White Paper

RECORDS MANAGEMENT

Integrating Privacy Using Generally Accepted Privacy Principles

AICPA/CICA Privacy Task Force
November 2009

CA Chartered Accountants of Canada

RECORDS MANAGEMENT

Integrating Privacy Using Generally Accepted Privacy Principles

AICPA/CICA Privacy Task Force
November 2009

Notice to Reader

DISCLAIMER: *This document has not been approved, disapproved, or otherwise acted upon by any senior technical committees of, and does not represent an official position of the American Institute of Certified Public Accountants or the Canadian Institute of Chartered Accountants. It is distributed with the understanding that the contributing authors and editors, and the publisher, are not rendering legal, accounting, or other professional services in this document. The services of a competent professional should be sought when legal advice or other expert assistance is required.*

Neither the authors, the publishers nor any person involved in the preparation of this document accept any contractual, tortious or other form of liability for its contents or for any consequences arising from its use. This document is provided for suggested best practices of record management and is not a substitute for legal advice. Obtain legal advice in each particular situation to ensure compliance with applicable laws and regulations and to ensure that procedures and policies are current as legislation and regulations may be amended.

AICPA/CICA Privacy Task Force

Chair

Everett C. Johnson, CPA

Vice Chair

Kenneth D. Askelson, CPA, CITP, CIA

Eric Federing

Philip M. Juravel, CPA

Sagi Leizerov, Ph.D., CIPP

Rena Mears, CPA, CITP, CISSP, CISA, CIPP

Robert Parker, FCA, CA•CISA, CMC

Marilyn Prosch, Ph.D., CIPP

Doron M. Rotman, CPA (Israel), CISA, CIA, CISM, CIPP

Kerry Shackelford, CPA

Donald E. Sheehy, CA•CISA, CIPP/C

Staff Contacts:

Nicholas F. Cheung, CA, CIPP/C
CICA
Principal, Assurance Services Development

and

Nancy A. Cohen, CPA, CITP, CIPP
AICPA
Senior Technical Manager, Specialized Communities and Practice Management

A special word of appreciation goes to Nicholas F. Cheung, CA, CIPP/C, for his dedication to this project.

TABLE OF CONTENTS

FOREWORD

More and more, organizations face the critical issue of information overload. Before the electronic age, information would be kept in paper form in file cabinets until there was no more room. Even then, the lack of storage did not necessarily motivate people to dispose of their information, let alone dispose of it securely.

With the electronic age, information could now be stored in vast quantities taking up less space and presumably less cost. With the widespread acceptance of the Internet, people have embraced shopping and banking online — leading to even more information being created than ever before.

It has been said that "information is power" but as with any valuable resource, it must be managed to maximize its benefit and minimize its cost. This includes ensuring that information of a personal, sensitive or confidential nature must be protected from falling into the wrong hands.

This paper discusses the importance of designing privacy into an organization's records management program and how that can be accomplished using *Generally Accepted Privacy Principles* (GAPP).

This publication will

- explain what is personal information and why privacy is an important business issue.
- identify privacy concerns regarding records management.
- explain how GAPP can be used to integrate privacy into a records management program.

DEFINITIONS

What is Records Management?

A *record* may be defined as information created, received, and maintained as evidence and information by an organization or person, in pursuance of legal obligations or in the transaction of business[1].

Records management therefore may be defined as the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records[2].

In essence, records management is the management of information throughout the information life cycle[3].

What is Personal Information?[4]

Personal information (sometimes referred to as personal identifiable information) is information that is about, or can be related to, an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Individuals, for this purpose, include prospective, current, and former customers, employees, and others with whom the entity has a relationship. Most information collected by an organization about an individual is likely to be considered personal information if it can be attributed to an identified individual.

Some examples of personal information are:

- Name
- Home or e-mail address
- Identification number (for example, a Social Security or Social Insurance Number)
- Physical characteristics
- Consumer purchase history

Some personal information is considered *sensitive*. Various laws and regulations consider the following, among other things, to be sensitive personal information:

- Information on medical or health conditions
- Financial information
- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Sexual preferences
- Information related to offenses or criminal convictions

---

1 ISO 15489-1, International Organization for Standardization, 2001
2 ibid
3 The information life cycle consists of the following stages: Creation and Collection, Disclosure or Distribution, Use, Maintenance, and Disposal.
4 Excerpted from the AICPA and CICA *Generally Accepted Privacy Principles*

Sensitive personal information generally requires an extra level of protection and a higher duty of care. For example, some jurisdictions may require explicit consent rather than implicit consent for the collection and use of sensitive information.

Some information about or related to people cannot be associated with specific individuals. Such information is referred to as nonpersonal information. This includes statistical or summarized personal information for which the identity of the individual is unknown or linkage to the individual has been removed. In such cases, the individual's identity cannot be determined from the information that remains because the information is deidentified or anonymized. Nonpersonal information ordinarily is not subject to privacy protection because it cannot be linked to an individual. However, some organizations may still have obligations over nonpersonal information due to other regulations and agreements (for example, clinical research and market research).

WHY IS PRIVACY AN IMPORTANT BUSINESS ISSUE?

The loss of personal information can lead to grave consequences for the organization and the individuals involved. The misuse of personal information such as a credit card number or birth date, can lead to unauthorized purchases and identity theft.

For the organization, inadequate privacy policies and procedure can lead to:

- Damage to the organization's reputation, brand, or business relationships
- Legal liability and industry or regulatory sanctions
- Charges of deceptive business practices
- Customer or employee distrust
- Denial of consent by individuals to have their personal information used for business purposes
- Lost business and consequential reduction in revenue and market share
- Disruption of international business operations
- Liability resulting from identity theft

Good privacy practices are a key part of corporate governance and accountability. An organization that is proactive in managing their privacy risk will benefit from customer goodwill and reduced costs related to privacy breaches. One of the ways to address privacy risk is to focus attention in managing your records that contain personal information at all stages of the information life cycle.

What Are Some of the Privacy Concerns Regarding Records Management?

Unlike other information that an organization may deal with, personal information requires special attention due to its importance and value to customers and the growing incidences of identity theft. Organizations must ensure that its records management program secures, protects and disposes of personal information in accordance with its privacy policy, industry standards and legislative requirements.

- **What type of information is being collected?** Different types of information require different levels of protection. Knowing what type of information is being collected allows an organization to classify it properly and employ the appropriate means to protect it.
- **Is there a need to collect or is too much being collected?** Collecting personal information that is not required may be prohibited under privacy legislation. In addition, an organization must take the appropriate measure to protect such information so collecting less helps to minimize the risk that information may be misused, lost or stolen.
- **To whom is information being disclosed?** Personal information that has been collected remains the responsibility of the organization that collected it, regardless of whether that information has been disclosed to a third-party.

Organizations should ensure that contracts with third party processors of such information incorporate privacy protections.

- **What privacy laws and regulations apply?** Organizations may be subjected to a number of laws and regulations that apply to the protection of personal information depending on the state, province or country. Such organizations should seek legal advice to be informed about which laws and regulations apply, including cross-border transfers of personal information.
- **Is the organization disposing or destroying personal information properly and on a timely basis?** Disposal of personal information in the garbage or recycling bins without secure and proper shredding has led to many cases of privacy breaches. If the disposal and destruction of records containing personal information is outsourced to third-parties, does the organization obtain assurances that it has been done properly and on a timely basis?
- **Are employees given the appropriate level of access to personal information?** Access to personal information should be restricted to a minimum number of employees and to only those with job responsibilities that require such access. Organizations should have controls, procedures and mechanisms in place to maintain and monitor these authorized access lists. Organizations should ensure that employees receive the appropriate level of access to carry out their job responsibilities.

USING GAPP TO INTEGRATE PRIVACY INTO A RECORDS MANAGEMENT PROGRAM

What Are Generally Accepted Privacy Principles?

Generally Accepted Privacy Principles (GAPP) were developed by the American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) as a global privacy framework to help organizations create an effective privacy program that addresses privacy risks, obligations and business opportunities. They are based on fair information practices included in many privacy laws and regulations of various jurisdictions around the world and recognized good privacy practices.

The 10 generally accepted privacy principles are:

1. Management
2. Notice
3. Choice and consent
4. Collection
5. Use, retention, and disposal
6. Access
7. Disclosure to third parties
8. Security for privacy
9. Quality
10. Monitoring and enforcement

For each of the 10 privacy principles[5], relevant, objective, complete, and measurable criteria have been developed for evaluating an entity's privacy policies, communications, and procedures and controls.

The remainder of this paper will explore the principles and criteria in GAPP that have particular relevance to a records management program.

GAPP Principle #1 — Management

Under this principle, the entity should define, document, communicate, and assign accountability for its privacy policies and procedures.

Conducting a Personal Information Inventory

In any organization, departments may be collecting different types of personal information for various purposes. For privacy officers, it is their responsibility to enforce the policies that protect personal information. In order to carry out that responsibility effectively, an organization should consider undertaking a personal information inventory.

5 See Appendix A for more details about the ten generally accepted privacy principles

A personal information inventory will determine what personal information is being collected and by whom. By completing a personal information inventory, records management personnel and the privacy officer can determine if the personal information being collected is necessary and if proper measures are in place to store and dispose of it securely.

The inventory can be conducted by asking each department the following:

- List all types of personal information (PI) being collected (i.e., name, address) and the purpose of that collection (i.e., sales transaction)
- Where the PI is collected from (i.e., directly from customer, transferred from third party)
- Identify business systems that collect and process personal information (for example, payroll systems, point-of-sale systems, loan and financing systems).
- Where the PI is stored (i.e., data warehouses, offsite storage, electronic files, paper files, laptops)
- Who is authorized to have access to PI and who has access to it
- To whom PI is being disclosed to externally

Classifying Personal Information[6]

Classifying information is based on an inverse relationship between security and accessibility: the higher the security level, the fewer number of persons that should have access to that information. Employee access to information should be restricted to those individuals that have the necessary security clearance (if applicable), have a need-to-know for the information in question and have been granted formal access approval. Access to personal information should be restricted to only that information necessary to perform a job. This practice is known as the "Principle of Least Privilege."

Information classification levels typically vary from two to five. One example of a three-tier information classification is identifying the information as Public, Business Confidential, and Secret:

Public:

The lowest security level; intended for publicly available information; minimal security controls required.
Example: Organizational privacy policies, marketing materials, press releases, etc.

Business Confidential:

The medium security level; intended for authorized personnel; moderate security controls required.
Example: Customer name, address, phone numbers

Secret:

The highest security level; intended for the most sensitive information; access restricted to a minimum number of persons operating under the highest security controls.
Example: Bank Account Numbers, Credit Account Numbers, financial information before public release, Social insurance numbers (SIN), Social security numbers (SSN), product formulas

---

6 Portions of this publication have been excerpted from *The Canadian Privacy and Data Security Toolkit for Small and Medium Enterprises* by Claudiu Popa. The Canadian Institute of Chartered Accountants, 2009

It may be advantageous to designate an information classification specifically for PI. In some jurisdictions, PI is specifically protected under privacy laws and may be subject to specific requirements concerning retention and disposal. Organizations need to retain PI (especially PI used to make a decision affecting an individual) for a suitable period to allow individuals to access their PI. Entities often need to respond to such access requests within a short period of time (i.e., 30 days). By designating an information classification for PI, privacy officers and records management personnel can more readily monitor the use and disclosure of PI and it can help to facilitate responding to access requests on a timely basis.

Applying Information Classification to Personal Information

Information can be segmented according to its sensitivity. A complete data record could be divided into segments to make some data available while securing the more sensitive segments for restricted use. For example, consider the employee profile of a person in a management position:

Public:
: As a representative of the company, the manager's name and business contact information can be made publicly available with no loss of privacy.

Business Confidential:
: The manager's private contact information (i.e., home address and phone number) is only provided to a select number of employees for use only within the company, such as an emergency contact list.

Secret:
: The manager's salary, Social Security or Social Insurance Number, and professional record are securely stored with only the manager and Human Resources having access.

GAPP Principle #2 — Notice

Under this principle, entities should provide notice about its privacy policies and procedures and identify the purposes for which personal information is collected, used, retained and disclosed.

An organization's privacy policy should address how long they will retain PI under their control. At a minimum, the privacy policy should state that PI is retained for no longer than necessary to fulfill the stated purposes, or where applicable for a period specifically required by law or regulation[7].

Privacy officers and records management personnel should also ensure that the protection of PI is properly reflected in the organization's records management policies and procedures. In particular, management should ensure that the records management policies properly reflect any provisions in the privacy policy that pertain to records management. Employees should receive applicable training about these records management policies and procedures.

7 GAPP, Section 5.1.1

GAPP Principle #5 — Use, Retention and Disposal

Under this principle, the entity should limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or where applicable as required by law or regulations and thereafter appropriately disposes of such information.

How Long to Retain Personal Information?
How long PI is kept within your organization will depend on a number of factors. A retention policy should address the different types of PI that an organization may collect. For instance, PI of a transactional nature such as credit card numbers may not be needed after the transaction has completed, while a customer's name, address and phone number may be kept on file for future customer service or transactions.

Two privacy considerations should be kept in mind in developing or reviewing a records retention policy:

- PI should be disposed of once its use or retention is no longer required for business or legal purposes
- PI should not be retained or used for purposes that have not been disclosed in the privacy policy. If PI is being retained for a purpose that has not been disclosed, consent from the individual is required.

Factors to Consider In Determining Appropriate Retention Periods[8]

- Nature of organization's business and current activities
- Access request obligations
- Legal and regulatory requirements, including those related to securities, privacy, health, taxes and employment
- Use/benefit of the records and the consequences of not having them, including historical considerations
- Purpose of data collection
- Customer authentication requirements
- Need to manage any potential risk (for example, future litigation, investigations, audits)
- Contractual obligations of the organization, including obligations to third-parties
- Industry or trade association guidelines

Destruction Of Personal Information — "You Can't Lose It If You Don't Have It"

After statutory or business retention regulations have been met, PI at the end of the information life cycle must be destroyed in a manner that is secure and does not allow that information to be recovered. Destruction of unneeded PI can save storage costs, reduce the possibility of loss and lower the risk of litigation. Electronic files should be securely deleted and physical files should be sent for secure disposal according to one of the following methods:

- For electronic read only media (such as CD ROMs) — crushing, pulverizing, drilling holes and other methods to render the media unusable and unreadable

8 Records Retention — Risk Review, PrivaWorks, Nymity (www.nymity.com)

- For electronic read/write media (such as hard drives, USB keys) — overwriting/wiping/deleting
- For paper records — shredding or burning

Particular attention should be paid to ensuring the process is irreversible and the data irretrievable. In general, burning or incineration is the most effective way to ensure that the information cannot be recovered; however, shredding is the most common method.

What To Consider Before Destroying Personal Information

- Whether the destruction has been properly authorized and adheres to records management policies and procedures, including established retention and destruction schedules
- Whether it would be appropriate to remove, redact or anonymize the data rather than destroy all the data. Redaction is the removal of specified PI from a customer's record without removing all PI in the record (such as the removal of credit card information once the transaction is complete). Anonymizing the data would involve the removal of PI that would prevent the linking of other information to a specific individual (such as the removal of all patient names, addresses and hospital identification numbers from data being used for a research study).
- Ensure records related to an investigation, audit, legal process, claim warranties, complaint, dispute or access request are not destroyed/disposed of. Flagging such records and making employees aware of such flags is one example.
- Ensuring that only employees that are properly trained in records management procedures carry out destruction procedures to prevent accidental or inappropriate destruction or inappropriate handling of personal information.

Shredding

Shredding Machines

Shredding machines should be standard office equipment so employees have a secure means of document destruction. Shredders should cross cut instead of strip cut to reduce the possibility of reconstructing documents and recovering the original data. Purchase reliable shredders that do not break down frequently as shredders that break down frequently will discourage employees from using them.

Employees must not dispose of personal information in a recycling bin. Many cases have been documented where personal information that was disposed of in the recycling bin or in the garbage have been found by individuals, becoming a treasure trove of information for identity thieves.

"...while it certainly seems like common sense that discarded personal information should be destroyed...this is not happening. There are media reports literally every day about privacy breaches resulting from unsafe information destruction practices. These range from documents left in dumpsters or recycling bins, where they are easily accessible to the public, to information being left on old computers or other electronic equipment slated for reuse or recycling."

Sheldon Greenspan, Government Relations Chair, NAID-Canada, February 6, 2008,
British Columbia Special Committee to review the Personal Information Protection Act (PIPA)

Organizations with a volume of documents too large to be handled through an in-house shredder must hire a professional shredding service. Shredding services will generally leave a secure receptacle on each floor that employees can discard any papers that need to be shredded. This eliminates any need for employees to shred and also decreases the likelihood that unauthorized personnel have access to personal information. Whether your organization opts for on-site or off-site destruction, your organization must ensure that a written contract is signed and that it includes appropriate provisions to make clear the responsibilities of both parties (see Off-Site Destruction below).

On-site Destruction
For on-site destruction a shredding vehicle is brought to your premises to enable a member of your staff to oversee and verify that the shredding has taken place on a timely basis. This can be especially attractive as your organization ensures that the chain of custody over the personal information has not been broken. The organization should ensure that a Certificate of Destruction is issued.

Off-site Destruction
Off-site destruction is ideal for larger volumes of information. The shredding service will come and pick up the materials to be destroyed and perform the service on their premises. An advantage to using off-site destruction is that materials are often co-mingled with material from other organizations, making it even more difficult for anyone to recreate the documents should they come into possession of the shredded information. However, the organization must take steps to ensure that the shredding service will carry out their responsibilities in a timely manner and allow your employees to visit and conduct audits as necessary.

What To Consider In a Contract with a Shredding Service

The Information and Privacy Commissioner of Ontario has published a fact sheet (http://www.ipc.on.ca/index.asp?navid=46&fid1=451) that outlines important things to consider when engaging a shredding service. It also includes sample contract clauses that your organization should consider when engaging a shredding service. Users are advised to consult with a qualified attorney or lawyer in order to determine how best to structure such an arrangement to satisfy the user's unique needs and circumstances.

The fact sheet recommends that the contract should[9]

- set out the responsibility of the service provider for the secure destruction of the records involved.
- specify how the destruction will be accomplished, under what conditions and by whom.
- require that a certificate of destruction be issued upon completion, including the date, time, location, and method of destruction and the signature of the operator (while a certificate itself cannot prove that destruction has actually occurred, its existence, along with the written service contract, documented reference-checking, accreditation, etc., demonstrates that you have taken reasonable steps to ensure secure destruction has taken place).
- include a provision that would allow you to witness the destruction, wherever it occurs, and to visit the service provider's facility.

9 Fact Sheet #10, Secure Destruction of Personal Information. Information and Privacy Commissioner of Ontario, December 2005

- state that employees must be trained in and understand the importance of secure destruction of personal information.
- require that if any of the work is subcontracted to a third party, the service provider must notify you ahead of time, and have a written contractual agreement with the third party, consistent with the service provider's obligations to you.
- specify a time within which records collected from you will be destroyed, and require secure storage pending such destruction.

The organization should also ensure that proper due diligence has been performed, proper reference checks have been received and whether the service provider has been accredited by an organization such as the National Association for Information Destruction (NAID).

GAPP Principle #8 — Security for Privacy

Under this principle, the entity protects personal information from unauthorized access (both physical and logical).

Earlier in this publication, it was discussed that one of the benefits of conducting an inventory of personal information would be that it would shed light on exactly where and how PI was being stored throughout various departments. By understanding where and how PI is being stored, it allows an organization to review and ensure that appropriate measures are being utilized to secure manage PI.

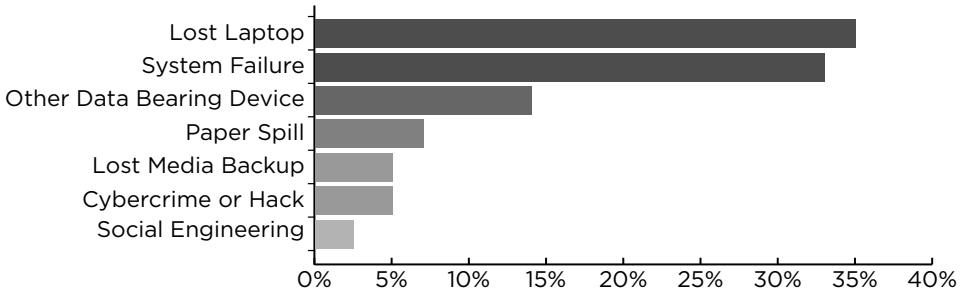

Figure A — Primary Causes of Data Breaches
Source: 2008 Annual Survey: U.S. Cost of a Data Breach. PGP Corporation and the Ponemon Institute.

Physical Storage
PI kept on paper must be kept secure by locking that information in file cabinets and not left on desks, even in a locked office. Papers left on desks in a locked office are still vulnerable as other staff members often access to these offices after-hours, such as night-time cleaning. Locking file cabinets that contain PI in both offices and in common areas should be part of daily operating procedures at the end of each business day.

Designated storage areas such as warehouses that contain large volumes of records should have adequate physical controls such as surveillance cameras, security guards, badge reader systems, security tape/locks on cartons/containers, alarmed entrances and exits, fire prevention systems, visitor logs, non-descript signs on the building and many other security techniques that may be necessary. Adequate controls should also be provided when records containing personal information are transported from one location to another (e.g. office to off-site storage).

Electronic Storage
Organizations must employ appropriate safeguards to secure mainframes, desktop computers, laptops and other portable electronic devices containing personal information. Many of the suggested safeguards for laptop computers below can be applied to desktop computers as well.

Many security experts suggest utilizing a "defense in layers" strategy to safeguard electronic assets such as personal information. A good information security program should address administrative, technical and physical controls to ensure personal information is adequately protected. Examples include assigning responsibility for information security, firewalls, encryption, user authentication, unique network and system IDs, complex passwords, audit logging, vulnerability assessments, software security patches and upgrades, monitoring for rogue wireless access points, code reviews, cameras to monitor data centers entrances and exits, and many others.

The following points should govern removal of personal information from the worksite:

- Does the PI really need to be taken offsite?
- Has only required information rather than the entire database been taken offsite?
- Is it possible to anonymize the PI by removing personal identifying elements from the information?
- Has the data been encrypted?

Understanding Mobile Computing Threats

Lost or stolen laptops and other devices such as USB flash drives account for almost half of all data breaches (see figure A). Laptops and notebooks are arguably the most useful mobile computing devices: they combine all the functionality and performance of a workstation with the portability of a briefcase. In many organizations, the laptop has already completely replaced the desktop. Unfortunately, its portability increases the likelihood of it being targeted for theft, thereby increasing the risk that any personal information on the device will be compromised.

Physically Securing Laptop

Only physical security can deter or prevent laptop theft. Whether at the office or on the road, always keep the laptop physically locked to a fixed object. Secure it with a cable lock even while in use to prevent "snatch-and-run" thefts. A visible cable lock also sends the message to opportunistic thieves that you are security-conscious and not an unassuming and vulnerable target.

Almost half of the most significant privacy breaches have occurred after laptops were stolen from cars parked in plain sight. When in cars, keep laptops in the trunk, underneath car seats, or otherwise covered to keep them out of sight of opportunistic thieves.

Additional Best Practices:

- Use hardware-based hard drive encryption. This new technology is now available from a variety of laptop manufacturers and allows computers to store data automatically in encrypted format on hard drives. Care must be taken to ensure that data is still encrypted when laptops are hibernating or in 'stand-by' mode.
- Use software-based hard drive encryption. In situations where hardware encryption is not available, companies can use the less secure, but very convenient Windows Encrypted File System (EFS) to protect sensitive data. By using this

transparent feature of the operating system, users can save files to encrypted folders, thus adding a layer of confidentiality. For stronger encryption, Pretty Good Privacy (PGP), Safeboot or other encryption software can be used.

- Enable BIOS (basic input/output system) or boot-up passwords. Unlike network user passwords, these passwords can and should be preserved by the IT department in a secure place, in order to access the computer should the user ever forget the password. Employee accountability is preserved because the login password is still only known to the user and not the IT department.
- Enforce a short lock-out period for password-protected screensavers. Although a quick lockout will not prevent theft of the laptop itself, it significantly reduces the risk of a security breach by minimizing the window of vulnerability through which data can be accessed.

Note: These best practices should be added to your company's Acceptable Use of Technology Policy or the Mobile Security Policy and communicated to all employees on a regular basis.

Understanding USB Threats

Universal Serial Bus (USB) flash drives give professionals the convenience of being able to transfer documents between workplace computers or even between work and home. As with mobile devices, the tiny USB drives are just as (if not more) easily misplaced or stolen. Because these devices can store a great wealth of information, the theft of a single USB drive could compromise the security of multiple gigabytes of potentially sensitive data. For this reason alone, the convenience that they bring may not be worth the risk and companies often choose to block removable USB devices altogether. If their use is absolutely necessary in your company, then USB drive security should be enhanced through the use of encryption features. These features may be built in by the device manufacturers or installed by third-party applications.

Brand-specific Locking to Prevent External Data Theft
Brand-specific locking refers to the practice of restricting the installation of USB devices to a single brand. This method simulates "authorized" devices so that only a single-brand USB drive can communicate with all computers; an intruder cannot simply insert an "unauthorized" USB drive and electronically "snatch-and-grab" confidential files with a simple drag-and-drop. In practice, a lesser-known brand may be used to reduce the likelihood of an unauthorized USB drive connecting to a computer under the guise of a legitimate company device.

Secure Storage: Data Under Lock and Key
A USB drive, as with any other device that stores confidential company data, is an asset that needs to be protected from unauthorized physical access. USB devices should be attached to keychains whenever possible or otherwise carried on one's person, and stored in a locked cabinet or secure area when not in transit. Policies should state clearly that USB drives must never be left unattended.

Applying Hard Drive Encryption to Protect Confidentiality

Removable drives are normally portable, high-capacity hard drives (or even re-writable DVD drives) that connect to a computer by means of a USB connector or similar mechanism. The main difference between USB drives and removable drives is size and capacity; USB drives have an average 2 to 4 gigabyte (GB) capacity and removable drives have an average of 250 to 400 GB. Because of their similar functions, most security measures for USB drives are applicable here.

Since larger hard drives carry more data, a security breach resulting from the theft of a hard drive is likely to be significantly more damaging than one resulting from the theft of a USB drive. Fortunately, some removable hard drives offer built-in encryption in particular for the purposes of archiving and backing up data offsite.

Ensuring Backups are Secure
Once data is retained in a relatively permanent medium such as a high-capacity tape cartridge, DVD, or hard disk, the question often becomes; "What do we do with it?" The primary options are onsite retention and offsite retention.

Onsite Backup Retention
Advantages: Store the data onsite in a secure, limited-access area. The data is stored securely, inexpensively, and is immediately available for use as required.

Disadvantages: Backup data stored onsite shares the same physical risks as the infrastructure: flooding, fire, earthquakes, etc., that threaten the servers that store the original data. A crisis could result in the loss of both primary and backup data storage with little or no chance of recovery.

Daily or weekly backups can quickly generate many storage media. Given that such media should be stored in protective cases such as flame-resistant or waterproof cabinets, costs can escalate and the space soon becomes insufficient.

Offsite Backup Storage — Satellite Office
Data can also be stored offsite at a satellite office geographically distant from the office processing the backups, or at a third-party storage service. All data should be encrypted before being removed from organizational premises. Encryption software is included in most of today's data backup hardware and software, but the process of encryption is time consuming when large volumes of data must be stored.

Advantages: Storage at a satellite office ensures backup data is stored under similar organizational security and can be retrieved quickly.

Disadvantages: Unlike onsite storage, offsite storage incurs the costs of courier services.

Executives at small organizations may be tempted to store backup tapes at home. Unfortunately, they may be *more* at risk there than being stored securely at the workplace. Statistically, more than 50% of data tape theft occurs in the homes of employees and more importantly, such theft usually indicates a targeted attack, rather than a random crime of opportunity. The workplace is a controlled environment with numerous physical and logical security and safety measures. Thoroughly review the security and safety measures in place before committing to an offsite location.

Did You Know?
Although it may be cost efficient to use employees who frequently commute between geographically distant offices as couriers, they lack the reliability and security of established courier services. For instance, courier services offer defined delivery times and security measures, while employees make little, if any, provision for security and service reliability.

Offsite Backup Storage — Third-Party Service Provider
An alternative to the above is to outsource data backup and retention altogether. There are a number of data retention services that will provide backup via encrypted remote network connections. The need for storage of physical media, transportation costs, and other logistical support is gone. This alternative, however, requires a significant investment in networking technology to ensure sufficient network capacity, speed, and reliability throughout the backup process.

A third-party Service Level Agreement should address:

- Environmental conditions: various media require specific temperature and humidity controls to prevent compromising the integrity of the data stored on them.
- Security of the media during transportation: media can be damaged, lost, stolen or destroyed in transit.
- Timeliness: the service provider's protocols must permit backup media to be stored in an easily-retrievable manner. Data recovery in a crisis must not be impeded.

Legal advice is recommended prior to entering into any agreement.

All data should be encrypted before being removed from organizational premises. Encryption software is included in most of today's data backup hardware/software, but the process of encryption is time consuming when large volumes of data must be stored.

GAPP Principle #10 — Monitoring and Enforcement

In this principle, the organization should monitor compliance with its privacy policies and procedures and have procedures to address privacy-related complaints and disputes.

In addition to establishing policies and procedures regarding the retention of PI, it is also essential that these policies and procedures are monitored and enforced to ensure their compliance. Failure to do so can lead to:

- Unnecessary additional costs for storage
- Increased likelihood of a breach
- More extensive impact of a breach

Failure to abide by established policies and procedures can lead to an increased likelihood of a breach. This can happen in a case such as employees not destroying PI properly, perhaps by dumping PI into a recycling bin instead of shredding it. Also, failure to destroy PI on a timely basis will make more data available for a breach, thereby making the impact of a breach more severe.

Organizations should have monitoring programs in place to ensure that records management policies and procedures are being followed. Examples include periodically (at least annually) reconciling personal information inventory records to confirm its accuracy. This reconciliation would confirm such things as location of data, data owners, types of personal information retained, third-parties where data is disclosed, and so forth. Organizations should also monitor access to personal information to ensure the data is not breached or compromised. They should have a management structure in place that takes appropriate corrective action when deficiencies are identified. An example is an incident response team in the event of a breach of personal information.

CONCLUSION

Designing privacy into an organization's records management policies and procedures is a critical component to having a robust privacy program. Both records management personnel and privacy officers must work together to ensure that personal information is properly and securely stored, retained and destroyed. GAPP provides a number of best practices that organizations should consider in their records management program to ensure privacy concerns have been addressed.

Certified Public Accountants and Chartered Accountants are business advisors who provide a number of services that can help organizations assess their compliance with their policies and procedures. An independent assessment may be conducted (for internal management use only) or independent audit may be undertaken where the organization desires a report that could be disclosed to external parties.

The AICPA and the CICA have developed privacy resources to assist organizations in meeting their privacy obligations. In particular, organizations are encouraged to make use of the AICPA/CICA Privacy Risk Assessment Tool. It is a spreadsheet-based tool that allows organizations to conduct their own privacy risk assessment against GAPP and helps to identify areas that may require additional attention and action. This and other privacy resources are available from www.aicpa.org/privacy and www.cica.ca/privacy.

APPENDIX A

Generally Accepted Privacy Principles

1. Management. The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
2. Notice. The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
3. Choice and consent. The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
4. Collection. The entity collects personal information only for the purposes identified in the notice.
5. Use, retention and disposal. The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. Access. The entity provides individuals with access to their personal information for review and update.
7. Disclosure to third parties. The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. Security for privacy. The entity protects personal information against unauthorized access (both physical and logical).
9. Quality. The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
10. Monitoring and enforcement. The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

ISBN 978-1-55385-466-1