St. Joseph's Healthcare Hamilton	Manual Corporate	Section ADM	Type Policy & Procedure	Pages 7	Number 184-ADM
Subject: Electronic Service Provider			Date: 20/01/2023		
Supersedes: NEW	Cross Reference: 178-ADM		Issuing Authority: Hospital Operations Committee		
☒ Charlton Campus ☒ King Campus			☒ West 5th Campus ☐ All Sites of Program		
This policy applies to all employees, members of the professional staff, volunteers, learners, contractors and all persons who have a relationship with SJHH					

Table of Contents

1.0 Purpose and Goals

To establish standards and practices to ensure compliance with s. 10(4) of the Personal Health Information Protection Act (PHIPA) and s. 6 of Regulation 329/04 made under PHIPA, where St. Joseph's Healthcare Hamilton (SJHH) acts as an electronic service provider (ESP), by providing services for the purposes of enabling a health information custodian (HIC) to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information (PHI) when St. Joseph's Healthcare Hamilton is not acting as an agent of that health information custodian.

The Personal Health Information Protection Act (PHIPA) details the rules for the collection, use and disclosure of personal health information by health information custodians (HIC). PHIPA applies to personal health information in the custody or control of both health information custodians and agents of health information custodians.

2.0 Definitions

Personal Health Information (PHI): Identifying information about an individual in oral or recorded format that relates to their physical or mental health, including information about the individual's family health history. Information may relate to the provision of health care, including the identification of the individual's health care provider and may include the identification of a substitute decision-maker. Personal Health Information may also include the individual's eligibility for health care, including their health card or identification number, payment information for receiving care, and eligibility/status for organ and other types of body parts and substance donation.

Health Information Custodians (HIC): A person or organization that as a result of their power, duties or work has custody or control of personal health information. Health Information Custodians include, but not limited to, health care practitioners, community care access corporations, hospitals, psychiatric facilities, long-term care homes, pharmacies, laboratories, ambulance services, retirement homes and homes for special care, medical officers of health, boards of health, the Ministry of Health, the Ministry of Long-Term Care, and Canadian Blood Services.

Agents of a Health Information Custodian: Any person who is authorized by a custodian to perform services or activities in respect to personal health information on the custodian's behalf and for the purposes of that custodian. An agent may include a person or company that contracts with, is employed by or volunteers for a custodian and has access to personal health information.

Health Information Network Provider (HINP): A person or organization that provides services to two or more Health Information Custodians (HIC) where the services are provided primarily to custodians to enable the custodians to use

electronic means to disclose personal health information (PHI) to one another, whether or not the person is an agent of any of the custodians.

Electronic Service Provider (ESP): A person or organization who provides goods or services for the purpose of enabling a Health Information Custodian (HIC) to use electronic means to collect, use, modify, disclose, retain or dispose of personal health information (PHI).

3.0 Equipment/Supplies

None.

4.0 Policy

When St. Joseph's Healthcare Hamilton provides information technology and project management services, such as but not limited to, software integrations, health informatics, data analytics and data science; software and patient portal implementations, to other health care systems, partners, agencies, and organizations, St. Joseph's Healthcare Hamilton may undertake the role of an Electronic Service Provider (ESP). When St. Joseph's Healthcare Hamilton is acting as an ESP it must comply with certain requirements of PHIPA and may also be required to comply with additional privacy obligations set out in any agreement(s) between St. Joseph's Healthcare Hamilton and health care system(s), partner(s), agency(ies) or organizations as the HIC(s) for whom it provides electronic service provider services.

St. Joseph's Healthcare Hamilton shall inform those working on its behalf of any unique obligations that they must meet for St. Joseph's Healthcare Hamilton to meet its legislative or contractual privacy commitments.

St. Joseph's Healthcare Hamilton shall only handle PHI within its capacity as an ESP to provide the services identified in its contract with the health care system(s), partner(s), agency(ies) or organizations as the HIC(s) for whom it provides electronic service provider services.

St. Joseph's Healthcare Hamilton shall protect PHI handled within its capacity as an ESP by employing procedures to meet the privacy and security requirements of Regulation 329/04, s. 6 (1) made under PHIPA, and any contractual provisions made directly between St. Joseph's Healthcare Hamilton and the other parties to whom it provides electronic service provider services.

St. Joseph's Healthcare Hamilton will notify and work with as required the HIC that is the custodian of the PHI of any privacy-related issues, requests, or breaches related to the PHI handled in its capacity as an ESP.

Where St. Joseph's Healthcare Hamilton is acting as an ESP and is a HINP, St. Joseph's Healthcare Hamilton Policy 178-ADM**,** Privacy Policy applies.

Where there is a discrepancy between this policy and PHIPA, PHIPA takes precedence.

5.0 Procedure

Procedures related to privacy-related issues and requests unrelated to a breach

It is the responsibility of all SJHH staff members, whom acting within their role to deliver information technology and project management services to external partners, to report any issues or requests they receive to the SJHH Department of Risk, Legal and Privacy.

SJHH Department of Risk, Legal and Privacy will in turn report the issue or request to the relevant HIC.

Procedures related to breaches

It is the responsibility of all SJHH staff members, whom acting within their role to deliver information technology and project management services to external partners, to report known or suspected privacy breaches as soon as reasonably possible, and to cooperate with the SJHH Department of Risk, Legal and Privacy. Where advised and/or requested by the SJHH Department of Risk, Legal and Privacy, SJHH staff will cooperate and collaborate with external health system(s), partner(s), agency(ies) and organization(s) privacy offices to ensure that privacy breaches are properly contained, investigated and further privacy breaches are prevented.

The privacy breach incident protocol contains five (5) steps, and follows pre-existing SJHH internal practices. The six steps are listed below:

1. Reporting of the Breach
2. Containment of the Breach
3. Investigation and Risk Assessment
4. a. Notification of the Breach

   b. Notification of Affected Organizations
5. Remediation

Step 1 of the incident protocol is the responsibility of the individual or individuals who

are first to become aware of the breach or potential of a breach. Steps 2 through 5 are the responsibility of St. Joseph's Healthcare Hamilton's Department of Risk, Legal and Privacy, in cooperation with the manager and staff of the affected department, area or team; the reporting staff, other internal SJHH stakeholders including Public Affairs, and depending on the level of severity, external SJHH legal counsel.

Step 1 Reporting of the Breach

A SJHH staff member acting within their role to deliver information technology or project management services to an external party, whom becomes aware of a known or suspected breach of privacy involving PHI in the custody or control of SJHH, partner health system, agency or other organization will immediately inform the Privacy Office in the Department of Risk, Legal and Privacy, along with their immediate supervisor. The Privacy Office may be contacted at privacy@stjoes.ca.

If the known or suspected breach of privacy occurs after-hours and/or is of a serious nature (i.e. stolen hardware), that requires immediate containment or other action, the staff member shall contact the acting Site Supervisor and the Service Desk (internal extension 33040) in addition to the notifying their immediate supervisor, and the Privacy Office in the Department of Risk, Legal and Privacy.

Step 2 Containment of the Breach

The SJHH Privacy Office will take immediate steps to limit the scope and impact of the breach. An initial assessment of the risks associated with the breach may be required to consider what immediate containment steps are required. Containment measures may include collaborating with the external party to take action to recover the PHI from the individual or organization, suspending access of the individual or organization, preventing access to PHI through device security, and/or reporting the incident to the police where the breach involves or may involve criminal activity.

If the known or suspected breach of privacy occurs after-hours and is of a serious nature, the acting Site Supervisor will assess whether the breach requires immediate action and will first escalate to the Hospital Administrator On-Call and Public Affairs On-Call staff members, and then if required, the Executive On-Call staff member.

Step 3 Investigation and Risk Assessment

An internal investigation by the SJHH Privacy Office to review the circumstances surrounding the breach will determine if further containment measures are required and assess the scope of the breach with respect to the PHI and individuals, and services affected. The investigation will identify the affected health system(s), partner(s), agency(ies) and organization(s) requiring notification of the breach and will also inform remediation actions.

Step 4a. Notification of the Breach

The Department of Risk, Legal and Privacy, together with Public Affairs shall determine notification steps arising from a breach. In cases of a serious nature, SJHH external legal counsel may be consulted to support the notification process due to legal and contractual obligations that have been mutually agreed upon by SJHH and the external party(ies).

Step 4b. Notification of Affected Organizations

Any affected health system(s), partner(s), agency(ies) and organization(s) whose PHI has been affected will be notified at the first reasonable opportunity at the discretion of the Privacy Office with consideration to the type of notification based on circumstance and contractual agreement obligations that have been mutually agreed upon by SJHH and the external party(ies).

Step 4c. Regulatory

In addition to the notification of affected organizations, SJHH will also cooperate in any Information and Privacy Commissioner of Ontario (IPC) investigation related to the breach.

Step 5 Remediation

a. System

Unless otherwise specified within contractual agreements between SJHH, health system(s), partner(s), agency(ies) and organization(s), SJHH internal processes, procedures and controls will be reviewed to determine whether there are any gaps or systematic opportunities for improvement arising from the privacy breach.

b. Staff

The actions of individual staff members involved in the privacy breach will be reviewed together with the staff member's supervisor or manager, and SJHH's Human Resource Department. Responses to staff privacy infractions shall be based on internal SJHH privacy sanction guidelines.

6.0 Documentation

Additional References:

Information and Privacy Commissioner of Ontario (www.ipc.on.ca)

The Kingston, Frontenac, Lennox & Addington Public Health Unit (www.kflaph.ca)

Health Sciences North (www.hsnsudbury.ca)

St. Joseph's Healthcare Hamilton (http://mystjoes/policies/Policies/178-ADM.pdf)

7.0 Author(s)

Senior Project Manager, Digital Solutions

Director, Digital Solutions

Chief Privacy Officer

8.0 Sponsor

Vice President & Chief Information Officer

9.0 In Consultation With

Executive Leadership Team

10.0 Posting Dates

Initial Posting Date: 25-01-2023

Posting Date History:

11.0 Scheduled Review Date

January 2026