- , The information was collected correctly.
- , It is being used only for the purpose it was intended.
- , Its retention is known and there is a process executing and proving its destruction as appropriate.
- , It is being stored in a private and secure way.

Once this initial task is complete, organizations must manage the ongoing gathering, storing, correcting, and destroying of personal information in accordance with the legislation, and be able to demonstrate that this is occurring.

On an ongoing basis, it will be essential to know where all copies of the personal information are held in the organization. This will be necessary to respond to requests from the public to see their information, or for the information to be corrected or deleted as required. This will also facilitate giving appropriate and timely access to personal information by the people about whom the personal information is being collected. This will instill a sense of confidence in the organization's ability to manage this information.

A key aspect of both pieces of legislation, is the need for organizations to be able to designate a time limit for retention of personal information at the individual field and record level, and to alert management when information needs to be removed from storage or to provide alerts that allow sufficient time for new consents to be obtained. Multiple retention periods for a single piece of information may be necessary if the information is subject to multiple regulations, or if a retention period must be extended because a record is subject to a legal hold or a client access request.

In addition to the specific requirements above related to the legislation, information systems will need to control access to prevent against fraud and malicious, innocent or careless destruction of personal information.

---

## 4. TECHNOLOGY IMPLICATIONS AND CHALLENGES

In addition to the above business considerations, the privacy legislation also highlights some challenges in the technology environments of public and private sector organizations. Since the amount of personal information being collected and managed is increasing rapidly, the scalability of any solution or system will need to be addressed to make sure that it has the ability to grow rapidly while maintaining the proper management of the privacy and security of the personal information. This increase is, in part, due to the migration of information from forms and paper files to electronic media. This is further complicated by the evolution of the nature of electronic records being stored to now include images, sound, biometrics, etc., and the rapid change of the computing technologies employed.

Electronic records have moved from simple, text-based files to complex digital objects that contain embedded images, drawings, biometrics, sounds, hyperlinks, and spreadsheets. Health records are a good example of the rapidly changing nature of personal information records, with images and scanned documents already commonplace. Links are being planned between health records in several organizations to address the need for a comprehensive record of the episode of care from primary care to hospital to homecare, raising additional challenges. Email may contain attachments, and are often part of a larger message thread that may include personal information.

Decentralization of computing environments, from mainframe worlds to networked computers, makes it more difficult to collect and manage all the various electronic files that constitute a formal record. A patchwork of systems, and a variety of technology “generations” makes interoperability even more difficult.

Technological innovation has resulted in storage media becoming obsolete. For example, there are few computers today that have disk drives that can support the 8 or 5 ¼-inch diskettes that were common even 10 years ago. Except for the most crucial records, few data archives are regularly refreshed onto newer media.

Electronic records that are created with specific software and hardware generate dependencies that will be difficult to deal with as those products become obsolete. These electronic records will become orphaned without the original hardware and software.

---

## 5. ACHIEVING COMPLIANCE

What does all this mean for Canadian public, and private sector organizations? Public awareness of the implications of collecting and storing personal information has grown considerably in recent years with a corresponding increase in expectations that organizations will safeguard that information. If personal information is not well managed, organizations in both the public and private sectors risk serious damage to their public image and public support in addition to legal sanctions. It is therefore critical for organizations to have the capacity to safeguard personal information, manage that information, and demonstrate compliance with laws and regulations.

The key implication of this is that organizations must be able to demonstrate they understand what personal information they have in their possession and that it was appropriately collected, and is being managed in accordance with the relevant legislation.

To achieve this compliance with privacy legislation and best practices requires education and training of staff, changes to records management policies and processes, and technology to support these. Organizations need to establish and maintain information systems that facilitate efficient and effective compliance with the requirements of the legislation.

Public and private organizations frequently use disparate technologies for the management of personal information. In addition, content is often stored in different formats, locations, and systems, within the same organization or government ministry. Compliance solutions will need to address this and overcome the issues posed by this context.

## **6. THE CENTERA CE SOLUTION FOR RECORDS MANAGEMENT**

### **6.1 Centera CE Overview — What it is**

EMC's Centera Compliance Edition (CE) is an integrated software/hardware magnetic-disk-based archival storage solution specifically designed to overcome the limitations of conventional archiving technology, while helping to facilitate compliance with current Canadian standards and legislation around the storage of electronic information.

It is the first content addressed storage (CAS) solution specifically designed to meet the unique requirements of "fixed content" — unchanging digital assets retained for active reference and long-term value. Centera provides online access with assured content authenticity and petabyte scalability for a wide range of fixed content including personal information, X-rays, electronic documents, e-mail archives, check images, and CAD/CAM designs.

The Centera product is a self-managing, self-configuring, and self-healing storage device that significantly reduces storage management overhead, while ensuring that content stored on the Centera device remains non-re-writeable and available throughout a specified retention period.

With Centera CE, users can create and manage electronic records with a variety of software applications including; email archiving systems, document management systems, imaging systems, backup systems, Records Management Applications (RMAs), and Picture Archiving Communications Systems (PACS) systems for storage on the Centera CE device.

### **6.2 Centera CE Functionality — What it does**

Centera CE is the first magnetic disk-based Write Once Read Many (WORM) device. Centera facilitates compliance with the most stringent regulatory requirements, and provides functionality not available in tape, optical, or traditional disk solutions. It uses an integrated hardware and software system to deliver its functionality in many environments, including; Windows NT, UNIX, and z/OS mainframe platforms.

Centera CE delivers the following functionality:

#### ***Simple Management***

Applications no longer have to track the physical location of stored information. Instead, Centera creates a unique identifier, based on the attributes of the content, which applications can use for retrieval. Centera calculates a unique digital fingerprint/content address for each record based on the content of the record, uniquely identifying the record from all others. Centera uses the fingerprint to guarantee that a record never changes, either accidentally or by nefarious means, over the life of the record. If the record is altered in any way, Centera will recognize the difference and give the new record a new fingerprint.

---

## ***Security of the Media and the Content***

Centera has been physically and logically secured to guard against improper access or destruction of data, and possesses configurable features including access security, and a hardened management platform to prevent against fraud, malicious intent, or innocent user error.

## ***Assured Authenticity Via Non-Re-Writeable Content, Efficient Replication***

EMC<sup>2</sup>'s Centera CE solution assures data integrity and authenticity for the life of the archive through its unique digital fingerprinting via its CAS technology. Using this technology Centera gives each stored object a unique content address, derived from the content itself and as a result, no duplicates of the same content are ever stored. This integrity and authenticity is further enhanced by Centera's internal authorization mechanisms that control who has the ability to access, remove or delete records, and when it can be done.

## ***Retention Management***

Unlike tape cartridges or optical platters, Centera CE has the ability to associate and enforce retention periods at the record level. Once a retention period is set, Centera will lock down the record and guarantee that it cannot be deleted until the retention period expires. Multiple retention periods can be associated with a single record, so if it is subject to multiple regulations or if a retention period must be extended because a record is subject to a legal hold, Centera will protect it until the longest retention period has expired. When records are deleted, Centera will electronically "shred" the record beyond recoverability.

## ***Record Destruction***

Based on the U.S. Department of Defence's requirements for marking, downgrading, and declassifying national security classified information, now defined in the DoD 5015.2 STD standard, Centera has been built so that when records are deleted, Centera will electronically "shred" the record beyond recovery as required by this DoD standard.

## ***Complete Solutions***

Centera stores information in the format in which it is created. Centera is integrated into many leading applications across a variety of industries by EMC's Centera Partners; e.g. e-mail, documents, images, etc.

## ***Self-Management Functionality***

Centera continuously monitors itself and performs self-configuration, self-management, and self-healing using internal automated tools. Centera can detect and repair soft errors. It can also automatically reconfigure itself and replicate objects as necessary if hardware failures occur such as disks or nodes—which are automatically reported through EMC's remote monitoring system. In addition, Centera also provides full reporting and analytical tools.

## ***Business Continuity Protection***

When using content mirroring protection, all information objects are synchronously mirrored within a local Centera cluster to support automatic recovery from component failures. It also can be configured to maintain duplicate copies of fixed content at a remote site to guard against site disaster. Data is protected from harm via either mirroring or parity-protection.

### ***Easy Installation and Non-disruptive Upgrades***

Install or upgrade Centera in under an hour, without disrupting content access. Centera's software operating environment, CentraStar, also can be upgraded non-disruptively as new versions are released.

### ***Scalability Without Reconfiguration***

Centera's architecture is based on redundant arrays of independent nodes (RAIN)—offering petabyte scalability. Adding capacity is easy: Centera auto-discovers and configures the new capacity as it's installed.

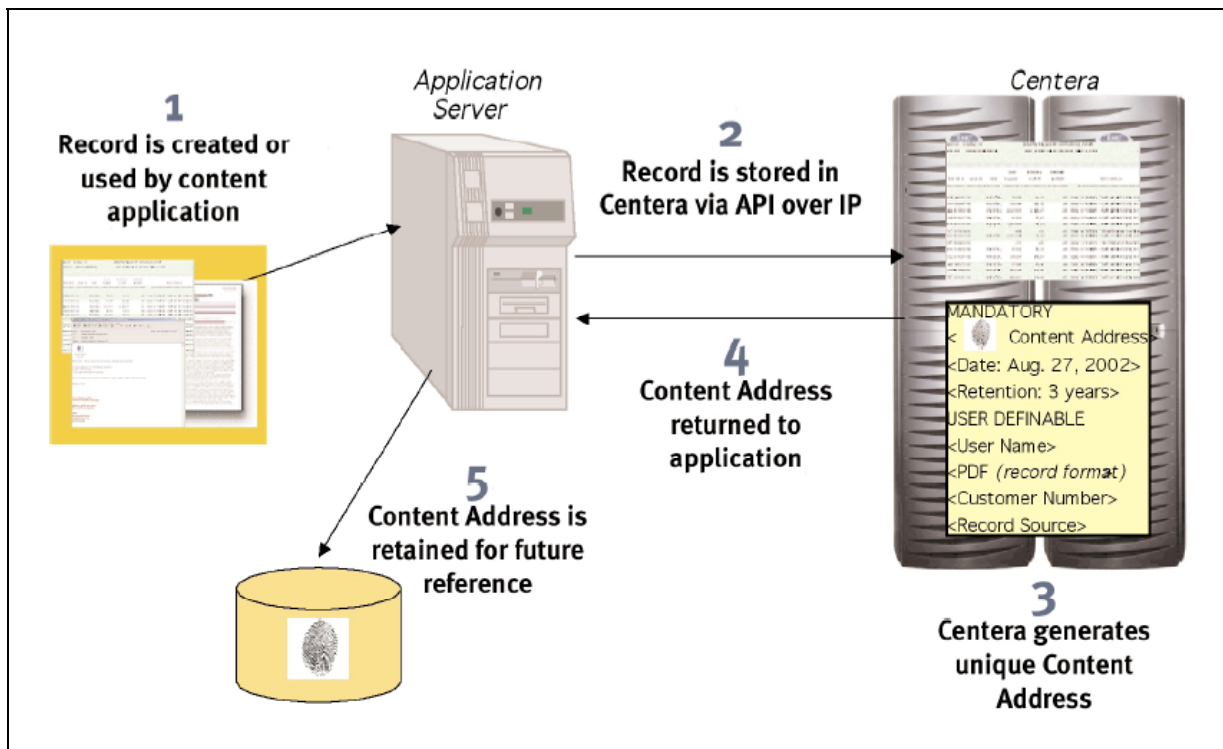
### ***Total Cost of Ownership***

When calculating the Total Cost of Ownership (TCO) of a technology solution, administrators must take into account not only the hardware and media costs, but also the costs of management, maintenance, and environmental. Centera CE is an automated hardware / software solution that effectively eliminates media costs and reduces management and maintenance costs. As a result, the TCO of the Centera solution can be significantly lower than storage alternatives such as WORM drives, tape, and network-attached storage, none of which provide online access nor provide assured content authenticity.

### ***Future-proof Architecture***

Content stored within Centera is location and hardware-independent as technologies evolve, records will continue to be accessible, independent of the underlying storage medium.

## **6.3 How it Works**



## 7. BEARINGPOINT ASSESSMENT AND ANALYSIS

### 7.1 Analysis

With the passage of the Privacy Act and PIPEDA, the federal government has effectively established new standards that records management applications must meet to support the creation, correction, management, retention and destruction of records with personal information. It is the opinion of BearingPoint that Centera Compliance Edition, when configured and used in conjunction with a certified RMA application, will effectively allow public and private sector organizations to meet the requirements of Canada’s new privacy legislation. *Figure 2: How EMC<sup>2</sup> Centera CE Supports Canadian Privacy Legislation* illustrates how the major requirements of the legislation are addressed with the Centera product.

*Figure 2: How EMC<sup>2</sup> Centera CE Supports Canadian Privacy Legislation*

Privacy Act	PIPEDA	Supporting Centera Functions
Limit its collection of personal information to the minimum details needed to operate programs or activities	Collect, use or disclose personal information reasonably, appropriately, and only for purposes that you have consented	The description of the data stored in Centera
Collect the information, whenever possible, directly from the person concerned		The “digital fingerprint” assigned to the records when they are created
Identify why information is being collected and how it will be used	Know why they collect, use or disclose personal information	N/A
Use the information for purposes specified, unless allowed by law		The “digital fingerprint”, security, retention management, and reporting functionality
Keep the information long enough to allow a reasonable opportunity to obtain access	Provide individuals access to their personal information and the ability to correct it	Centera retention management
Ensure the information is as accurate, up-to-date and complete as possible	Ensure that personal information is accurate, complete up-to-date	The “digital fingerprint”, security, retention management, and reporting functionality
Not disclose personal information unless specifically allowed by the Privacy Act or another law		The “Digital Fingerprint”, security, Retention Management, and reporting
	Know who in the organization is responsible for protecting personal information	Access controls
	Protect personal information by taking appropriate security measures	Supported by the “Digital Fingerprint”, security, Retention Management, and reporting
	Manage complaints about how they handle personal information, confidentially if requested	N/A

With the growing amount of information, these applications must be complemented by a robust storage repository that can efficiently and cost-effectively store and manage terabytes to petabytes of data. Centera Compliance Edition has an additional layer of data protection and security to make for a complete records management solution. Based on its assessment and analysis of Centera Compliance Edition, BearingPoint is confident that by implementing and managing Centera Compliance Edition in conjunction with other appropriate, compatible, and certified technologies, Canadian public and private sector organizations will immediately and cost-effectively address the electronic records management challenges that they are faced with today and for the foreseeable future.

In summary, the Centera CE solution has the ability to demonstrate legislative compliance for the personal information stored within the solution. It has the functionality and tools to be able to demonstrate and show an auditable history of compliance with the key aspects of the Privacy Act and PIPEDA including that:

- , The information was collected correctly — this is demonstrated via the traceability of who generated and stored the information and when.
- , It is being used only for the purpose it was intended — this is demonstrated via the traceability of who accessed the information and when.
- , Its retention is known and there is a process executing and proving its destruction as appropriate — this is demonstrated via the functionality that identifies what the various, and potentially multiple, retention rules are for each piece of information.
- , It is being stored in a private and secure way — this is demonstrated via the security of the device and the record depersonalization solution. It is further supported by the ability to trace who has accessed what information and when.

## 7.2 The Authors

Steve Pasquill is a Managing Director in the Canadian Public Services practice of BearingPoint.

Steve Lough is a Senior Manager in the Canadian Public Services practice of BearingPoint specializing in governance and accountability.

*BearingPoint has relied exclusively upon information supplied by EMC<sup>2</sup> regarding the functionality and operation of Centera. This information was made available in the form of written explanations, marketing materials, technical specifications, and from meetings and oral presentations.*