Guidelines for Secure Destruction of Personal Information

This section will:

- describe best practices for the secure destruction of personal information
- identify key considerations and elements of contracts with a service provider to support the destruction of records

Under PIPA a practice is expected to securely dispose of documents that contain personal information that are no longer required for legal or business/professional purposes, in order to prevent unauthorized access, inappropriate use or identity theft. The goal is to permanently destroy personal information or irreversibly erase it so that it cannot be reconstructed, whether in paper or electronic format. This includes the original records and any duplicate copies of records that may have been created for use in the practice. A service provider may be contracted to provide the record destruction services.

Industry best practices for the secure destruction of data are constantly evolving and it is generally the responsibility of all parties who handle personal information to adequately protect that personal information.

Best Practices

Best practices for the secure destruction of personal information include:

- developing and implementing a retention and secure destruction policy
- disposing of paper records securely by cross-cut shredding (do not use single-strip, continuous shredding because it is possible to reconstruct the strips)
- incinerating paper records, if practical
- disposing of personal information stored on electronic devices (such as disks, CDS, DVDs, USB storage devices, and hard drives) securely by physically damaging the item and discarding it, or by using a wipe utility to remove the original information (note that deleting electronic information does not constitute destruction, and a wipe utility may not completely erase the information)
- ensuring machines such as photocopiers, fax machines, scanners or printers with storage capabilities are overwritten, erased, removed, or destroyed when the machines are replaced
- keeping a destruction log that includes the patient's name, time period covered by the destroyed record(s), the method of destruction and person responsible for supervising the destruction (if applicable)

- conducting audits to ensure compliance by staff and service providers and that the retention and destruction policy is effective

The Ontario OIPC and NAID 2009 Guidelines for Destruction is a useful document that provides further details on destruction practices in Canada.

Using a Service Provider to Destroy Records

When contracting a service provider to support the destruction of records,

- look for one that is accredited by an industrial trade association such as the National Association for Information Destruction
- check their references
- insist on a signed contract

The contract for record destruction services usually covers these key points:

- clear description of:
  - the responsibilities of the service provider for the secure destruction of the records involved
  - how the service provider will collect the records from the practice
  - how the destruction will be accomplished for the records involved
  - what the methods are for secure storage of records pending destruction
- the limited timeframe upon which records will be destroyed
- upon request:
  - provision of a certificate of destruction documenting date, time, location, operator, and destruction method used
  - permission for an authorized person from the practice to visit the facility and/or witness the destruction
- request for proof of or requirement for employees receiving training on the importance of secure destruction of confidential personal information
- if the provider is subcontracting the destruction to a third party, require that notice be provided ahead of time with a contract in place with the third party that is consistent with the service provider's obligations to the practice

In order to have Canadian privacy protections apply to personal information, it is recommended that service providers operating within Canada be engaged. However, for a variety of reasons many service

providers operate some or all portions of their services outside the country. Be sure to understand where personal information is being stored, who has access to it, what security provisions are in place, and from what locations personal information may be accessed (e.g., if there is remote access for support).

For more information, see Guidelines for Confidentiality Agreements Service Contracts and Information Sharing Agreements and the BC E-waste website End-of-Life Electronic Equipment Recycling Program.