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 the BC Personal Information Protection Act (PIPA) a physician's office is expected to securely dispose of personal information that is no longer required to prevent unauthorized access, inappropriate use, or identity theft. The goal is to permanently destroy personal information or irreversibly erase it so that the information 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 in-office use. A service provider may be contracted to provide the record destruction services.

Best Practices

Best practices for the secure destruction of personal information include the following:

1. Dispose of paper records securely by cross-cut shredding. Don not use single-strip, continuous shredding because it is possible to reconstruct the strips. If practical, consider incinerating paper records.
2. Dispose 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 a wipe utility may not completely erase the information.
3. If office machines such as photocopiers, fax machines, scanners, or printers contain storage devices, ensure that they are overwritten, erased, removed, or destroyed when the machines are replaced.

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 (www.naidonline.org). Check the references of any service provider and insist on a signed contract. The contract should cover these key points:

1. Clearly describe the responsibilities of the service provider for the secure destruction of the records involved.
2. Describe how the service provider will collect the records from the physician's office.
3. Describe how the destruction will be accomplished for the records involved.
4. Upon request, provide a certificate of destruction documenting date, time, location, operator, and destruction method used.
5. Allow an authorized person from the physician's office to visit the facility and/or witness the destruction upon request.
6. Require—or request proof of—employees receiving training on the importance of secure destruction of confidential personal information.
7. Require that if the provider is subcontracting the destruction to a third party, that notice be provided ahead of time with a contract in place with the third party consistent with the service providers' obligations to the physician's office. The service provider must remain liable for all services performed.
8. Describe the secure storage of records pending destruction.
9. Specify the limited timeframe upon which records will be destroyed.

(For more information, see the section Guidelines for Managing Contracts and Information-Sharing Agreements. Also check the BC E-waste: End-of-Life Electronic Equipment Recycling Program at www.rcbc.bc.ca/education/hot-topics/e-waste.)

Finally, while PIPA does not include the FIPPA provisions regarding prohibition of storage and access to personal information from outside Canada, it is recommended that service providers operating within Canada be engaged. However, many service providers do operate some or all portions of their services outside the country, for a variety of reasons. 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). If any aspect of their operations are to be out-of-country, make sure the contract binds the service provider to BC's privacy requirements as they may not feel compelled to respect privacy laws beyond their own jurisdiction.