Saskatoon Health Region	**POLICY** Number: 7311-75-010 Title: Information Classification, Labelling and Handling
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Enterprise Risk Management Cross Index: 7311-25-006 Date Approved: June 20, 2011 Date Revised: June 6, 2019 Date Effective: June 9, 2015 Date Reaffirmed: Scope: SHR and Affiliates

SECTIONS OF THIS POLICY ARE SUPERSEDED (REPLACED) BY SASKATCHEWAN HEALTH AUTHORITY POLICY:

SHA-07-004 CORPORATE AND PERSONAL HEALTH INFORMATION GOVERNANCE

DEFINITIONS

All staff means SHR employees, practitioner staff, professional staff, affiliates, contractors, vendors, students and volunteers.

Anonymous means information collected without identifiers that cannot be used to identify the individual to whom it relates, and cannot be linked to other information that would lead to identification of the individual to whom it relates.

AVERT (Application Verification of Enterprise Risk and Threats) **Toolkit** consists of a collection of standards, checklists, and technical assessment software tools that support the evaluation and documentation of risk and security vulnerabilities for new applications. The AVERT process evaluates whether business, technical, and information system processes are in compliance with SHR IT policies and standards, thus ensuring that the security controls on personal health information continue to be effective and extensive.

IT (Information Technology) Assets means computer hardware (e.g. desktop computers, laptops, tablet PCs, etc.), printers, MFPs (Multi-Function Printers), printer ribbons, fax machines, cell phones, smart phones, desktop telephones or electronic storage that could store (or may reasonably be expected to store) internal/confidential SHR information (i.e. information that is not in the public domain) such as USB keys, CDROMs, DVDs, and VHS or cassette tapes. IT Assets can sometimes contain environmentally hazardous material.

Medical Equipment means instruments used in diagnostic and treatment procedures of patients/clients and classified as Class III or IV medical device by Health Canada. Examples include, but are not limited to, intravenous pumps, ventilators, cardiac monitors, and other diagnostic equipment.

Personal Health Information (PHI) means[1], with respect to an individual, whether living or deceased:

(i) information with respect to the physical or mental health of the individual;
(ii) information with respect to any health service provided to the individual;
(iii) information with respect to the donation by the individual of any body part or any bodily substance of the individual or information derived from the testing or examination of a body part or bodily substance of the individual;
(iv) information that is collected incidentally to the provision of health services to the individual;
(v) registration information (e.g. demographic information).

Privacy Impact Assessment (PIA) means an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form; and (iii) to examine and evaluate protections for handling information to mitigate potential privacy risks.

1. PURPOSE

The purpose of this policy is to establish the requirements for information labelling, disclosure, storage and destruction relating to information held by Saskatoon Health Region (SHR).

2. PRINCIPLES

2.1 SHR is responsible for ensuring information within its responsibility is maintained with an appropriate level of protection.

2.2 Classification of information is determined based on the type of information, sensitivity of the information and the potential for negative impact to SHR or our patients/clients/residents.

3. POLICY

3.1 This policy applies to all information within SHR regardless of storage medium (e.g. paper, CD, electronic system) and regardless of form (e.g. text, voice, video).

3.2 Information Classification

3.2.1 Information shall be classified and labelled to indicate the need, priorities and degree of protection. Information has varying degrees of sensitivity and criticality and some may require additional levels of protection or special handling. Refer to Information Security Classification and Standards Chart (Appendix A).

3.3 Default Information Classification

[1] HIPA Section 2 (m)

3.3.1 All personal health information (PHI) will be assumed "Confidential" and protected with the necessary measures.

3.3.2 Any information other than PHI that is not classified by the information owner will be assumed to be "Internal" and will be protected with the necessary measures.

3.4 Classification Guidelines

3.4.1 Business and legislative requirements shall be used to assist in information classification. In the cases where technology based applications are used to collect and maintain information the Privacy Impact Assessment (PIA) and Application Verification Toolkit (AVERT) may be used to assist in the classification process.

3.4.2 SHR maintains the following three classification levels (refer to Appendix A - Information Security Classification and Standards Chart):

- **Public:** Non-sensitive information available to the general public.
- **Internal:** Information that is generally available to health stakeholders and approved non-health stakeholders with a legitimate business need to know. This does not include personal health information.
- **Confidential:** Information that is sensitive and is intended for use only by specified, approved groups of stakeholders for a specific purpose.

4. ROLES AND RESPONSIBILITIES

4.1 All Staff

4.1.1 Ensure that all information is classified and all confidential information is labelled so appropriate protection methods can be implemented.

4.1.2 Follow regional standards and departmental protocols for information access, storage, transport, reproduction, and disposal that are appropriate to the classification of the information they are working with.

4.1.3 Employ reasonable physical security measures to protect information from view or theft when viewed or stored on IT Assets or removable media, especially when in a public place.

4.1.4 Immediately report any incident or suspected incidents of unauthorized information access, loss, and/or disclosure to their manager.

4.2 Directors/Supervisors/Managers

4.2.1 Provide assistance to staff in relation to this policy.

4.2.2 Implement a departmental protocol for ensuring information is classified and corresponding levels of protection are in place.

4.2.3 Immediately report any incident or suspected incidents of unauthorized information access, loss, and/or disclosure to the SHR Privacy and Access Department.

4.3 Privacy and Access Department

4.3.1 Respond and investigate potential breaches of this policy, when appropriate.

4.3.2 Provide assistance to staff and Managers in relation to this policy.

5. POLICY MANAGEMENT

The management of this policy including policy education, monitoring and implementation is the responsibility of the Privacy and Access Department. Amendment is the responsibility of the Director, Enterprise Risk Management.

6. NON-COMPLIANCE/BREACH

Non-compliance with this policy may result in disciplinary action up to and including termination of employment and/or privileges.

A privacy breach may be reported to the Information Privacy Commissioner (IPC). The IPC and the Ministry of Justice may charge an individual with an offence under HIPA. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment.[2]

7. REFERENCES

Other relevant policies include:
SHR Policy *Email Acceptable Use*
SHR Policy *Internet Acceptable Use Policy*
SHR Policy *Emailing Personal Health Information*
SHR Policy *Facsimile (FAX)*

[2] HIPA Section 64(1)

PROCEDURE Number: 7311-75-010 Title: Information Classification, Labelling, and Handling	
Authorization [ ] President and CEO [X] Vice President, Finance and Corporate Services	Source: Director, Enterprise Risk Management Cross Index: 7311-25-006 Date Approved: June 20, 2011 Date Revised: June 6, 2019 Date Effective: June 9, 2015 Date Reaffirmed: Scope: SHR and Affiliates

1. PROCEDURE

PORTIONS OF THIS SECTION HAVE BEEN REMOVED. PLEASE REFER TO SHA-07-004.

1.1 Determination of Information Classification

1.1.1 Classification will be determined based on the type of information, sensitivity of the information and the potential for negative impact to SHR or our patients/clients/residents. SHR maintains the following three classification levels (refer to Appendix A - **Information Security Classification and Standards Chart)**:

- **Public:** Non-sensitive information available to the general public.
- **Internal:** Information that is generally available to health stakeholders and approved non-health stakeholders.
- **Confidential:** Information that is sensitive within the health information system and is intended for use only by specified groups of health stakeholders.

1.1.2 If unsure how to classify specific information, refer to Information Security Classification and Standards Chart (Appendix A). If still in doubt, contact the SHR Privacy and Access Department.

1.2 Labelling

1.2.1 Information deemed Public or Internal does not need to be physically labelled in any way.

1.2.2 Any documents deemed 'Confidential', other than documents containing personal health information, must be marked with this text clearly in the header and footer or by watermark. If the material is already printed and has not been word-processed, it should be hand-written with this text in the top and bottom margins of the first page and stapled together.

1.2.2.1 Any document containing personal health information will be deemed "Confidential" and labelling, although recommended, is not a requirement.

1.2.3 Labelling requirements pertain to all information on all media types such as removable media (e.g. USB keys and CDs). These should be labelled with the text 'Confidential' on the media's label.

1.2.4 If internal mail envelopes are used to pass such information between inter-office or regional staff, the above marking should also be included on the outside of the envelope.

1.3. Storage

All information should be stored in a manner appropriate to its classification, as follows.

1.3.1 **Public**

1.3.1.1 As this is information that is freely available to anyone, it does not require any safe storage, but periodical backups will be maintained for Business Continuity Planning / Disaster Recovery Planning reasons.

1.3.2 **Internal (Default)**

1.3.2.1 The information is not required to be marked in any way. However, safe storage and shredding are still required.

1.3.3 **Confidential**

1.3.3.1 Confidential information must be secured under lock at the end of each day, or when not being used or under direct supervision. This applies regardless of the format that this information is held on (e.g. paper, disk, files, tapes, faxes, post). Some confidential information may not be able to be physically locked away and therefore should be protected by applying passwords or encryption to information held electronically.

1.3.3.2 Information classified as confidential shall not be stored on unrestricted shared network drives or folders.

1.3.3.3 Confidential information should not leave SHR facilities (e.g. employee's homes) without management approval, unless in accordance with departmental policies and job duties (eg. community workers).

1.3.3.4 Care must be taken when verbally discussing (including mobile phone conversations) confidential information in public places or on public transport in order to ensure the conversation is not overheard. The same applies for messages that can be left on answering machines, voicemail and information which is sent/received by fax.

1.4.

THIS SECTION HAS BEEN REMOVED. PLEASE REFER TO SHA-07-004.

1.5. Security of Information in Transit

If SHR employees and/or contractors providing services to SHR are required to transport any kind of information, there are controls that must be used in order to avoid the loss of IT Assets or electronic media in transit, which could in turn lead to information misuse, unauthorized access or corruption.

1.5.1 The transport method (Canada Post, Courier, etc.) must be appropriate for the classification of the IT Asset or media.
1.5.2 Obtain an approved list of couriers, if applicable.
1.5.3 Courier is required to show identification prior to transferring custody of the IT Assets or media and a receipt acknowledging the transfer of same.
1.5.4 Packing used in transit must protect the package from damage and elements (e.g. enclosed container, binder). If the package contains internal or confidential information, it shall also be protected from unauthorized access (e.g. sealed envelope) if not in the presence of an SHR employee at all times.

1.6. Copying

Staff will not copy internal or confidential information unless they are authorized by management to do so.

2. PROCEDURE MANAGEMENT

The management of this policy including policy education, monitoring, implementation is the responsibility of the Privacy and Access Department. Amendment is the responsibility of the Director, Enterprise Risk Management.

3. NON-COMPLIANCE/BREACH

Non-compliance with this procedure may result in disciplinary action up to and including termination of employment and/or privileges.

A privacy breach may be reported to the Information Privacy Commissioner (IPC). The IPC and the Ministry of Justice may charge an individual with an offence under HIPA. Any person who knowingly contravenes HIPA may be subject to a fine of not more than $50,000 and/or not more than one year of imprisonment[3].

4. REFERENCES

Other relevant policies include:
SHR Policy *Email Acceptable Use*
SHR Policy *Internet Acceptable Use Policy*
SHR Policy *Emailing of Personal Health Information*
SHR Policy Facsimile (FAX)
SHR Policy Disposal of IT Assets

[3] HIPA Section 64(1)

Appendix A

INFORMATION SECURITY CLASSIFICATION AND STANDARDS CHART
Saskatoon Health Region

Inquiries regarding information classification should be directed to the SHR Privacy and Access Department.

Classification – Public/ Unrestricted *(No identifiable information)*

Potential Harm (examples)	▪ No possibility of harm. ▪ Liability damage of $0.
Information Type (examples)	▪ Non-sensitive information available to the general public (http://www.saskatoonhealthregion.ca/). ▪ General Programs and Services. ▪ Clinic hours of operations, hospital services, etc. ▪ Anonymous data such as those reported in the Chief Medical Health Officer's Health Status Report (e.g. number of influenza cases in the City; rates of diabetes, number of surgeries in rural areas or use of services, etc.)
Access Privileges	▪ Everyone
Storage	**All locations:** 1. Any area. 2. On a publicly-accessible SHR server. 3. In publicly accessible areas (e.g. internet, posters). 4. In designated secure off-site records storage areas.
Transport/ Transmission	No restrictions.
Reproduction	No restrictions.
Disposal	Recycling (preferred) or disposal.

Classification - Internal/Protected (*Sensitive and personal information)*

Potential Harm (examples)	▪ Threat or potential breach of individual privacy, or release of identifiable individual information without permission. ▪ Erosion of Region credibility and reputation. ▪ Inappropriate release or communication of sensitive Region information. ▪ Limited economic harm to the Region or third parties. ▪ Liability of approximately $10,000. ▪ Risk to region emergency preparedness and recovery. ▪ Erosion of Region credibility as service provider.
Information Type (examples)	▪ General internal assessments or documents not meant for general disclosure. ▪ Employment records such as salary and benefit information, unless public disclosure is mandatory. ▪ Third-party business confidences. ▪ Unapproved or incomplete policies or proposals. ▪ Administrative data, quality assurance and evaluation, committee minutes or documents.
Access	▪ Granted on a need-to-know basis to deliver services or carry out job functions; or ▪ As authorized by a Director (or positional equivalent) or as delegated. (Access is normally restricted to health stakeholders and approved non-health stakeholders for business purposes only.)

Storage	**Region Locations:** 1. In locked areas under surveillance during business hours, restricted to authorized personnel. 2. In unlocked Regional administrative/clinical areas with non-public access under constant direct surveillance. 3. On a secure Region network, application, or database server. Site Storage should be adequate to prevent casual disclosure. **Off-site Locations** Off-site storage requires the approval of the Director (or positional equivalent) or as delegated, and is based on program needs. 1. In locked areas or vehicles during daytime transport. 2. Under surveillance of staff member in homes. 3. On directories accessible only to staff member. 4. In designated secure off-site records storage areas. 5. In Information Systems reviewed and approved by Director Privacy and Access and/or Manager of IT Security.
Transport/ Transmission	▪ Standard mail, courier or transport. ▪ Faxing (see SHR Policy Facsimile (Fax) ▪ or internet transmission (see SHR Policy: Email Acceptable Use .
Reproduction	No restrictions but Region copies destroyed immediately after use.
Disposal	▪ Confidential shredding ▪ In accordance with ITS Security Standards and <Information Technology Services - Standard Operating Procedure - Asset Disposal>

Classification - Confidential *(Personal health information and/or Employee Performance Information)*

Potential Harm (examples)	▪ Threat or potential breach of individual privacy, or release of personal or personal health identifiable individual information without permission. ▪ Economic harm to the Region or third parties. ▪ Liability of approximately $100,000 or higher. ▪ Risk to region emergency preparedness and recovery. ▪ Complete erosion of Region credibility as service provider. ▪ Will undermine confidence in the security of the Region's information systems. ▪ Possible threat to health, safety or reputation of patients, staff, or other individuals. ▪ Interference with civil or criminal justice administration. Immediate threat to health and safety of patients, staff, or other individuals. ▪ Threat to security systems protecting medical facilities and equipment.
Information Type (examples)	▪ Personal patient registration, diagnostic, and treatment Information, including identifiable photographs. ▪ Personal and health related information that is identifiable and intended for use only by specified groups of health stakeholders involved in that patient's care. ▪ Employee performance and human resource information.
Access	▪ Access by external parties must be subject to a Memorandum of Understanding and/or a business or clinical "need to know", unless authorized by Management. ▪ Access for users after a successful security screening and authorization

	from a Director (or positional equivalent) or as delegated. ▪ Audit logs and reports on information access must be generated and reviewed at regular intervals.
Storage	**Region Locations:** 1. In locked areas under surveillance during business hours, restricted to authorized personnel; 2. In clinical areas with public access under constant direct surveillance or in a locked area; and 3. On a secure Region network, application, or database server. **Off-site Locations** Off-site storage requires the approval of a Director (or positional equivalent) or as delegated, and is based on program needs. 1. On directories accessible only to individuals with proper privileges; 2. In designated secure off-site records storage areas, and in Information Systems approved by the Privacy and Access Department.
Transport/ Transmission	▪ Mail, courier, or transport in properly labelled secure packaging or lockable chart transport bags, using reputable companies that employ secure conditions. ▪ Faxing and Internet transmission shall be done in accordance with the following SHR Policies: Emailing Personal Health Information , Email Acceptable Use , Internet Acceptable Use and Facsimile (FAX) Policy.
Reproduction	▪ Copy only when necessary and when access to original is highly impractical or for vital records backup.
Disposal	▪ Confidential shredding ▪ In accordance with ITS Security Standards and <Information Technology Services - Standard Operating Procedure - Asset Disposal>