

Get rid of it *Securely* to keep it Private

**Best Practices for the Secure Destruction of
Personal Health Information**



**Information and Privacy Commissioner,
Ontario, Canada**



**National Association for
Information Destruction, Inc.**

October 2009

Acknowledgements

These *Best Practices* build upon the Commissioner's previous publications: Fact Sheet No. 10, *Secure Destruction of Personal Information*, and No. 26, *Safe and Secure Disposal Procedures for Municipal Institutions*, as well as the National Association for Information Destruction's *Information Destruction Compliance Toolkit*.

The Commissioner gratefully acknowledges the work of Catherine Thompson, Regulatory and Policy Advisor, in preparing this report.

The Commissioner also wishes to gratefully thank Robert Johnson, Executive Director of NAID, not only for his contributions to this paper, but for his tireless work in advancing the field of secure destruction.

This publication is also available on the IPC website (www.ipc.on.ca) and the NAID website (www.naidonline.org).

Table of Contents

I	Foreword	1
II	Introduction	2
III	Definitions	3
IV	Best Practices for the Secure Destruction of Personal Health Information	4
	A. Develop and Implement a Secure Destruction Policy	4
	B. Segregate and Securely Store Personal Health Information	6
	C. Determine Best Methods of Destruction	7
	D. Document the Destruction Process	9
	E. Considerations Prior to Employing a Service Provider	11
	F. Disposal of Securely Destroyed Materials	13
	G. Auditing and Ensuring Compliance.....	13
V	Summary	15
VI	Conclusion	16
VII	Resources	17

I Foreword

A single medical record can testify to a great deal. It can speak to the recreational and lifestyle habits of a person, as well as the intimate details about his or her sexual practices and personal hygiene. It can reveal major health issues, the unauthorized access of which could be a devastating blow to an individual, potentially resulting in a loss of dignity, alienation of family and friends, or discrimination by an employer.

At the same time, personal health information is the lifeblood of many businesses and an indispensable part of the health-care industry. As a result, providing much-needed health-care services while ensuring privacy may seem like walking a tightrope, where the slightest misstep may result in harmful consequences. This concern often arises with regards to the secure destruction of personal health information.

Organizations developing secure destruction policies to destroy virtually any type of personal information often face difficult questions. What are the risks versus the consequences of adopting a certain destruction practice? What are the expectations of the person, whose personal health information is contained in the record, regarding the secure destruction of their personal health information?

My co-author Robert Johnson, Executive Director of NAID, and I are very pleased to present this *Best Practices for the Secure Destruction of Personal Health Information*. As Mr. Johnson points out, the stakes are very high — where financial standing may be repaired, stealing and using someone's personal health information may put that individual's life at risk if key health details, such as a different blood type, are incorporated into their medical file. It may seem like an oxymoron, but you really need to think about the end of the process, right at the beginning.

We hope that these *Best Practices* will assist organizations in protecting the privacy of health-care recipients *and* make it possible for organizations to meet their business objectives — this will result in a positive-sum outcome for both. While our focus may be on health information, these *Best Practices* also apply to any sensitive information, and may assist organizations in other sectors.

Ann Cavoukian, Ph.D.
Information and Privacy Commissioner,
Ontario, Canada

II Introduction

These *Best Practices for the Secure Destruction of Personal Health Information* will help organizations ensure that their information destruction policies move beyond basic statements that records should be destroyed when they are no longer useful, or for legal reasons. Organizations considering the destruction of records containing personal health information that fall under the *Personal Health Information Protection Act* (PHIPA) should develop a policy on secure destruction for their organization that is clear, understandable and leaves no room for interpretation.¹ Key additional considerations in developing a secure destruction program are discussed in the following chapters and relate to the secure storage of personal health information before it is destroyed, the types of records and media to be destroyed, and the methods of destruction. These *Best Practices* also underscore that developing a secure destruction policy must go hand in hand with providing clear instruction to staff regarding the need to protect discarded information.

The approach underlying these *Best Practices* is *Privacy by Design*. First coined by one of the authors of this paper in the '90s, Dr. Ann Cavoukian, Ontario's Information and Privacy Commissioner, *Privacy by Design* involves proactively building privacy into the design, operation and management of information processing systems. Using a *Privacy by Design* approach, privacy is built into secure destruction programs at the outset, rather than treating it as an afterthought, in a way that provides for functionality and security. This can widen the path for the health-care industry to deliver functional services *and* ensure the security of personal health information, resulting in a win-win scenario for patients and providers.

The scope of these *Best Practices* includes personal health information in the custody of health information custodians as defined under *PHIPA*, and beyond — many of the practices described can be applied to the various personal information that organizations must dispose of securely. Unless governed by legislated retention periods, organizations will also need to look at creating a records retention and information classification policy. This should be developed separately from their secure destruction policy and is not covered by these *Best Practices*. In addition, organizations must also separately address the destruction of cash value items (e.g., unused cheques) and prototypes (e.g., new product research) separately, as well as the organization's procedures and systems for discontinuing the destruction of information related to any litigation, legitimate audit or investigation.

1 *PHIPA* requires health information custodians protect personal health information in their custody or control and to ensure that records are retained, transferred and disposed of in a secure manner. Also, a health information custodian must protect personal health information against theft, loss and unauthorized use or disclosure. *PHIPA* also requires that information practices be in place to comply with the *Act* and its regulations. (See sections 10, 12 and 13). The need for a policy governing information practices and procedures is widely referenced in internationally recognized privacy protection principles and instruments, Canadian federal and provincial privacy laws, U.S. federal child, health and credit legislation and agreement, as well as several state laws regarding the security of personal information.

III Definitions

Degaussing means to remove or erase a residual magnetic field from a magnetized object, such as a tape or disk, usually by introducing much stronger and gradually diminishing magnetic fields of alternating polarity.

Destruction means to permanently destroy or erase in an irreversible manner to ensure that the record cannot be reconstructed in any way, and does not include recycling or placing in the trash.

Electronic media includes micro media (film media, such as microfilm and microfiche), magnetic tape media (reels, VCR, cassette), optical media (DVD, CD), and electronic equipment with magnetic storage media (computers, servers, any equipment utilizing a hard drive, or the hard drive that has been removed from any equipment), personal hand-held computing or processing devices (PDAs, mobile phones, portable memory devices, removable memory cards from phones and cameras), and office machines such as photocopiers, fax machines, scanners and printers containing storage devices (such as a hard drive).

Personal health information is defined in section 4(1) of *PHIPA* as identifying information about an individual in oral or recorded form, and includes, for example, information relating to the physical or mental health of the individual, providing of health care to the individual, payments or eligibility for health care, as well as the individual's health number.

Record is defined in section 2 of *PHIPA* as a record of information in any form or medium, whether in written, printed, photographic or electronic form or otherwise, but does not include a computer program or other mechanism that can produce a record.

Mechanical destruction is the act of destroying media by breaking it into smaller pieces or distorting through use of a mechanical device.

Media includes paper records and electronic media.

Sanitization is the process of masking information recorded on a hard drive by overwriting with random meaningless data.

Secure erase is the process of permanently removing information from a computer hard drive by activating a pre-existing protocol hard wired into the hard drive by the manufacturer.²

² Developed by the Center for Magnetic Recording Research at the University of California, San Diego, secure erase is different than software-based sanitization. Since 2001, it has been embedded in common hard drives and can purge data beyond forensic reconstruction. However, this process is not accessible directly through the functions of any computer so that it cannot be inadvertently activated. It must be activated by physically accessing the hard drive directly with the proper equipment and software.

IV Best Practices for the Secure Destruction of Personal Health Information

A. Develop and Implement a Secure Destruction Policy

(i) Take a team approach

Organizations developing secure destruction policies should use a team approach by consulting internally with the organization's records management, risk management, information technology, security, privacy, facilities management, and auditing departments. Secure destruction policies should be part of a complete Corporate Policy Manual that addresses all aspects of *PHIPA*. Organizations may wish to also consult with outside legal counsel and potential service providers.

(ii) Determine in advance what records should be destroyed

An organization may choose to destroy records confirmed to have personal health information only if the organization has very well-controlled and well-organized documentation regarding its information holdings. Alternatively, an organization may choose to securely destroy: 1) all records, 2) records where there is an absence of information about whether personal health information is contained in the record(s), or 3) only those records where there is likelihood that personal health information is contained, but it is impractical to confirm that fact (i.e., it would cost the same or more to confirm rather than securely destroy). These decisions should be made taking into consideration the types of record and the nature of the media that may contain personal health information.

(a) Types of records

The secure destruction policy should outline which types of record the policy applies to, such as stored records, duplicate records, incidental records, and electronic media, as well as e-mail and voice mail. In the health-care context, records containing personal health information may include patient identification cards and wristbands, as well as X-rays. Policies should refer to the organization's records retention and information classification policy in defining what information is to be considered confidential, and should also require document labeling or access restrictions. Every organization has a 'daily waste stream' (or incidental records), usually paper, which is made of discarded records such as printing mistakes, notes and memos. This stream of records should be addressed in the secure destruction policy and should not be categorized as simple recycling if it may contain personal health information.

(b) Types of media

Secure destruction policies must address all media that may be destroyed, including, but not limited to, paper, micro media (film media, such as microfilm and microfiche), magnetic tape media (reels, VCR, cassette), optical media (DVD, CD), and storage media (computers, hard drives, PDAs, mobile phones, and portable memory devices). If office machines such as photocopiers, fax machines, scanners, or printers contain storage devices, ensure that these devices are overwritten, erased,

removed, or destroyed when the machines are replaced. The policy should describe the specific methods for destroying each different type of media, the different internal authorizations for destruction, if any, and requirements for securing the media before destruction. If there are several accepted processes for destroying a type of media, the policy should identify the preferred process in particular. For example, magnetic tape may be destroyed by degaussing, shredding or incineration, and the organization's policy should specify which method is to be used. See also 'Determine Best Methods of Destruction' section at page 7.

(iii) Define roles and responsibilities

An organization's secure destruction policy should designate a policy compliance officer who will be the person ultimately responsible for organizational compliance, as well as compliance officers for each of the organization's physical locations. Ensuring compliance need not be a full-time job and can be simply part of an individual's job description to be responsible for the location complying with the organization's destruction policy. In addition to naming compliance officers, the policy should state that the employees' immediate supervisor is responsible for ensuring compliance with the policy on a daily basis. The policy should also name the individuals responsible for development of the policy, approval of the policy, employee orientation and training regarding the policy, contracting destruction services or equipment, performing internal audits, distributing updated policies, and informing employees about updates. In addition, organizations should consider whether they wish to have someone witness the destruction. Note, some destruction companies offer the option for witnesses to view the destruction through a webcam over the Internet.

(iv) Consider the design of the secure destruction program

(a) In-house or outsourced

Deciding whether a secure destruction program should be conducted in-house, outsourced or partially outsourced is a key decision that each organization must determine and detail in their secure destruction policy. The policy should state that when contracting a service provider, the transfer of custody should be clearly documented and the service provider must accept fiduciary responsibility for destroying the records. See section at page 11 'Considerations Prior to Employing a Service Provider.' Organizations may wish to engage a secure destruction service provider that offers mobile or on-site destruction services. Whether destroyed internally or by a service provider, the individuals performing the destruction must be properly trained in the operation of the destruction equipment. Also, destruction must always be performed under secure and controlled conditions.

(b) Centralized or decentralized

Organizations performing an in-house destruction program should determine if the program will be centralized or decentralized. A centralized model of internal destruction involves employees collecting records to be destroyed in a container at their desk, where it is securely collected and transported by a designated employee to the location of the destruction equipment within the organization.³ In a centralized program, it may be a prudent policy to have some records isolated from the program

³ Documentation of the destruction can be achieved by creating an internally-generated Certificate of Destruction once the destruction is complete. See section at page 10 'Certificate of Destruction.'

and destroyed at the department level. A decentralized model of internal destruction involves employees destroying records themselves throughout the workday using equipment in the vicinity of their workstations. In this model, the organization may choose to have employees contact a specific person in the organization for large purges of paper. The decentralized model may be less suitable for very sensitive records as employees must be diligent in not leaving records or media unattended, as well as reporting any malfunctions in equipment to their supervisor. Regardless of which model is chosen for an organization's destruction program, this should be detailed in its secure destruction policy.

(v) Contingency planning

Policies should describe a contingency plan should a contracted secure destruction service provider suddenly not be available, or if destruction equipment such as a crosscut shredding machine ceases to operate. Some measures may increase the risk of theft, loss and unauthorized use or disclosure, such as transferring records and media to another satellite location that has working equipment without a pre-established protocol to do so. Alternative measures may include keeping all materials to be shredded in a secure, clearly marked container until a new crosscut shredder is available. Or, another secure destruction service provider may be contracted in accordance with an organization's criteria for choosing a service provider.

(vi) Application of the policy

A secure destruction policy should apply to all operating units of an organization, including remote operations, divisions, or subsidiaries. The policy should document variations in the application of the policy such as, for example, if secure destruction is outsourced at a remote operating unit location, but destroyed internally at a central location.

B. Segregate and Securely Store Personal Health Information

(i) Prior to destruction

As emphasized in the Information and Privacy Commissioner's health orders (HO-001 and HO-006) organizations must ensure that personal health information in its custody or control is securely stored and protected against theft, loss and unauthorized use or disclosure. Also, that no unauthorized person will have access to the information between the time the records leave the organization until their actual destruction. As such, organizations should establish a procedure for segregating and securing personal health information prior to destruction.

Once paper records have been segregated or stored prior to destruction, an organization may wish to isolate and label those records to lessen the possibility that there is unauthorized access or that they are disposed in an inappropriate manner (e.g., mistakenly placed in the recycling bin instead of destroying). Options for storing paper media include a secured workstation container or secured general office container kept in a separate location from all recycling bins.

Electronic media should also be segregated and secured. An organization may want to have satellite locations refrain from sending electronic media to another unit of the organization without detailed written permission from a designated individual within the organization. Organizations may wish to provide an easy point of contact for coordinating removal of electronic storage media from service such as hard drives.

(ii) After the destruction

Following degaussing or sanitization, access to electronic media must be restricted and further distribution delayed until an internal audit of a percentage random sampling of the media demonstrates that the degaussing or sanitization process was effective. Destroyed materials such as paper particles, after destruction, should be restricted from public access and eventually recycled to minimize heroic attempts at reconstruction.

C. Determine Best Methods of Destruction

The goal of record destruction is to have records containing any personal health information permanently destroyed or erased in an irreversible manner that ensures that the record cannot be reconstructed in any way. It is incumbent upon organizations to determine the destruction method that credibly implements their secure destruction policy requirements.⁴ Organizations must determine which destruction method is best suited to the classification of the record, taking into consideration cost and convenience as well as the sensitivity of the record.⁵ This determination will constitute the “approved methods of destruction” and should be detailed in the organization’s secure destruction policy.

(i) Paper records

Methods of destroying paper include mechanical destruction (such as crosscut shredding, pulping, and pulverizing), and incineration. When mechanically destroying paper, material residue should be reduced to pieces millimetres in dimension. These pieces may be part of the organization’s normal recycling program. When incinerated, material residue should be reduced to white ash and be contained so that partially burned pieces do not escape.

4 Organizations should consult available resources to research options for destruction. For example, the Destruction Evaluations and Guidance Branch of the U.S. National Security Agency publishes evaluated lists of products that give adequate security for destruction of various media, including paper shredders, high security disintegrators, and degausser equipment. See ‘National Security Agency Media Destruction Guidance’ online at <http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml>. Also, the National Institute of Standards and Technology (NIST) has published minimum sanitization recommendations for various types of media. See *Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-99, September 2006, Appendix A, p. 17 -25.

5 “For instance, it may not be cost-effective to degauss inexpensive media such as diskettes. Even though clear or purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc.) to destroy media rather than use one of the other options.” *Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-99, September 2006, p. 9.

(ii) Electronic media

The method of destruction for electronic media includes mechanical destruction to render it unusable, degaussing, and sanitization (including secure erase), and should involve removing all labels or markings that indicate previous use. Simply deleting computer files or reformatting a disk does not securely destroy the data because even deleted files may be subject to data recovery efforts.

For all personal hand-held computing or processing devices (such as PDAs and mobile phones) storing sensitive contact information, calendars, documents, e-mail correspondence and other information, methods of destruction may include mechanical destruction of the entire unit, or destruction of the replaceable memory circuits or card so that the device can be redeployed with a new memory component.

(iii) Employing more than one method

Organizations may wish to employ more than one method of destruction to ensure personal health information cannot be reconstructed. For example, an organization may wish to go beyond shredding and ensure that pulverization or incineration of the records takes place in the case of paper records, or the physical destruction of degaussed or sanitized electronic media.

(iv) Organizational control

Organizations should take into consideration whether media will one day not be under their organization's control when determining which method of destruction should be chosen. For example, an organization wishing to return a hard drive for warranty purposes may wish to employ secure erase.

(v) Recycling ≠ secure disposal

As underlined by the Commissioner's health orders (HO-001 and HO-006), when it comes to the disposal of personal health information, recycling documents is not an acceptable option for secure destruction. In the recycling process, paper may be stored in warehouses for lengthy periods of time until enough has accumulated, and then may be sold while still intact. Remember, recycling does not equal secure destruction.

D. Document the Destruction Process

Documenting the destruction will assist in creating an audit trail for monitoring compliance with the organization's secure destruction policy.⁶

(i) Authorization to destroy

Organizations should include in their secure destruction policies a provision that employees must obtain internal authorizations prior to the destruction of personal health information.⁷ An organization may develop a process to authorize batches of records or media on a single authorization. The authorization should include a signature field for sign off and the level of authorization required (e.g., specific department such as legal or audit). The authorization document may include the following information:

- date of destruction
- name, title, contact information, and department of the person submitting the authorization
- description of the information or media being destroyed
- retention schedule reference number
- any relevant serial numbers
- quantity being destroyed
- origination or acquisition year (can be a range)
- retention expiration date
- location of the records
- reason for destruction
- method of destruction
- whether destruction is to be performed in-house
- approved contractor and vendor number, if relevant
- approved destruction method according to the organization's secure destruction policy.

6 For organizations in the clinical setting (e.g., hospitals, physicians) please see the Physician Privacy Toolkit and Hospital Privacy Toolkit.

7 To further assist in audit trailing, the service provider may record the organization's internal authorization serial number in its Certificate of Destruction.

An organization may decide to exclude records not subject to the organization's retention schedule, such as incidental or duplicate records. However, organizations should note that without an internal authorization to destroy, further documentation should be substituted, for instance an internal log of the destruction or internally-generated Certificate of Destruction issued on a routine basis (e.g., daily, weekly, etc.) to document the destruction of incidental or duplicate records. If outsourcing the destruction of incidental or duplicate records to a service provider, then the Certificate of Destruction or other transactional record, such as an invoice or service order, may act to provide documentation for audit trailing purposes.

(ii) Certificate of Destruction

Although it cannot serve as absolute proof that a destruction of records has taken place, a consistent and chronological series of Certificates of Destruction over an extended period of time may assist in establishing that the organization has adhered to its secure destruction policy. The policy should indicate the required fields in a Certificate of Destruction, whether produced by a secure destruction service provider or generated internally, and may include:

- company name
- a unique serialized transaction number
- the transfer of custody
- a reference to the terms and conditions
- the acceptance of fiduciary responsibility
- the date and time the information ceased to exist
- the location of the destruction
- the witness to the destruction
- the method of destruction
- a reference to compliance with the contract (if employing a secure destruction service provider)
- signature.

Organizations creating internally-generated Certificates of Destruction may also wish to include fields such as: who the destruction was conducted by (name, title, contact information, department, etc.); when collection of the information to be destroyed began (if using a centralized model of internal destruction); the type of media collected and from which specific containers; and the time at which the collection was completed. Regarding the destruction event itself, the internally-generated Certificate of Destruction may detail the start time, location, equipment used, quantity destroyed, and destruction completion time. An organization may develop a process to certify the destruction of batches of records or media.

(iii) Logs

In addition, creating a log for the destruction of records not subject to the organization's retention schedule, such as incidental and duplicate records, organizations may also include a provision in their secure destruction policy to create a record documenting the destination and disposal of the media particles following the destruction. In addition, the results of random sampling audits following the degaussing and sanitization process for electronic media should be logged.

E. Considerations Prior to Employing a Service Provider

(i) Criteria for choosing a service provider

Organizations should develop criteria for choosing a secure destruction service provider and include it in their secure destruction policy. For example, organizations may wish to look for a provider accredited by an industrial trade association, such as the National Association for Information Destruction (NAID), or at least be willing to commit to upholding its principles. Criteria may also include finding a service provider that has written policies and procedures that must be approved by a specific person or committee within the organization.⁸ Additionally, criteria may also relate to whether the service provider creates a Certificate of Destruction for each destruction event, has a confidentiality agreement with each employee, and is willing to submit itself to independent audits.

(ii) Confirm method of destruction

Organizations outsourcing the secure destruction of paper and electronic media should include a requirement in their secure destruction policy to confirm which methods the potential service provider employs for the destruction of records.

(iii) Secure transportation

Organizations should confirm whether a potential service provider offers secure transportation of the materials to the destruction site, or whether the organization must obtain secure transportation services. Organizations should also develop procedures to ensure that the transfer of paper and electronic media for destruction is secure. When transferring to a secure destruction service provider, transfer procedures may include: appropriately documenting transfer of custody and acceptance of fiduciary responsibility by the service provider or approved secure transportation carrier. Upon receipt of the media, the service provider should document and verify the reception of all media by checking serial numbers, etc.

⁸ The secure destruction service provider's written policies and procedures should explain in detail: employee screening (including restricting high-risk people from working there); transport procedures; access control; facility monitoring; destruction time frames; the use of subcontractors; particle size requirements; the fate of the destroyed materials; indemnifications; and audit trailing (including the Certificate of Destruction).

An organization may wish to determine whether satellite locations will provide the paper records and electronic media to be destroyed directly to the approved service provider, or whether the satellite should ship the media to the central arm of the organization. If the satellite location deals directly with the service provider, the organization may choose to follow a procedure of having the authorization accompanying the records to the secure destruction facility, with a copy remaining at the satellite location.

(iv) Elements of a service provider contract

Organizations should sign a formal contract or agreement with all external service providers hired for the purpose of securely destroying records, or for transporting records to be destroyed. This will ensure that all parties fully understand their respective roles and responsibilities.

An organization's secure destruction policy should specify the required elements of a service provider contract, and may include for example:⁹

- the requirement that the service provider has written policies and procedures, which the organization should keep on file, and appended to the contract
- that the service provider accepts fiduciary responsibility to protect and destroy the organization's materials in accordance with the service provider's written policies and procedures
- that the service provider can demonstrate that it maintains indemnification coverage for any contractual liability it accepts¹⁰
- how the destruction will be accomplished, under what conditions and by whom
- the time within which records collected from the organization will be destroyed, and require secure storage pending such destruction
- that a Certificate of Destruction be issued upon completion of the destruction
- a provision that would allow the organization to witness the destruction, wherever it occurs, and to visit the service provider's facility
- that there may be announced and unannounced audits of the service provider's processes to verify adherence to the service provider's written policies and procedures
- that employees must be trained in and understand the importance of secure destruction of personal health information
- that the service provider must ensure the particles are disposed of in a secure manner and will not be placed at risk of unauthorized access

⁹ Please note, these examples of contract clauses are not intended to provide legal advice and must not be construed as such. It is prudent for organizations to consult their own legal counsel prior to entering into any agreement.

¹⁰ Note, General Liability Insurance may not cover the liability of damages resulting from non-performance of professional services. Additionally, Professional Liability (Errors and Omissions) Insurance may exclude coverage for intentional acts of employees and acts of breach of privacy.

- that the service provider must notify the organization ahead of time if any of the work is subcontracted to a third party, and that a written contractual agreement with the third party be consistent with the service provider's obligation to the organization.

F. Disposal of Securely Destroyed Materials

An organization's secure destruction policy should include a requirement to discard securely destroyed materials such as paper particles after destruction. Materials should be restricted from public access, and a record should be created documenting the destination and disposal of the media particles. Following degaussing or sanitization, access to the media must also be restricted and further distribution delayed until an internal audit of a percentage random sampling of the media demonstrates that the degaussing and sanitization process was effective. It is up to the organization to determine the appropriate percentage for random sampling.

G. Auditing and Ensuring Compliance

Secure destruction policies and procedures must be applied consistently in order to be effective. Organizations should document violations of their secure destruction policy by employees and service providers, including a description of the violation, the nature of the media, and any remedial action taken. The report of a violation can be given to the individual responsible for corporate security or human resources, or the supervisor responsible for the area where the violation occurred. Where the violation is a criminal act, a violation of contract or employment agreement, or involves the release of personal health information, the organization should determine whether law enforcement, legal counsel or the Information and Privacy Commissioner of Ontario, Canada, should be contacted.

(i) Employee compliance

Policies should detail how employee acceptance and championing of the secure destruction program will be obtained. Options for employee orientation and training may include a training class, completion of internet-based orientation training, or self study. Organizations should obtain from employees an acknowledgement to verify their understanding and agreement to comply with the secure destruction policy prior to handling any personal health information. It should also be acknowledged by the employee that complying with the policy is a basis for continued employment, and that failure to adhere to the policy could result in disciplinary action or dismissal. The organization may wish to perform employee compliance audits where a designated individual, such as the employee's immediate supervisor, records findings such as whether collection containers are deployed and compliant, and whether unused electronic equipment is secured.

(ii) Service provider compliance

When developing a secure destruction policy, consideration should be given to how a contracted secure destruction service provider could be audited, including the frequency of audits. When performing an announced or unannounced audit of a service provider, the organization should check that criminal history screening or police background checks are performed, only authorized employees have access to records to be destroyed and the processing area, each employee signs a confidentiality agreement, and there are written policies and procedures. To ensure compliance, an organization may choose to require the service provider file documents showing an update to policies and procedures, logs, employee screening, and access control.

The service provider may offer verification of its current industry association certification status such as the National Association for Information Destruction (NAID) which may satisfy an organization's auditing requirement for secure destruction. NAID Certification is a voluntary program offered to its members. The program consists of an annual audit conducted by one of a network of independent security professionals who are accredited by ASIS International as Certified Protection Professionals. Professionals audit the applicant against the security standards of the NAID Certification Program. The program also includes unannounced, random audits of NAID Certified locations by the same security professionals.

V Summary

- Organizations considering the destruction of records containing personal health information should develop a secure destruction policy that determines in advance what records should be destroyed, by whom, and when.
- The policy should describe the destruction program, including details regarding methods of in-house or outsourced destruction, and contingency planning.
- Records to be destroyed should be segregated and securely stored throughout the entire process, before and after the destruction.
- In determining the method of destruction, organizations should consider the medium of the record, whether the records require a stronger method of destruction based on their sensitivity, and whether the media will be reused internally or moved out of the organization.
- Neither recycling records nor simply placing them in the trash are acceptable methods of destruction—avoid both.
- The destruction of records containing personal health information should be documented by way of internal authorizations prior to their destruction, and a Certificate of Destruction must be created once the destruction is completed.
- Before employing a service provider that will securely destroy all records, organizations should develop criteria for choosing a provider, as well as confirming the provider’s methods of destruction and how records will be securely transported to the provider selected.
- Organizations should sign a contract or formal agreement with all external service providers hired to destroy records.
- Once materials are securely destroyed, they should be restricted from public access until disposed of permanently.
- Organizations should audit their secure destruction programs to ensure employee and service provider compliance.



VI Conclusion

Personal health information is highly sensitive and personal in nature. Yet medical data must be shared often and immediately, among a potentially wide range of health-care providers, for the benefit of the individual's well-being. The result is that personal health information often resides within a number of different organizations, each of which may have data destruction programs at various levels of development. We hope that the information provided in this *Best Practices* document will assist you in ensuring that personal health information which has reached the end of its life cycle is moved out of organizations and destroyed in a consistently secure and privacy-protected manner.

VII Resources

National Association for Information Destruction Information Destruction Compliance Toolkit
<http://www.naidonline.org>

Guidelines for Media Sanitization, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-99, September 2006
http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf

Publications available on the Office of the Information and Privacy Commissioner of Ontario's website (www.ipc.on.ca), such as:

- Fact Sheet No. 10 Secure Destruction of Personal Information
- IPC Practices No. 26 Safe and Secure Disposal Procedures for Municipal Institutions
- IPC PHIPA Fact Sheet No. 1 Safeguarding Personal Health Information
- BlackBerry® Cleaning: Tips on How to Wipe Your Device Clean of Personal Data

About the Authors

Ann Cavoukian, Ph.D., Information and Privacy Commissioner of Ontario, Canada

Dr. Ann Cavoukian is recognized as one of the leading privacy experts in the world. Noted for her seminal work on Privacy Enhancing Technologies (PETs) in 1995, her concept of Privacy by Design seeks to embed privacy into the design specifications of technology, thereby achieving the strongest protection. An avowed believer in the role that technology can play in protecting privacy, Dr. Cavoukian's leadership has seen her office develop a number of tools and procedures to ensure that privacy is strongly protected, not only in Canada, but around the world. She has been involved in a number of international committees focused on privacy, security, technology and business, and endeavours to focus on strengthening trust and confidence in emerging technological applications. Recently reappointed as Commissioner for an unprecedented third term, Dr. Cavoukian intends to grow Privacy by Design, and make it go viral.

Robert Johnson, Executive Director, National Association for Information Destruction, Inc.

Robert Johnson is the founder and Executive Director of the National Association for Information Destruction (NAID), a non-profit association promoting proper destruction of discarded information. Mr. Johnson has testified before the Canadian House of Commons, as well as before the Privacy Commissioner of Canada on the issue of proper information destruction. He served on the British Standards Institution's committee responsible for developing practices standards for information destruction firms in the U.K. Johnson is also routinely sought out by policy makers in the United States as they look to create regulations and standards concerning proper information disposal. He currently sits on the Information Asset Protection Council and the Information Protection Guidelines Committee of ASIS International. With over 27 years in the secure destruction industry, Mr. Johnson is often invited to speak and write on a wide range of issues related to the proper disposal of information, data protection legislation, compliance development and vendor selection.

Information and Privacy Commissioner of Ontario, Canada

2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
Canada

Telephone: (416) 326-3333

Toll-free: 1-800-387-0073

Fax: (416) 325-9195

TTY (Teletypewriter): (416) 325-7539

Website: www.ipc.on.ca

Privacy by Design: www.privacybydesign.ca

E-mail: info@ipc.on.ca



National Association for Information Destruction

1951 W. Camelback Rd., Suite 350
Phoenix, AZ 85015
USA

Telephone: (602) 788-6243

Fax: (602) 788-4144

Website: www.naidonline.org

E-mail: info@naidonline.org

