Electronic Document Imaging (EDI) Policy

Reviewed Date		Number	IM-0123
Revised Date		Approved Date	September 29, 2022

Introduction

The Simcoe Muskoka District Health Unit (SMDHU) supports electronic document imaging (EDI), which is the conversion of physical documents to electronic documents using fax, scanning, or photographic technologies. Document imaging enables remote and efficient access to, and management of, electronic documents, many of which will be official Health Unit records, wherever they are located.

Purpose

The purpose of this policy is to inform Health Unit employees and students of procedures in relation to the creation and management of imaged documents and records. The procedures enable effective management of the documents and records. They also ensure the accuracy and trustworthiness of the electronic images which may replace original hard copy records.

Legislative and Standards Authority

The Health Unit's practices relating to document and record imaging are governed by:

- *Copyright Act*, (C-42) *R.S.C., 1985*
- *Evidence Act, R.S.O. 1990*
- *Information and Privacy Commissioner of Ontario, "FIPPA and MFiPPA: Bill 8 – The Recordkeeping Amendments" (December 2015)*
- *Information and Privacy Commissioner of Ontario, "Improving Access and Privacy with Records and Information Management" (November 2016)*
- *Municipal Freedom of Information and Protection of Privacy Act. R.S.O., 1990, (MFIPPA)*
- *National Standard of Canada; CAN/CGSB-72.34-2017 "Electronic records as documentary evidence" (October 2018)*
- *Personal Health Information Protection Act, S.O.2004 (PHIPA)*

Policy Definitions and Interpretation

See full set of terms and definitions in *Appendix A: Additional Policy Definitions*

Imaged Document or Record: An imaged document may be a record or non-record created by electronic fax, scanner, or digital photography (including photo taken on mobile phone), and may or may not be digitized (i.e., a 'picture' rather than text that is machine readable, editable, or searchable).

Official record: A legally recognized document that provides evidence of business activities, decisions, and transactions. These records are required to meet financial, legal, regulatory, operational, historical, or other legislative obligations.

Examples of Official Records: key internal and external communications including, briefing notes, policies, directives, approved minutes, formal plans, contracts

Unofficial records: include Transitory and Non-records

Transitory Records: Records that have temporary, limited or no business value or significance for the Health Unit and are ***not*** required for financial, legal, operational, historical, and other official requirements. Examples include drafts, copies, miscellaneous administrative notices.

Non-records: Documents that are not considered a Health Unit record and would include personal messages or publicly published and available items such as books, brochures, or superseded or obsolete blank forms or templates.

Personal Health Information: Identifiable information about an individual if the information:

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,
- relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual,
- is derived from the testing or examination of any such body part or bodily substance,
- is the individual's health card number, or,
- Identifies an individual's substitute decision-maker.

Record Series: Group of records that are normally created, processed, used, and maintained together, as a unit, in support of the same activity, function or business process. They are evaluated as a unit for retention and disposition purposes.

***SMDHU Sensitive or Confidential Information*:** Includes information maintained by SMDHU that is not routinely made publicly available, including financial, administrative, legal, employee-related, and technical information.

Policy

SMDHU will ensure any imaged document is managed in compliance with Health Unit standards, relevant legislation, and industry standards that are subject to the same legal, fiscal, regulatory, and operational requirements as physical and other electronic records.

SMDHU will ensure imaged documents fulfill evidentiary requirements. All imaging must be processed in compliance with *Appendix B: SMDHU EDI Quality Assurance Guideline* to ensure the authenticity, integrity, reliability, and accuracy of SMDHU electronically imaged records. If all conditions are met in managing imaged records, the requirement to retain the physical copy could be eliminated.

If the imaged record is deemed the official record i.e., not a copy, any original hard copy source documents should be destroyed (see details in Procedures below).

Procedures

When using a scanner, the default is that images are saved to a temporary storage location on the SMDHU network. Staff must select one of the following options on the scanner menu -T:\ drive, I:\drive or M:\drive and the relevant department and program (see next section).

Scanner Menu – Four Options for Saving Images

1. **T:\ drive for General Documents/Records**
    a) For documents or records that are not defined as secure or confidential or are not part of a group of records for program service delivery. Examples of acceptable documents include information brochures or packing slips etc.
    b) **Scanner Menu Selection**: From the scanner menu, choose one of the team (program) folders on the T:\drive, e.g.,
        - T-CFH-HBHC
        - T-CSD-ID
        - T-EHD-SW
        - T-HRI-IT
        - T-PFF-ADMIN
    c) **Retrieve the image from:** T:\drive > DEPARTMENT NAME > PROGRAM NAME > "Imaging" folder

2. **I:\drive for Sensitive or Confidential Documents/Records**
    a) For secure or confidential documents or records related to program service delivery with specific procedures and access permissions that managers have developed (see *Appendix C: Instructions to Develop a New EDI Process*).
    b) **Scanner Selection**: Choose the appropriate folder e.g.:
        - I-CSD–OH
        - I-CFH-HGD
    c) **Retrieve the image from**: I:\drive >Agency Imaging > DEPARTMENT NAME > PROGRAM NAME

3. **M:\Drive for Sensitive or Confidential Department Documents/Records**
    a) For documents or records for Management (include managers, vice-presidents, administrative coordinators).
    b) **Scanner Selection**: Choose the appropriate folder:
        - M-CFH
        - M-CSD
        - M-EHD
        - M-HRI
        - M-PFF
    c) **Retrieve the image from:** M:\drive > DEPARTMENT NAME > "Imaging" folder

4. **M:\Drive for Sensitive or Confidential Executive Documents/Records**
    a) For documents or records exclusively for Vice Presidents and the Admin Coordinator
    b) **Scanner Selection**: Choose the appropriate folder:
        - M-CFH-VP
        - M-CSD-VP
        - M-EHD-VP
        - M-HRI-VP
        - M-PFF-VP

c) Retrieve the image from: M:\drive > DEPARTMENT NAME > “Admin” folder (only accessible by A/C and VP)
d) Note the office of the Medical Officer of Health has a dedicated scanner and their process is unique to that scanner.

Saving Images Using Electronic Faxing System

1. Images sent via an electronic fax server to a network folder, or a shared email inbox are managed in the same way as scanned images in I**:\drive for Sensitive or Confidential Documents/Records** (see *Appendix C: Instructions to Develop a New EDI Process*).

Image Storage Locations

1. Imaged documents must be moved from the temporary locations to the intended final location on the network immediately after quality checks are complete.
2. The final intended location may include structured databases such as CHRIS, CCM, Hedgehog, Dynamics 365, etc. Imaged documents or records are not to be saved to personal desktops where only one person can retrieve the images, and no one can audit to ensure the repository is emptied.

   See *Instructions for Using Imaging Devices* for links to detailed user manuals.

Developing New EDI Process

1. Any new scanning or e-faxing EDI process that requires storage in a secure location (i.e. I:\drive for Sensitive or Confidential Documents/Records) also requires program manager(s) (process owner) to develop written procedures (see Appendix C: Instructions to Develop a New Electronic Document Imaging (EDI) Process) with consultation of IT and RIM (Records and Information Management) staff. Consultation ensures the procedures align with RIM and IT standards and best practices.

Destruction of Original Hard Copies of Sensitive or Confidential Records

1. Original hard copy record(s) can only be destroyed if the corresponding EDI process (as noted above) has been completed.
2. Destruction of the record(s) must be approved by the program manager and department Vice President.
3. The original hard copy record(s) must be shredded and disposed of within 60 days after the imaging process is complete.
4. A record must be kept of the approval for destruction of the original hard copy records, and that the destruction of the hard copy record has occurred.
5. Original hard copy records cannot be destroyed where contractual, legal, or regulatory requirements dictate that an image is not an acceptable format for retention of the record.
6. Hard copy records that have deemed to have a permanent retention value, will be deemed the official record copy until such time as the corresponding digital records are maintained in a digital preservation system.

Copyright

All Health Unit employees must avoid copyright infringement as per SMDHU policy PR0102 – Agency Copyright and Use of Images, Audio and Video.

Appendix

1. Appendix A: Additional Policy Definitions
2. Appendix B: EDI Quality Assurance Guideline
3. Appendix C: Instructions to Develop a New Electronic Document Imaging (EDI) Process

Related Policies (SMDHU)

- IM0101 Personal Health Information Privacy Policy
- PR 0102 Agency Copyright and Use of Images, Audio and Video Policy
- IM0120 Fax Policy

Related Guidelines and Procedures (SMDHU)

- Instructions for Using Imaging Device

Final Approval Signature: _____

Review/Revision History

Appendix A: Additional Policy Definitions

Term	Definition
Admissibility (of Records)	The capability of recorded information to be introduced as evidence in a legal proceeding.
Digitized Document or Record	A digitized document or record is machine readable, editable, or, searchable. Images (i.e., a picture of text) can be digitized with an optical character recognition (OCR) program.
Dots Per Inch (Dpi)	The measure of output of the device resolution and quality (e.g., number of pixels per inch used when printing with ink or toner). Measures the number of dots horizontally and vertically. Generally, 300 dpi is recommended for imaging. Lower than that and the readability is compromised, more than that increases computer resources and processing time.
Imaging	Imaging is the process of capturing documents by reproducing their appearance through faxing, scanning, photography, or micrographics to convert them to electronic images that are stored in a computer electronically.
OCR Technology (Optical Character Recognition)	OCR software recognizes text characters in images and converts them into machine-readable text. OCR engines take time and use system resources.
Official Record Owner	The official record owner is identified in the ***SMDHU Records Classification Retention and Disposition Schedule*** and has the responsibility for maintaining the official records series.
Original (Source) Record	The original record from which an electronic image is made.
PDF Or Portable Document Format	The file format which captures formatting information from a variety of applications and makes it possible to transmit and display documents in an identical way, independent of the platform. Preferred in SMDHU for document management vs other formats such as .jpg, .png, .tiff etc.
PDF/A Or Portable Document Format/Archival	The file format based on a subset of the Adobe PDF format that is optimized for the long-term archiving of electronic documents.
Record	Any document made or received by an organization in the course of business, **regardless of form or characteristics, recorded physically, graphically, mechanically, electronically, digitally, or by any other means. Records are required to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of the organization.**
Records And Information Management (RIM)	The field of management concerned with the creation (making, receiving, or capturing), maintenance, use and disposition of records.
Records Classification	The systematic organization of records in groups or categories according to methods, procedures, or conventions represented in a plan or scheme.
Records Disposition	The final action taken on a record that has met its prescribed retention period. E.g., destruction, migration, conversion, preservation.
Records Retention Period	The specified period of time that records are kept to meet operational, legal, regulatory, fiscal, or other requirements.

Appendix B: EDI (Electronic Document Imaging) Quality Assurance Guideline

Introduction

This guideline provides direction to create and dispose of electronic imaged documents that serve as official Health Unit records.

For any assistance in understanding and implementation these processes, please contact the Records Administrator.

Quality Control (For ALL staff)

Quality control occurs during and immediately after scanning, electronic faxing, or digital photographing to ensure that the imaged document mirrors the original hard copy source document. Verification is necessary to determine that the image captures the full details of the original document and that it is completely readable.

The process must create sufficiently high-quality electronic substitutes of physical documents so that the electronic substitute will serve ongoing business needs as well as unanticipated future requirements.

Errors in document imaging can occur due to issues including document misfeeds or poor-quality original physical documents. To avoid errors, complete the following:

1. Count the number of pages to ensure the same number of pages of the digital document matches that of the physical document (take note if multi-sided; use fax cover sheet to know the number of pages in original).
2. Ensure images are in the correct order.
3. Ensure all parts of the original hard copy source document are legible.
4. Ensure the condition of the image is adequate (avoid using a hard copy source document that is folded, faded, crumpled, thin).

Audits (For Managers and Administrative Staff)

The procedures and workflow chart developed by the program will specify which audits are to be conducted, when and by whom.

- Audits will be completed by assigned staff to ensure procedures are followed. These audits should include:
    - information is cleared daily from temporary storage locations
    - information is processed according to the procedures
    - access permissions are up to date
    - naming conventions are followed
    - retention and disposition is completed

Appendix C: Instructions to Develop a New Electronic Document Imaging (EDI) Process

Program managers will prepare procedures to outline the creation and management of imaged documents and records to ensure the integrity of an organization's electronic records system. This is particularly true if the imaged documents are intended to become official records and thereby provide legal admissibility and defensibility of the electronic-only record.

There is some risk that records saved in the **I://drive** may not be deemed admissible in certain legal proceedings because these records can potentially be modified. However, if these records are maintained in structured databases e.g., Panorama, Hedgehog, ISCIS, CHRIS, where records cannot be altered and audit trails exist, these records would be admissible.

Instructions
The instructions should include these components:

1. Purpose: a brief description of what is to be achieved with document imaging
2. Imaging method, e.g., scan, e-fax, photography etc.
3. Storage locations (network, structured database)
4. Organization - How documents are organized and naming standards
5. Flow of work for each phase or each location and format (hard copy or electronic)
6. Outline if records contain any private information and/or personal health information
7. Access – who has permission to access folders
8. Which records are official, and which are transitory
9. Retention and Disposition of records:
10. Responsibilities - who maintains records
    a. Quality checks – who does which quality checks and when in the process
    b. Audits – Which audit checks are done when and by whom
    c. Training – who is trained, who facilitates training

When complete:

Please forward the new process to the departmental Records Liaison and the Agency's Records Administrator and initiate a ticket for IT and attach the documented process. Records and Information Management (RIM) and IT staff will review the process to ensure it includes details on the life cycle of the record(s) (i.e., the flow and management of the document from its creation to its final disposition). Please contact the Records Administrator if you have questions as you are documenting the process.