SURREY PLACE

STATEMENT OF POLICY AND PROCEDURE

Department:	Operational Excellence	**Policy Number:**	PRI-001
Approved by:	Executive Team	**Accountability:**	VP, Quality & Strategy
Operational Lead:	Director, Operational Excellence	**Policy Origin Date:**	November 2004
Revision Date:	July 12, 2023	**Review Date:**	July 2024

POLICY TITLE:

Privacy Policy

1 POLICY

1.01 As a health information custodian, Surrey Place (SP), its agents (including employees, physicians, contractors, consultants, volunteers, students and other workers at SP, including all personnel affiliated with third parties) are responsible for ensuring that the personal health information of our clients are treated with respect and sensitivity.

1.02 SP maintains privacy in compliance with the Personal Health Information Protection Act (PHIPA), 2004 and takes into account the Personal Information Protection and Electronic Documents Act (PIPEDA), 2015.

1.03 SP will follow the standards set by PHIPA, Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008 (SIPDA) and Ontario Regulation 299/10 Quality Assurance Measures (QAM) in:

a) The collection use and disclosure of personal health information (PHI).
b) Providing individuals with a right of access to PHI about themselves, subject to limited and specified exceptions set out in PHIPA.
c) Providing individuals with a right to require the correction or amendment of PHI about themselves, subject to limited and specific exceptions set out in PHIPA.
d) Providing for an independent review and resolution of complaints with respect to PHI.
e) Providing effective remedies for contraventions of PHIPA.

1.04 This policy will be reviewed annually, or as prompted by change in relevant legislation.

2 PURPOSE

2.01 The purpose of this Statement of Policy and Procedure is to establish internal controls over the privacy of personal and personal health information for clients.

3 SCOPE

3.01 This policy applies to all individuals with access to personal information and personal health information of SP clients and includes procedures for:

a) Consent for the collection, use and disclosure of personal health information (PHI)
b) Limiting the collection, use and disclosure of PHI
c) Retention, archiving and destruction of PHI
d) Client rights
e) Ensuring accuracy and safeguarding of PHI
f) Privacy breaches and privacy complaints
g) Employee training and awareness
h) Exceptions
i) Enforcement
j) Reporting

4 LEGAL AUTHORITY

4.01 SP maintains privacy in compliance with the Personal Health Information Protection Act (PHIPA), 2004 and takes into account the Personal Information Protection and Electronic Documents Act (PIPEDA), 2015.

5 RESPONSIBILITY

5.01 The CEO retains ultimate responsibility for privacy at SP but delegates day-to-day operational responsibility to various personnel noted below.

5.02 The Vice President, Quality & Strategy acts as SP's Chief Privacy Officer (CPO) with responsibility for:

a) Establishing and maintaining standards of privacy, confidentiality and data security to protect personal health information of SP clients
b) Creating a culture of continuous improvement for supporting organizational procedures and practices
c) Annual organizational reporting, analysis and training

5.03 The Director Operational Excellence acts as SP Privacy Officer with responsibility for:

a) Directing, guiding and coordinating day-to-day privacy matters
b) Escalating all privacy concerns to the CEO, CPO and appropriate Senior Management members in a timely manner.

5.04 Executive Team and Management staff are responsible for:

a) Reviewing, comprehending and adhering to this policy
b) Developing and implementing appropriate supporting procedures/ practices within their department

c) Ensuring all staff, consultants, contractors, students, volunteers and vendors have access to and are knowledgeable of privacy policies and procedures
d) Immediately documenting any privacy concerns and reporting them to the Privacy Officer
e) Proactively documenting and consulting with the Privacy Officer and Director of Information Technology before engaging in any new or modified activities that could affect the privacy of personal or personal health information.

5.05 SP staff, consultants, contractors, students, volunteers and vendors are responsible for:

a) Reviewing, comprehending and adhering to this policy
b) Immediately raising any privacy concerns to the appropriate senior manager.
c) Who is responsible

6 DEFINITIONS

6.01 ***Agent*** – a person that, with the authorization of SP, acts for or on behalf of the organization in respect of personal health information for the purposes of SP and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by SP and whether or not the agent is being remunerated. Examples of agents of SP include, but are not limited to, employees, volunteers, students, physicians, residents, contractors, consultants, researchers, vendors.

6.02 ***Confidential information*** – confidential information maintained at SP can fall under three categories: Personal information, personal health information and corporate confidential information.

6.03 ***Corporate confidential information*** – information maintained by SP that is not routinely made publicly available, including financial, administrative, commercial and technical information, and can also include records containing legal advice and employee-related information.

6.04 ***Health information custodian*** – listed persons or organizations under PHIPA, such as hospitals, who have custody or control of personal health information as a result of the work they do. As an outpatient hospital, SP is considered to be a health information custodian.

6.05 ***Lockbox*** – A request by a client or their caregiver that the client's PHI be restricted. A full lock means that all PHI, including future documentation, is restricted from use by one or more SP staff and/or from disclosure to external healthcare providers. A partial

lock means that any or all client existing PHI is restricted from use by one or more SP staff and/or disclosure to external healthcare providers.

6.06 ***Personal health information (PHI)*** – Any identifying information about an individual relating to the individual's health or to the provision of health care to the individual. For example, an individual's health number and/or health record would be considered PHI.

6.07 ***Personal information (PI)*** – Identifying information about an individual that does not contain health care information. Examples include age, religion, address and telephone number.

6.08 ***Personal Health Information Protection Act (PHIPA), 2004*** – Establishes rules for the collection, use and disclosure of personal health information about individuals that protect the confidentiality of that information and the privacy of individuals with respect to that information, while facilitating the effective provision of health care.

6.09 ***Personal Information Protection and Electronic Documents Act (PIPEDA), 2015*** – Sets ground rules for how organizations may collect, use or disclose personal information in the course of their activities.

6.10 ***Privacy Breach*** – The disclosure of client's PHI to an individual(s) or organization without the client's expressed consent.

6.11 ***Research Ethics Board (REB)*** – A select group of professionals who ensure that all research carried out at Surrey Place meets the highest ethical standards in all phases of the research.

6.12 ***Risk-Based Model in Privacy*** – A focused approach on utilizing limited resources to proactively scrutinize and develop policies and procedures for the most significant privacy risks at Surrey Place.

7 REFERENCES and RELATED STATEMENTS of POLICY and PROCEDURE

7.01 Personal Health Information Protection Act, 2004
7.02 Personal Information and Protection of Electronic Documents Act, 2015
7.03 Services and Supports to Promote the Social Inclusion of Persons with Developmental Disabilities Act, 2008 (SIPDA)
7.04 Ontario Regulation 299/10 Quality Assurance Measures (QAM)
7.05 Research Ethics Board Terms of Reference Policy
7.06 Security of Health Information policy

7.07 Client Request for Correction to Health Records Policy
7.08 Information Security and Appropriate Use of Technology Policy
7.09 Logging and Auditing Policy
7.10 Privacy Breach Policy
7.11 Confidentiality Policy
7.12 Code of Conduct Policy
7.13 Serious Occurrence Reporting
7.14 Reporting a Privacy Breach to the Commissioner, Information and Privacy Commissioner of Ontario (2017)

8 PROCEDURES

Consent for the Collection, Use and Disclosure of Personal Health Information (PHI)

8.01 The knowledge and consent of the individual are required for the collection, use or disclosure of PHI, except where appropriate. Permitted purposes for the collection of PHI include: delivery of direct client care; administration of the health care system; research, teaching statistics, fund development and meeting legal and regulatory requirements.

8.02 To make consent meaningful, the purpose will be communicated in a manner that the individual can reasonably understand how the information will be used or disclosed.

8.03 SP will not, as a condition of providing service/ care, require an individual to consent to the collection, use or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes. SP can assume that an individual's request for treatment constitutes consent for specific purposes.

8.04 When collecting PHI:

a) At or before the time of collection, the intended purpose should be documented to limit collection to what is required
b) Depending on the way in which the information is collected, this can be done verbally or in writing
c) Notices identifying the purposes for the collection of PHI should be readily available to clients
d) When PHI collected is to be used for a purpose not previously identified, the new purpose should be identified prior to use. Unless law requires the new purpose, the consent of the individual is required before information can be used for that purpose.
e) Persons collecting PHI will be able to explain to individuals the purpose for which information is being collected

8.05 In certain circumstances, PHI can be collected, used or disclosed without the knowledge and consent of the individual. For example, legal, medical or security reasons may make it impossible or inappropriate, for example when the individual is seriously ill or mentally incapacitated. In these circumstances, consent of the individual's substitute decision maker will be sought, where feasible.

8.06 SP may use or disclose PHI for research purposes without an individual's consent if strict conditions are met (e.g. the approval of the Research Ethics Board). For example, a custodian who uses PHI for research and similarly a researcher who seeks disclosure of PHI for research, must both submit a detailed research plan to the SP Research Ethics Board (REB) for approval. In reviewing a research proposal involving the use and disclosure of PHI, the REB must consider:

a) Whether the research cannot be reasonably accomplished without access to the information
b) The public interest in conducting the research and in protecting privacy
c) Whether obtaining consent directly is impracticable
d) Whether adequate safeguards are in place to protect the privacy of individuals and the confidentiality of their information.

Limiting the Collection, Use and Disclosure of Personal Health Information (PHI)

8.07 The collection of PHI will be limited to that which is necessary for the purposes identified by SP; information will be collected by fair and lawful means.

8.08 At or before the time PHI is collected, SP will identify the purposes for which the PHI is collected. Permitted purposes include: the delivery of direct client care; the administration of the health care system; research; teaching; statistics; fund development; and meeting legal and regulatory requirements.

8.09 SP may use information from non-SP organizations if SP has been granted contractual authority to use it for the direct care of a client.

Retention, Archiving and Destruction of Personal Health Information (PHI)

8.10 SP has established information retention guidelines that define consistent minimum standards and requirements for the length of time PHI and records of PHI are to be maintained in accordance with the Security of Health Information policy.

8.11 SP has established appropriate practices for the timely and secure disposal of PHI consistent with confidentiality, legal and regulatory requirements. (See Security of Health Information policy)

8.12 Researchers are responsible for the storage/ retention of research data, at a minimum for the length of their appointment at SP or as required by regulatory bodies, whichever is greater.

8.13 A research project or activity should be regarded as having ended after: (a) final reporting to the research sponsor; (b) final financial closeout of a sponsored research award; or (c) final publication of research results, whichever is later. (See Security of Health Information policy)

Client Rights

8.14 Upon request, an individual will be informed of the existence, use and disclosure of his or her PHI, and will be given access to that information as per SP's Client Access to the Health Record policy.

8.15 SP will make specific information about its policies and practices relating to the management of PHI readily available to individuals.

8.16 An individual will be able to address a challenge concerning compliance with this policy. SP will inform individuals who make inquiries or lodge complaints of the existence of relevant complaint procedures.

8.17 SP will investigate all complaints. If a complaint is found to be justified, SP will take appropriate measures, including amending its policies and practices where necessary.

Ensuring Accuracy and Safeguarding of Personal Health Information (PHI)

8.18 SP will take reasonable steps to ensure that information is as accurate, complete and relevant as necessary to minimize the possibility that inappropriate information may be used to make a decision about an individual. (See Security of Health Information policy)

8.19 An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate. (Refer to Client Request for Correction to Health Records policy). If a challenge is not resolved to the satisfaction of the individual, SP will record the substance of the unresolved challenge in the form of a letter from the client, to be stored in the client's health record. When appropriate, the existence of the unresolved challenge will be transmitted to third parties having access to the information in question.

8.20 SP will protect the safety and respect the confidentiality of PHI through appropriate safeguards as per Information Security & Appropriate Use of Technology policy.

8.21 SP will inform clients of the loss, theft or inappropriate access of their PHI as soon as reasonably possible. (See Security of Health Information policy)

8.22 The Privacy Officer (PO) along with appropriate staff will review, respond to and administer and lockbox requests as follows:

a) Creating awareness of the right and potential implications for healthcare service delivery of requests for a lockbox on PHI
b) Reviewing and responding to all written requests for lockbox in a timely and appropriate manner
c) Ensuring legislative and permitted disclosures of PHI are followed for lockbox cases that may include but not be limited to express consent from the client or substitute decision maker for disclosure and eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

Privacy Breaches and Privacy Complaints

8.23 SP is committed to maintaining an open and transparent environment in which privacy complaints and/or breaches are handled in a respectful and transparent manner.

8.24 A privacy complaint or breach must in no way impact the quality or quantity of services received by a client, family member or caregiver.

8.25 Any agent of SP who becomes aware of a potential privacy breach and/or privacy complaint is required to immediately inform the Privacy Officer (PO) verbally, immediately followed with a written incident report. (See Privacy Breach Policy)

8.26 If the privacy breach relates to a shared system (e.g. ConnectingOntario), the Privacy Officer must notify the program office responsible for the shared system by the end of the next business day after identifying the privacy breach. Surrey Place will follow instructions from the respective program office on managing the privacy breach, understanding that remediation or disciplinary activities must be approved by the applicable oversight body at the program office responsible for the shared system.

8.27 Privacy complaints may be submitted verbally or in writing to the Privacy Officer (PO) at:

Privacy Officer (PO)
Director, Operational Excellence
Tiffany Gurprasad
Surrey Place

2 Surrey Place, Toronto, ON M5B 2C2
tiffany.gurprasad@surreyplace.ca

8.28 Complaints must be submitted in sufficient detail for a thorough investigation and appropriate resolution with the affected parties.

8.29 The Privacy Officer (PO) will lead and manage all aspects of a privacy breach and/or complaint, including but not limited to:

a) Working with appropriate staff member(s) to complete the incident report
b) Escalating awareness of the incident to the Chief Privacy Officer (CPO), CEO and other Senior Management as needed
c) Investigating all concerns and ensuring appropriate resolution that may include verbal and/or written apologies, policy and/or process improvements and disciplinary action with the appropriate supervisory and human resources staff

8.30 Should a complainant not be satisfied with the results of the investigation conducted by the Privacy Officer (PO) or the Privacy Officer (PO) face a conflict of interest in conducting an investigation:

a) The complainant or the Privacy Officer (PO) may request that the complaint be investigated by the Chief Privacy Officer (CPO) or the CEO
b) The CPO or CEO will review all materials regarding the complaint to determine whether further action is required, provide a written response to all parties concerned and supervise all necessary matters for complete resolution

External Reporting

8.31 As of October 1, 2017, custodians must notify the Information and Privacy Commissioner of Ontario about certain privacy breaches: use or disclosure without authority, stolen information, further use or disclosure without authority after a breach, pattern of similar breaches, disciplinary action against a college member, disciplinary action against a non-college member, and any other significant breaches. Custodians are required to provide the Information and Privacy Commissioner with an annual report of the previous calendar year's statistics.

8.32 Surrey Place will submit a Serious Occurrence Report for any breach or potential breach of privacy and/or confidentiality, including any instance/suspected instance when personal information of an individual who is receiving a service has been collected, used, stolen, lost or disclosed without authority that results in serious harm or risk of serious harm to the individual and/or others, or is in contravention of the YCJA. See Updated Serious Occurrence Reporting Guidelines and Surrey Place's Serious Occurrence Reporting Policy for details on how to submit a Serious Occurrence Report.

Logging and Auditing

8.33 Surrey Place will ensure that internal systems log/audit activities, where possible, to ensure compliance with PHIPA, the Privacy Policy and any relevant agreements. (See Logging and Auditing Policy)

Employee Training, and Awareness

8.34 SP will make its employees aware of the importance of maintaining the confidentiality of PHI. As a condition of employment, all new SP employees/ agents must sign the Confidentiality Policy. (See SP's Code of Conduct Policy). This safeguard may also be facilitated through contractual provisions. The policy will be reviewed annually thereafter.

8.35 Ongoing education efforts will be delivered to ensure employees, agents and third parties are provided with tools, training and support as appropriate to enable them to fulfill their duties as it relates to the privacy of PHI.

Exceptions

8.36 Any exceptions to this policy must be requested in writing to the Privacy Officer and approved in advance by the Chief Privacy Officer, in consultation with the CEO. As assessment of the request may involve other groups and a response to the request will be made in writing.

Privacy Officer (PO)	Chief Privacy Officer (CPO)
Director, Operational Excellence	Vice President, Quality & Strategy
Tiffany Gurprasad	Felix Camposano
tiffany.gurprasad@surreyplace.ca	felix.camposano@surreyplace.ca

Enforcement

8.37 The Chief Privacy Officer (CPO) and Privacy Officer (PO) will monitor adherence to this policy using a risk-based model, and report to the CEO and Senior Management.

8.38 Breaches of this policy and related privacy procedures may be subject to disciplinary action, as outlined in the Confidentiality Policy.

8.39 SP and its agents may also be subject to the fines and penalties set out in PHIPA, up to $50,000 for individuals and $250,000 for the organization.

9 ATTACHMENTS

9.01 None noted.

10 REVISION HISTORY

Date Revised	Reviewer (Director or designate)	Comments
Mar/15/18	Coordinator, Special Projects	7.30 updated to include annual statistical reporting requirement
Aug/10/18	Coordinator, Special Projects	7.26, 7.32 updated to reflect EHR requirements
Mar/18/20 May/27/20	Director Quality & Performance	Minor Revisions
Jul/12/23	Director, Operational Excellence	Minor Revisions, Updated Contact Information