Purpose
To set out conditions by which physical records or media (paper charts, x-ray film, DVD’s, etc.) containing personal or health information may be transported to ensure the secure transfer of the information between sender and recipient, protecting the integrity and confidentiality of the information at all times.

To establish reasonable safeguards as required by the Freedom of Information and Protection of Privacy Act (FOIP) and the Health Information Act (HIA).

Policy Statement
Covenant Health is committed to protecting the confidentiality of the information and security of the records in our custody and control. All persons acting on behalf of Covenant Health utilize safeguards to protect personal and health information from unauthorized or inadvertent disclosure.

Applicability
This policy and procedure applies to all Covenant Health facilities, staff, physicians, volunteers, students and any other persons acting on behalf of Covenant Health (personnel).

Responsibility
All staff, physicians or other persons transporting physical records or media containing personal or health information are responsible to implement safeguards to ensure the confidentiality of the information contained in Covenant Health records.

Principles
1. Transportation of physical records that contain personal or individually identifying health information is carried out according to established procedures to maintain the security of the records and confidentiality of the information.

2. There are no restrictions on the methods for transporting records which do not contain personal or individually identifying health information. Normal business procedures may be followed to transfer these types of records to intended recipients.

Policy Elements
1. General Conditions
   1.1. Transportation of originals or copies of physical records containing personal or health information shall only occur when there is a reasonable and direct connection to the purpose for which the information was originally collected, or when the use or disclosure of the information is authorized under FOIP, HIA or COV policies.

   1.2. The individual transporting the records is responsible for the security of the records and protection of the information.

   1.3. Departments responsible for managing records must establish standards which define the circumstances when records may be transported from
their original location.

2. **Transportation of Records Within a Covenant Health Facility**

2.1. Records transported by interoffice mail must be sealed in an envelope, clearly labeled with the name of the intended recipient or department, marked confidential and placed in a designated, secure location for pick up by staff assigned to transport the records.

2.2. Patient names or other personal information should never be recorded on the exterior of interoffice envelopes intended for re-use.

2.3. When transporting records containing personal or health information between offices or clinical areas within a facility, the person responsible for transporting the records:

   - should cover or otherwise place out of view the patient names or other record identifiers
   - must move the records directly from their originating location to the delivery location with no unrelated stops in between
   - must not leave the records unattended in a public or non-secure area at any time

3. **Transportation of Records Outside a Covenant Health Facility**

3.1. **Transportation of Records for Care Purposes**

3.1.1. When a patient is accompanied by a health service provider, the records containing health information must be properly secured for transport and be kept under the direct control of the responsible health service provider.

3.1.2. When a patient travels alone or is transported by a private transport service or a family member, the record must be placed in a sealed envelope, courier bag, or other secure container. The envelope or container must be marked confidential, fully addressed to the intended recipient and show the return address of the department preparing the record for transport.

3.1.3. As a general rule, original health records must not leave a facility. Where an original health record is required for urgent patient care, the approval of the responsible program manager or health information management manager must be obtained prior to the record leaving the facility. It is preferable to transport copies of only the pertinent health information rather than an active original patient care record.

3.1.4. If an original record is to be sent with a patient, the receiving organization must be asked and agree to return the record to the originating facility as soon as a copy can be made or when the record is no longer required for care.

3.1.5. When a record is not accompanying a patient for direct care, the most secure method of delivery should be used. If transportation is not performed by a COV employee or physician, an approved courier service should be utilized. The identity and credentials of the courier
should be verified prior to the release of records to the individual.

3.1.6. Records shall only be sent by taxi when no courier service is available. The records should be accompanied by a staff member or other authorized person.

3.2. Transportation of Records for Other Purposes

3.2.1. Personnel shall not remove COV records (copies or originals) from any facility unless absolutely necessary to perform job related duties and when removal is approved by their direct supervisor or the Health Information Management department.

3.2.2. Records must be prepared for transport by placing them in an enclosed, non-translucent, secure container (eg. banker’s box taped shut, fastened mail envelope, closed/locked briefcase, etc.) Personal or health information should not be visible on the outside of the container.

3.2.3. The container or envelope must be marked confidential and clearly labeled with the full return address and phone number of the sender and the name of the intended recipient and full address for delivery.

3.2.4. Records being transported by private or rental vehicle must not be left unattended and visible. When the records cannot be kept under the direct control of the individual transporting them, the records must be secured in the vehicle’s trunk, or equivalent.

3.2.5. During business related travel, records containing personal or health information must not be placed in any checked bags or luggage. If overnight travel is required, the records must remain in the physical possession of the staff member or be stored securely in a safe location.

3.2.6. When transporting inactive records to an off-site storage location, standard procedures must be followed to create an inventory, box, and label the records. Information and Privacy can be contacted at privacy@covenanthealth.ca or 1-866-254-8181 for guidance.

4. Tracking Records During Transport

4.1. Methods for tracking records during transportation should be developed and implemented, particularly when transportation is not assigned to the same individual for the entire course of transport.

4.2. When transporting records by courier, it is preferable to use a courier service that has an electronic tracking system and that can provide same day service.

4.3. Where electronic tracking is not available, the sender should confirm receipt of the records by contacting the intended recipient.

4.4. If records are not received by the intended recipient within the expected timeframe, steps must be taken to locate the records. Information and Privacy should be contacted by emailing privacy@covenanthealth.ca or calling 1-866-254-8181 to report the potential privacy breach.
Transportation of Personal or Health Information

Definitions

**Health Information** means any recorded information that relates to an identifiable individual and is collected during the provision of a health service to the individual such as:
- demographics, registration, residency, health service eligibility or billing information
- diagnostic, treatment and care information

**Personal Information** means recorded information, not including health information, about an identifiable individual including, but not limited to, name, home address or contact information, race, ethnic origin, gender, marital status, educational/financial/employment/criminal history, and opinions of others about the individual.

**Record** means documents, data of information of any kind, in any medium (e.g., paper, digital, audiovisual) and in any format (e.g., documents, spreadsheet, databases, emails, blogs, website page) created, received, recorded and maintained by Covenant Health as part of its services or business. This definition does not include computer software or any mechanism that produces a record.

**Security** means employing methods to guard or protect information technology resources against misuse, theft, or other dangers, safeguarding the information held on the resources from unauthorized access or disclosure.

Related Documents

Corporate Policies:
- III-55, Records Management
- X-10, Confidentiality Agreement and Privacy Training
- X-25, Contractor Requirements for Security of Information and IT Resources
- X-40, Information Privacy Breach or Information Systems Security Incident Response
- X-45, Information Security Classification
- X-50, Information Technology Acceptable Use and Safeguards
- II-52, Human Resources Employee Files
- VII-B-255, Transfer of Patient/Resident Information and Accountability Policy

Information and Privacy Resources [http://www.compassionnet.ca/Page1507.aspx](http://www.compassionnet.ca/Page1507.aspx)

References

*Freedom of Information and Protection of Privacy Act*
FOIP Guidelines and Practices, 2009

*Health Information Act*

Revisions

N/A