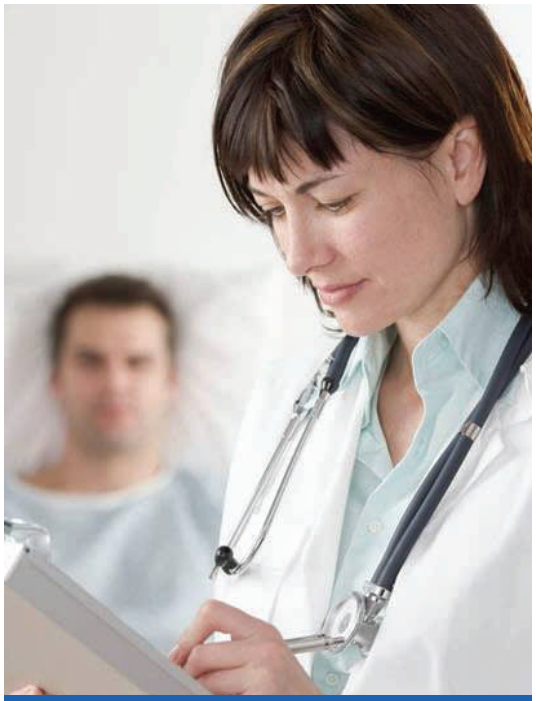
Guidelines for Safeguarding Information



Information Privacy

For information or assistance with your questions, please contact:

privacy@albertahealthservices.ca
Phone: 1-877-476-9874
Fax: 1-877-573-5107

At Alberta Health Services (AHS), it is our responsibility to respect confidentiality and privacy. This means protecting the information of our patients, clients, co-workers and AHS organizational information. Every staff member is expected to follow the *Freedom of Information and Protection of Privacy Act* (FOIP) and the *Health Information Act* (HIA) when collecting, using, accessing, disclosing and disposing of information.

Protect patient information as if it was your own.
Only collect, use, access and disclose the least amount of information necessary to perform your duties. Limit information to what you need to know to do your job, not information that is nice to know.

Access information only as required to do your job.
The ability to access information does not give us the right to. Accessing health information of family members, friends or yourself is prohibited.

Retain and dispose of records in a secure manner.
Store information securely and follow the AHS retention schedule. Materials that contain personal or health information should be disposed of securely and should never be placed in the regular garbage.

Always safeguard health or personal information.
Keep paper records secure at all times. If your job requires you to take information with you, transport only the minimum information needed for the task. Protect against unauthorized access of electronic records by locking or logging out of workstations.

Never discuss confidential information in a public forum. Do not engage in public discussions about patients, clients, employees or confidential AHS business. Be aware of who is around you when verbally sharing information. Remember social media sites are not private, always use caution and never post confidential information online.

Respect the privacy of all patients.
If a famous person, family member, friend or co-worker is receiving treatment and care, respect their right to privacy as you would anyone else's.

Limit information disclosed to the patient's family members and friends. Unless patients specify otherwise, you may tell family members and friends of patients that they are or are not in the facility, their location and their progress and prognosis on the day the family member asks.

Consider the expressed wishes of patients when disclosing information. If a patient has indicated how they want their information shared, this must be considered before disclosing information.

Ensure that the disclosure of health or personal information to anyone external to AHS is authorized.
Unless disclosure without consent is authorized by the HIA or FOIP, obtain the written consent of the individual to disclose their health or personal information. There are limited situations when consent may not be required. Contact the AHS Information & Privacy office.

Report breaches of personal or health information as soon as possible. A breach is the unauthorized collection, use, access, disclosure or disposal of personal or health information. Take immediate measures to protect against further breach of the information, advise your supervisor and contact the AHS Information & Privacy office.

AHSecure
Collect IT. Protect IT.

PROTECTING INFORMATION is everyone's responsibility

31/07/2012

Guidelines for Securing Information

IT Security & Compliance

For information or assistance with your questions, please contact:

securityincident@albertahealthservices.ca

Or your local IT Service Desk

Keeping patient and other confidential and sensitive information safe and secure at all times is everyone's responsibility. Alberta Health Services (AHS) uses consistent administrative, technical and physical safeguards to protect the security of Information Technology (IT) resources and information. AHS Information Management policies outline security risks and provide direction on how to protect information. These can be viewed on the AHS intranet Insite at:
http://insite.albertahealthservices.ca/corporate-policies.asp

Protect your user ID and password. You are responsible for all actions undertaken with your user ID. Create a password that is not easy to figure out, such as using the first letters from a song line. Do not share your password.

Never allow anyone who does not have proper credentials to access your computer. Maintain and protect the confidentiality of information accessed through the use of IT resources, and safeguard the information in your workstation from unauthorized access.

Report suspicious activity. Everyone is required to report suspected or actual incidents of improper activities involving IT resources to IT Security & Compliance.

Be careful with e-mail. E-mails to addresses outside of AHS are not secure unless they are encrypted. Visually check all e-mail addresses prior to sending the message. Ensure that messages contain the least amount of information necessary for the purpose. Use caution regarding confidential and sensitive information.

Always transport resources securely. Only store personal or health information on mobile computing devices (i.e., laptops, mobile phones, USB sticks) if there is a business need. To prevent theft, use locking mechanisms, keep information and IT resources in your possession, and use approved encryption standards to ensure the confidentiality and integrity of the information.

Safeguard against risks when faxing information. Understand the security features of your fax machine. When possible, use pre-programmed numbers. If you must enter a number manually, visually confirm it is entered correctly. Only send the least amount of information required to fulfill your purpose.

IT resources are for authorized activities only. IT resources are to be used for business purposes. E-mail accounts are corporate resources, and e-mail transmissions are owned by AHS. Occasional use of the Internet for personal reasons is permitted but abuse may result in having your Internet access restricted or revoked entirely.

Ensure confidential information is stored in a secure location. Store information on network drives, not on your workstation. Before leaving your workstation unattended, log off or lock your computer.

Prevent virus infections. Before connecting to the AHS network, make sure that devices are scanned, encrypted and have approved virus protection. Do not download software to AHS resources unless approved, and never open attachments sent by unknown or suspicious parties.