PURPOSE

- To set out conditions by which information in the custody or control of Alberta Health Services (“AHS”) may be transmitted by facsimile (“fax”) or electronic mail (“email”).

- To ensure compliance with the Health Information Act (Alberta) and the Freedom of Information and Protection of Privacy Act (Alberta).

POLICY STATEMENT

AHS is committed to employing stringent safeguards and standards for maintaining the privacy, integrity and availability of Information collected, transmitted, and stored. AHS Information shall not be used by, disclosed, or shared with unauthorized individuals or organizations.

Information classified as “Protected”, “Confidential”, or “Restricted” (see Information Classification policy (#1142)), shall be transmitted externally by fax or email under limited conditions. Information classified as “Public” may be transmitted by fax or email without restriction. Transmissions must directly relate to, and be necessary for, the purpose for which the information was originally collected and must only be directed to persons authorized to receive the information. Users (senders and receivers) are individually responsible and accountable for protecting the information being faxed or emailed.

APPLICABILITY

Compliance with this policy is required by all AHS employees, members of the medical and midwifery staffs, students, volunteers, and other persons acting on behalf of AHS (including contracted services providers as necessary). This policy is subject to all applicable laws.
POLICY ELEMENTS

1. Conditions for Fax or Email Transmission

1.1 Transmission of Protected information shall only occur:
   a) when there is a reasonable and direct connection to the purpose for which the Information was originally collected; and
   b) through approved AHS systems and procedures (see Sections 2 and 3).

1.2 Unless expressly authorized by the Information & Privacy Office, Transmission of Confidential information shall only occur:
   a) when there is a reasonable and direct connection to the purpose for which the information was originally collected;
   b) through approved AHS systems and procedures (see Sections 2 and 3); and
   c) if the information is required either for operational purposes, or to provide timely access to health services, or to provide emergent continuity of care.

1.3 Information classified “Restricted” shall only be transmitted by email to an external email account or by fax in emergency situations. Transmission of Restricted information by email shall only take place if the information is encrypted and the intended recipient can be authenticated.

1.4 Health Information shall be faxed only when the information is required immediately and no other means of obtaining secure access to the information is practical.

1.5 The fax cover sheet shall not contain Health or Personal Information other than the contact information of the individual sending and the intended recipient of the fax.

1.6 Faxed or emailed documents used for patient care purposes or containing Health Information shall be included in the patient/client’s health record in accordance with applicable AHS policies.

1.7 Staff requiring further guidance on conditions for Transmission shall consult the IT Security and Compliance Office or the Information & Privacy Office.

1.8 Information & Privacy Office may conduct spot audits without notice to ensure compliance with the requirements of this policy.

2. Fax Transmission

2.1 Fax Transmissions shall be in accordance with the Requirements for Faxing Information (Appendix “A”).
2.2 Manager/Directors (or designates) are responsible for learning the security features of their fax machines and shall ensure that Appendix “A” is posted in the vicinity of fax machines in their area.

2.3 Fax equipment shall be monitored by authorized personnel or located in a secure area unavailable to unauthorized individuals.

2.4 All fax Transmissions sent from AHS fax machines shall include a completed cover sheet containing the following disclaimer:

Confidential: This communication is intended only for the individual or institution to which it is addressed and should not be distributed, copied, or disclosed to anyone else. The document(s) in this communication may contain personal, confidential, or privileged Information, which may be subject to the Freedom of Information and Protection of Privacy Act, the Health Information Act and other legislation. If you have received this communication in error, please notify the sender immediately. Thank you for your cooperation and assistance.

2.5 In the event that a fax Transmission containing Restricted or Confidential information is sent to an incorrect fax machine, the sender shall:

a) contact the recipient and request that the document be returned immediately. If misdirected internally, the sender shall request that the document be secured and returned in a sealed envelope marked “confidential”. If the fax was misdirected externally, arrangements shall be made for an AHS-approved courier that utilizes secure methods to retrieve the documents from the recipient and promptly return it to the sender;

b) retain a copy of all information sent (e.g. AHS fax cover sheets, fax status report, and all other related documents); and

c) immediately report the event to the Information & Privacy Office.

2.6 Restricted or Confidential information requiring transfer from a central fax area to an alternate destination shall be secured in a sealed envelope marked “restricted” or “confidential” as applicable.

3. Email Transmission

3.1 External email accounts (i.e. those without an AHS address) shall not be used to send any information classified Restricted or Confidential unless the connection has been verified as secure by the IT Security and Compliance Office.

3.2 All information classified Restricted or Confidential sent to an external email account shall be encrypted. Senders unable to encrypt the email service shall contact the IT Service Desk for appropriate instruction.

3.3 Acceptable use of email service shall be in accordance with AHS Information Technology Acceptable Use policy (#1109).
3.4 The following disclaimer shall be automatically attached to each Transmission sent to an external email account:

This message, and any documents attached hereto, is intended only for the addressee and may contain privileged or confidential Information. Any unauthorized disclosure is strictly prohibited. If you have received this message in error, please notify us immediately so that we may correct our internal records. Please then delete the original message. Thank you.

3.5 Email account owners shall immediately contact the IT Service Desk for assistance where the disclaimer is not being automatically attached to email Transmissions.

3.6 Staff shall visually check all email addresses prior to sending any email to ensure it is correct. If an email message and/or attachment containing Restricted or Confidential information has been sent to an incorrect email address, the sender shall:

a) contact the recipient and request that the message and attachment be deleted immediately;

b) print out and record the corrective actions taken on a hard copy of the email message; and

c) report the event and send the hard copy of the email message to the Information & Privacy Office.

4. User Responsibilities

4.1 Users of Restricted and Confidential information are responsible and accountable for protecting the Information’s confidentiality, privacy, integrity, and availability at all times and only using such information for its intended purpose.

4.2 Prior to disclosing Health Information through encrypted email, a Repository Owner may be required to create or amend a PIA and submit it to the Information & Privacy Office.

DEFINITIONS

Breach means a failure to observe security or privacy processes, procedures or policies, whether deliberate or accidental, which results in the Information being viewed, or having the potential to be, accessed, used, transmitted or held by unauthorized persons.

Confidential means the classification applied to information where the unauthorized disclosure could cause moderate risk or harm to any individual, AHS, third-party, or to the privacy of individuals, compromise the organization’s ability to respond to disaster, or threaten the secure containment of vital records.

Health Information means information that identifies an individual and is stored in any format that relates to:
a) diagnosis, treatment and care; and
b) registration information (e.g. demographics, residency, health services eligibility, or billing).

Information Security Incident means any incident where there is a Violation or Breach of the Security of Information or a weakness or malfunction of IT infrastructure that could potentially cause a Violation or Breach, is identified.

IT Resource means any AHS-owned or controlled asset used to generate, process, transmit, store, or access AHS Information, which includes but is not limited to IT infrastructure, computer facilities, systems, hardware, software, information systems, networks, shared drives, computer equipment and devices, Internet, email, databases, applications, Mobile Computing Devices, and Mobile Storage Devices.

Personal Information means recorded information, not including Health Information, of any kind stored in any format that identifies an individual including, but not limited to:

a) address and contact Information (including an identifying number or symbol assigned to an individual);
b) race, ethnic origin, gender or marital status;
c) educational, financial, employment or criminal history;
d) opinions of others about the person; and
e) personal views and opinions of a person (except if these are about another person).

Privacy Impact Assessment means a process to assist AHS in reviewing the impact new projects might have on individual privacy.

Protected means the classification applied to information where unauthorized disclosure could cause low risk or harm to any individual, AHS, or third party. Protected information is available to AHS employees and those persons acting on behalf of AHS and who are authorized to view Protected information.

Repository Owner means the individual(s) responsible for defining the processes and controls for the assessment, storage, security, privacy, and disposition of the information in a Repository.

Restricted means the classification applied to information where unauthorized disclosure could cause serious risk or harm to any individual, AHS, third-party, or to the integrity, image, service delivery, or sustainability of AHS.

Transmission means the sending of Information (including files and images) using electronic means such as fax, email, or other technologies.

User means any person who accesses or uses an AHS IT Resource.

Violation means a particular incident or system-wide condition that violates Security or privacy policy, but does not result in a breach.
REFERENCES

- Appendix “A” - Requirements for Faxing Information
- AHS Policies and Procedures:
  - Access to Information (Physical, Electronic, Remote) (#1105)
  - Collection, Access, Use, and Disclosure of Information (#1112)
  - Contractor Requirements for Security of Information and Information Technology Resources (#1107)
  - Delegation of Authority and Responsibilities for Compliance with FOIPP and the HIA (#1108)
  - Information Classification (#1142)
  - Information and Privacy Safeguards (#1143)
  - Information Technology Acceptable Use (#1109)
  - Privacy Impact Assessments (#1145)
  - Records Management (#1133)
  - Records Retention Schedule (#1133-01)
- Freedom of Information and Protection of Privacy Act (Alberta)
- Health Information Act (Alberta)

REVISIONS
January 10, 2012
APPENDIX “A”

REQUIREMENTS FOR FAXING INFORMATION

The following minimum requirements shall be followed to avoid an information breach:

1. Users of paper and electronic fax machines shall:
   a) comply with all applicable AHS policies regarding the security of information and the protection and privacy of Health and Personal information;
   b) where possible, use the speed-dial function and the built-in security features of the fax machine;
   c) gather all the required contact information for the recipient of the fax;
   d) where possible, take reasonable measures to verify the identity of the individual receiving the fax;
   e) visually check and verify the dialled number for accuracy prior to transmitting a fax;
   f) complete the AHS fax cover sheet containing the confidentiality statement;
   g) ensure fax cover sheets do not contain Restricted, Confidential, and/or Protected information (including patient-identifying Personal or Health Information);
   h) print a transmission log report and/or record transmission in an associated fax log; and
   i) promptly remove sent or received documents from fax machine and store in accordance with AHS policies.

2. Departments shall:
   a) undertake a risk assessment to determine the need for putting fax machines in a secure area unavailable to unauthorized person;
   b) designate a person(s) to receive, sort, and file fax transmissions in a timely and secure manner; and
   c) periodically update and confirm fax number lists, including pre-programmed numbers on fax machines.

If you have any questions or comments regarding the information in this policy, please contact the Corporate Policy Department at corporatepolicy@albertahealthservices.ca. The Corporate Policy website is the official source of current approved corporate policies, procedures, and directives.