ALBERTA NETCARE PORTAL
Hardware and Information Disposal Quick Reference

When moving from an existing electronic medical record (EMR) to a new EMR, physicians and custodians of patient records must ensure that hardware replaced in the migration is securely destroyed or has health information permanently deleted. These are physician and custodian data responsibilities under the Health Information Act that must be met, so that the privacy of patient data is secure. The following information may assist physicians and custodians in this process.

DEVELOPING AN INFORMATION DISPOSAL STRATEGY

It is the physician's responsibility to make decisions related to data management and to meet the medical legal and continuity of care requirements for patient records. Patient information must be retained for a specific period of time according to the Health Information Act and the College of Physicians & Surgeons of Alberta Custodian Policy.

As custodians of patient health information, clinics are legally obligated to safeguard that information. Secure destruction techniques are an essential step in the life cycle of patient records and clinics must plan records management processes and activities that take place on a scheduled basis. It is the custodian's responsibility to securely dispose of patient records after the necessary retention period.

FIRST STEPS

1. List all hardware that contains personal health information.
2. Review the list of options and organizations that provide destruction services on the National Association for Information Destruction (NAID) Canada website. ***www.naidonline.org/ncan/en/consumer/members.html***
3. Schedule the destruction and reconcile the destruction certificates against the hardware list. Keep this information on file.
4. Moving forward, develop a strategy for destroying records on a regular schedule based upon legal requirements.

SECURE DATA DESTRUCTION

It is important to be aware that physically destroying hardware and patient information records can be difficult. Secure destruction of electronic records requires professional expertise.

According to the NAID Canada, there are four main options available for secure data destruction. Some options are more secure than others.

1. Wiping Hard Drives - Data-wiping software is available to wipe hard drives previously used in a practice or clinic.
2. Degaussing Hard Drives - Degaussing uses a reverse magnetic field to scramble electronic data in a hard drive and make stored information unreadable.
3. Secure Erase - Secure erase permanently removes information from a hard drive by prompting a pre-existing protocol coded into the hard drive by the manufacturer.
4. Physical Destruction - Physical destruction of a hard drive means to physically destroy in an irreversible manner so that the record(s) cannot be reconstructed in any way.

DESTROYING, DISPOSING OF AND RECYCLING HARDWARE

Once the data is no longer accessible, the next important consideration is disposing of the electronic waste. Most clinics and practices are likely to replace monitors and keyboards as well as computer devices over time.

- There is usually no cost—some sites may charge a tipping fee—to take the end-of-life electronics to one of over 250 collection sites across the province so they can be recycled in an effective, secure and environmentally safe manner. For details on the locations of the collection sites refer to ***www.albertarecycling.ca***.
- Recycling collection sites accept televisions, computer monitors, CPUs, keyboards, cables, mice, speakers, laptops, notebook computers, printers and other electronics.

NOTE: The information in this fact sheet is provided for education and guidance only and is not intended to replace expert advice. Physicians are responsible for making informed decisions to meet their medical-legal obligations.

RESOURCES

NATIONAL ASSOCIATION OF INFORMATION DESTRUCTION

NAID Canada is the national association representing companies that specialize in secure information and document destruction. NAID also has a Certification Program and recommends working with NAID certified providers. When NAID certified providers are used, an official certificate of destruction is provided.

For more information about NAID, see the NAID Canada website ***www.naidonline.org/ncan/en/***. It is recommended that only certified NAID service providers be used in the destruction of EMR hardware.

Review a listing of NAID service providers ***www.naidonline.org/ncan/en/consumer/members.html***. Select ***Canada- Alberta*** from the drop-down menu and check ***Yes*** to the NAID Certified option.

THE OFFICE OF INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

The Office of Information and Privacy Commissioner (OIPC) is the regulatory body for the Freedom of Information and Protection of Privacy Act, the Health Information Act and the Personal Information Protection Act (Private Sector Privacy).

The OIPC recommends the following for hardware disposal:

"…computer data storage components or portable media containing health information that requires exchange or disposal should be destroyed, or the health information should be permanently deleted through use of a commercial disk wiping utility."

For more information:

http://www.oipc.ab.ca/media/127692/H2003-002IR.pdf

THE GOVERNMENT OF ALBERTA HEALTH INFORMATION ACT

Health Information Act

www.qp.alberta.ca/574.cfm?page=H05.cfm&leg_type=Acts&isbncln=9780779724758

Health Information Act Guidelines and Practices Manual

www.health.alberta.ca/documents/HIA-Guidelines-Practices-Manual.pdf