Transporting Records Policy

Reviewed Date		**Number**	IM0121
Revised Date		**Approved Date**	February 11, 2020

Introduction

In the course of the day-to-day operations of the Simcoe Muskoka District Health Unit, corporate and client records are created. The security of health unit records must be ensured regardless of the format in which the information is saved and status of the record. Some records may include confidential and sensitive information including personal health information, personal information and/or corporate confidential information. Sensitive confidential records are protected to ensure client privacy and health unit integrity. Records containing personal health information receive the highest level of protection as required by law and legislation.

Purpose

To inform Simcoe Muskoka District Health Unit Board of Health members, employees, students, volunteers and consultants of the parameters for transporting health unit records and the safeguards that must be taken when doing so.

Legislative Authority

Personal Health Information Protection Act (“PHIPA”) (Ontario)
Personal Information Protection and Electronic Documents Act (“PIPEDA”) (Canada)
Municipal Freedom of Information and Protection of Privacy Act (“MFIPPA”) (Municipal)
Health Protection and Promotion Act (“HPPA”) (Ontario)

Policy Definitions and Interpretation

***Active records*:** Official records currently in use and/or referred to, and must be immediately available for reference.

Administrative staff: Refers to Administrative Coordinators, Executive Assistant, Administrative Assistant, Program Assistants and Data Management Assistants.

Agency approved case: Any agency-issued carrying container used to transport records. These containers should be lockable or sealable.

***Breach*:** An incident where sensitive and/or confidential information is lost, misplaced, accessed, retained, disclosed or disposed of in a manner that does not comply with applicable legislation or agency policies.

***Corporate confidential information*:** Information maintained by the health unit that is not routinely made publicly available, including financial, administrative, commercial and technical information. Can also include records containing legal advice and employee-related information.

Courier*:* A contracted bonded company used to transport records.

***Electronic tracking system*:** A security measure that enables the location of an object or vehicle to be monitored using GPS or similar technology.

Employee - includes all full time, part-time, contract, temporary, or casual staff.

Non-employee - includes Board Members, externally contracted individuals/service providers, volunteers and unpaid students.

Health Unit: Means the Simcoe Muskoka District Health Unit

Inactive record: Official record that is needed to meet long-term operational, legislative compliance or historical requirements, and does not need to be available for immediate access.

Lost or stolen record: A record is deemed to be lost or stolen if there is concrete evidence of loss or theft or if the records have not been located within 24 hours.

Official record: A legally recognized document that provides evidence of business activities, decisions and transactions and is managed within a records classification system. These records are required to meet financial, legal, regulatory, operational, historical or other legislative obligations. E.g. briefing notes, policies, directives, approved minutes, materials of historical or research importance, contracts.

***Non-record*:** Documents and materials available from public sources. E.g. magazines, books, catalogues, journals.

Record: Any record of information however recorded. This includes correspondence, minutes, reports, photographs, computer tapes and disks, files, and any other recorded information regardless of medium or format.

Record tracking log: A form used to track the transportation of health unit records for purposes other than the execution of job duties.

Security: A term which embodies the concepts of confidentiality, integrity, and access.

Sensitive confidential: A term which encompasses personal health information and/or corporate confidential information.

***Transitory record*:** A record of temporary usefulness that is not managed within a records classification system and is needed only for a limited period for the completion of an action or preparation of a document. These records are not required to meet financial, legal, regulatory, operational, historical or other legislative obligations and are destroyed before the end of the retention period which applies to the correlating official record. E.g. copies used for convenience, draft documents, working materials used in preparation for the final version, meeting requests.

***Transport*:** The movement of official and transitory health unit records between SMDHU locations and/or for the execution of job duties.

Policy

Simcoe Muskoka District Health Unit will ensure systems and processes used to transport records protect against loss, damage, breach, destruction, unauthorized change and/or access and are in compliance with applicable legislation. Simcoe Muskoka District Health Unit employees and non-employees are responsible for ensuring that the transportation of health unit records in their possession is done in accordance with this policy.

Removal of sensitive confidential information from health unit locations and/or network is prohibited except when in transit between health unit locations or when necessary for the execution of job duties and in either case, only in the limited circumstances outlined in this policy.

Procedures

A. Transporting Sensitive Confidential Records

1. Only remove records containing sensitive confidential information from Simcoe Muskoka District Health Unit (SMDHU) locations and/or make copies of records saved to SMDHU network in the following limited circumstances:
   - providing care and/or delivering service in the community
   - transporting records to a storage or destruction facility
   - another authorized purpose
2. Only the minimum information is removed and/or copied, and only for the least amount of time necessary to complete the task.
3. Electronic sensitive confidential information must be encrypted, protected with sufficiently strong passwords and follow the health unit policy on Use of Portable Electronic Storage Devices if the information cannot be de-identified.
4. Sensitive confidential information stored in hardcopy is returned to SMDHU location and removed from electronic devices as soon as no longer needed
5. Sensitive confidential records transported by courier should be done by a service that has an electronic tracking system, requires an electronic signature, and can provide same day or overnight service whenever possible. Refer to Appendix A: Courier Options.

B. Transporting Active Records by SMDHU Employees or Contracted Services

1. SMDHU employee and non-employees secure and protect SMDHU sensitive confidential active records while transporting by:
   a. ensuring that information about the records is entered into the Sensitive Confidential Active Record Tracking Log (IM0121-F1)) [internal tracking mechanism by admin staff]
   b. using an agency approved container
   c. keeping records under lock and key while in transit
   d. never leaving records unattended in public areas
   e. removing records from transport vehicle as soon as possible
   f. taking the most direct route to the destination and avoiding stops in transit if possible
   g. limiting access to records by unauthorized individuals
   h. limiting the transportation to one person for the entire course of the transport where feasible.
2. Hard copy records and/or electronic devices temporarily left in an employee's vehicle are to be placed out of view, in a locked (where possible) agency-approved container and in the trunk of a locked vehicle, where possible.
3. Records kept in an employee's residence must be secured where sensitive confidential information cannot be breached, damaged, destroyed and/or accessed by unauthorized individuals.

4. Couriers must have control of SMDHU records while in transit, and should move records from their originating location to the delivery location with no unauthorized stops.
5. Records must be prepared for transport by placing them in an agency approved container which must be clearly labelled with the full return address and phone number of the agency. If transported by a contractor, the name of the intended recipient and the full address and phone number for the delivery must be visible. If transported by an employee, the name and location of the intended recipient must be clear, as long as there is a recipient. This does not apply when an employee is transporting records in the normal course of their work.
6. Sensitive confidential information should not be visible on the outside of the agency approved carrying case and entered into the **Active Sensitive Confidential Records Tracking Log (IM0121-F1).**
7. Program-related records should be addressed to 'PROGRAM NAME – ADMIN SUPPORT' e.g. HBHC Administrative Support so that the package will not sit on any employee's desk or mail slot if that person is away from the office.
8. Corporate confidential records should be marked 'confidential' and directed to the intended recipient and not opened by administrative staff.

C. Tracking Active Sensitive Confidential Records during Transportation

1. All active sensitive confidential records for transportation must be entered into the **Active Sensitive Confidential Records Tracking Log ("Log", IM0121-F1)** so that information about the records being transported is available should they go missing in transit.
2. Logs are located within a Transporting Active Records folder in the I:Drive and within these folders they are organized by year and originating office.
3. Information in the log is entered and maintained by administrative staff who have access permissions.
4. Employees must provide the appropriate administrative staff with the required information for the log when requesting use of a courier to transport sensitive confidential active records
5. Administrative staff responsible for sending the records will verify in the log that the records have been received within 2 business days of being sent.
6. Employees receiving the records must inform the appropriate administrative staff of their receipt so that they can update the log.
7. Administrative Coordinators are to review their logs quarterly, at a minimum, to ensure that the required information has been fully entered and that all transported records are accounted for.
8. The logs are retained for the current year plus one additional year.

D. Transporting Inactive Paper Records by SMDHU Employees or Contracted Service

1. SMDHU employee and non-employees secure and protect SMDHU inactive paper records while transporting by:
    a. using an agency approved container, locked where possible
    b. keeping secure while in transit
    c. taking the most direct route to the destination and avoiding stops in transit if possible.
    d. limiting access to records by unauthorized individuals
    e. limiting the transport vehicles to one where feasible
    f. ensuring same day delivery

2. All inactive records are processed prior to transportation as outlined in the **Inactive Paper Record Transfer Form (IM021-F3)** so that information about the records being transported is available should they go missing in transit.
3. Administrative staff are responsible for preparing inactive records ready for transport and completing Section A of the Inactive Paper Record Transfer Form.
4. The completed Transfer Form is faxed to the appropriate Records Liaison.
5. The receiving Records Liaison is responsible for verifying that all records are accounted for and completing Section B of the Inactive Paper Records Transfer Form.
6. The receiving Records Liaison forwards the completed Inactive Paper Records Transfer Form to the Records Administrator.
7. The Transfer Forms are retained for the current year plus one additional year.

E. Record Transport Breach

1. A record transport breach is deemed to have occurred if:
    a. the records did not reach their destination
    b. the container used to transport the records appears to have been tampered with
    c. the records are lost or stolen or breached.
2. The employee who discovers a record transport breach or potential breach must notify their manager or supervisor immediately and take action to contain the breach.
3. The agency privacy breach policy and procedures are to be followed.

Appendix

Appendix A – Courier Options

Related Forms

IM0121(F1) Sensitive Confidential Active Record Tracking Log

IM0121(F2) Label for Sensitive Confidential Active Records

IM0121 (F3) Inactive Paper Records Transfer Form

Related Policies

TQ0107 Use of Portable Electronic Storage Devices

TQ0101 Acceptable Use [Policy]

OP0110 Work From Home

IM0101 through IM0108 Information Management Policies

IM0110 Records Management

Final Approval Signature: _____

Review/Revision History:

Appendix A: Courier Options

There are three types of courier currently used at the health unit, depending on the type of record that needs to be transported from office to office. The three options are:

1. Moving Company is used to transport several boxes of records, non-stop from office to office. Currently SMDHU uses Dwinnels.
2. Contracted courier requiring an electronic signature is used to transport sensitive confidential records that required the highest level of protection and tracking. This service, though more costly than other services, is used when the risk of records loss or destruction warrants the expense. Currently SMDHU uses Purolator.
3. Contracted courier is used to transport important and/or confidential records that do not require the same level of protection and tracking as in # 2. SMDHU currently uses OMS.

A. Inactive Records – multiple boxes that are transferred to Barrie, 15 Sperling Drive for inactive storage. The health unit uses option #1, specifically Dwinnels, for transferring these records.

Examples of Records:

- Group records over 2 years old that will be stored in the records storage room at 15 Sperling Dr.
- Individual HBHC client records that have been closed/discharged for current plus 4 years and are being transferred to 15 Sperling for inactive storage

B. Active Records – Sensitive Confidential – The health unit currently uses option #2, specifically Purolator, for transferring these records. An exception would be specimens sent by the Infectious Diseases and Sexual Health programs after regular business hours when OMS (option #3) is used.

Examples of Records:

- Sexual Health or HBHC active client files where client has moved to another office's catchment area
- Rabies records where victim name is included
- Completed staff WSIB form
- Employee contract
- Financial reports for senior management only
- Tick submission in blue locked EHD bag
- Immunization child care records
- Affidavits/Medical Exemptions

C. Active Records – not Sensitive Confidential – These records can still be considered confidential and important. The health unit currently uses option #3, specifically OMS courier, for transferring these records. An exception would be for the Muskoka offices where OMS does not provide service and Purolator is used.

Examples of Records:

- Special event applications
- Food handler exams in locked blue EDH bag
- Staff PERs (inside sealed envelope marked 'personal')
- Expense reports
- Money and petty cash report to finance in locking finance bag