COMMUNITY CARE FOR CENTRAL HASTINGS

Privacy Policies

Revised: February 26, 2019

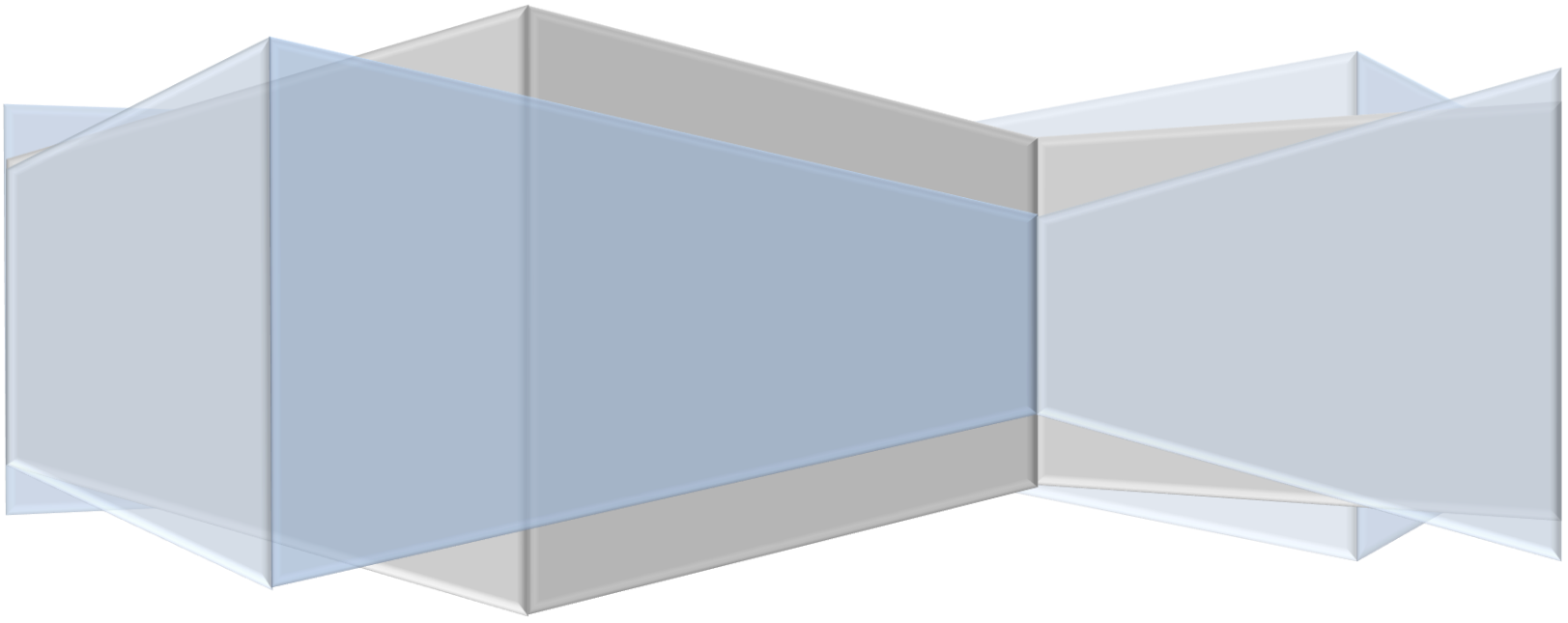

Table of Contents

1. Privacy Policy

Purpose This policy describes Community Care for Central Hasting's (CCCH) role as a custodian of personal health Information (PHI), and describes its obligations and requirements for the protection of client privacy and the appropriate management of PHI, as defined in applicable legislation and recognized best practices in privacy protection.

This policy supports CCCH's commitment to appropriately share PHI with regional health care providers to ensure that these providers have the information they require to provide timely and effective health care.

Applicability This policy applies to all CCCH employees, contractors, and third party service providers.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Chief Executive Officer approves this policy

Status of Community Care for Central Hastings (CCCH)

1.1. CCCH is a health information custodian under the Personal Health Information Protection Act, 2004, and is required to manage and protect the personal health information (PHI) in its custody according to the Act and its Regulations.

1.2. CCCH's privacy and information management practices will ensure that its employees appropriately collect, use and disclose personal health information to support the effective and efficient delivery of health care to clients.

Definitions

1.3. In this policy and all of its associated privacy policies, the term "employee is used to refer both to CCCH employees and contractors and volunteers."

1.4. Personal health information (or PHI) is defined in PHIPA as follows:

- Personal health information means identifying information about an individual in oral or recorded form, 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 a plan of service within the meaning of the Home Care and Community Services Act, 1994 for the individual,
  - relates to payments or eligibility for health care, or eligibility for coverage for health care, in respect of the individual,

---

- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance,
- is the individual's health number, or
- Identifies an individual's substitute decision-maker.

Privacy Standards

1.5. CCCH's practices for managing and protecting PHI will be informed by, and meet or exceed, the following standards and best practices:

- The Personal Health Information and Protection Act, 2004
- Canadian Standards Association Model Code for the Protection of Personal Information
- Orders, guidelines and best practices produced by the Office of the Information and Privacy Commissioner of Ontario.

1.6. CCCH will promote a culture of privacy, which will include privacy training and awareness activities for all CCCH's employees.

1.7. CCCH will follow privacy-by-design principles espoused by the Office of the Information and Privacy Commissioner of Ontario to develop privacy safeguards intended to reduce privacy risks and forestall the occurrence of privacy incidents.

1.8. CCCH will have a privacy governance and accountability framework in place, which will define roles and responsibilities for ensuring the appropriate collection, use and disclosure of PHI, and the protection of PHI in the custody of the CCCH.

CCCH privacy program

1.9. CCCH will meet its privacy accountabilities through an organization-wide privacy program.

1.10. CCCH's Privacy Officer will be responsible planning and management of the privacy program

1.11. The Privacy Officer will

- maintain privacy policies and procedures that define the practices supporting CCCH's compliance with PHIPA;
- ensure that privacy and security awareness training is delivered according to the requirements of the CCCH's Privacy and Security Training and Awareness Policy;
- develop and distribute communications materials that describe CCCH privacy program to the public;
- monitor the compliance of CCCH's employees with CCCH's privacy policies.

1.12. The Privacy Officer will assess CCCH's privacy and security safeguards when CCCH:

- implements new programs and initiatives;
- learns of changes to existing legislation, the introduction of new legislation or directives issued by the Office of the Information and Privacy Commissioner of Ontario.

Policy Authority

1.13. Where there is a discrepancy between this privacy policy and any applicable legislation or regulation, the legislation or regulation will take precedence.

1.14. Where there is a discrepancy between this policy and any other CCCH standard or process for the protection or management of PHI, this policy will take precedence.

1.15. Failure on the part of any CCCH employee to comply with this policy will result in disciplinary action up to and including dismissal and legal action.

Identification of Purposes

1.16. The purposes for collection use and disclosure of PHI will be limited to those purposes required to achieve the lawful objectives of the CCCH, or specified in legislation, Including:

- To provide or assist in the provision of health care to clients;

1.17. Where consent is required for collection, use or disclosure of PHI, CCCH will ensure that the purposes for collection, use and disclosure will be communicated to clients before these activities take place.

Consent

1.18. CCCH will obtain knowledgeable consent for the collection, use and disclosure of PHI from the clients to which it provides services.

1.19. CCCH will implement measures to inform clients of its purposes for collection, use and disclosure, including:

- Conspicuous public posting of notices indicating the CCCH's purpose for collection of PHI to support implied knowledgeable consent of the client;
- Client communications materials such as brochures and consent forms
- Face-to-face interactions between CCCH employees and clients

1.20. CCCH will rely on <implied or express> consent for collection, use and disclosure of PHI from its clients for the purposes of providing health care.

1.21. CCCH will obtain the express consent of clients

- for disclosures to people or CCCH that are not health information custodians under PHIPA;
- for disclosures to health information custodians that are not for the purpose of providing health care;
- for uses and disclosures the purpose for which was not communicated when consent was initially obtained by CCCH.

1.22. CCCH employees collect, use and disclose PHI with the consent of clients, except where collection, use and disclosure without consent is authorized under legislation.

1.23. CCCH employees will conduct assessments on the capacity of clients to provide knowledgeable consent, and will work with a client's family and caregivers to determine a substitute decision maker for the client where she or he is assessed to be incapable of providing knowledgeable consent.

1.24. CCCH employees will never obtain consent through deception or coercion.

1.25. CCCH employees will respect a client's right to request that her or his PHI be withheld from specific individuals and CCCH, and will take reasonable measures to ensure that PHI is withheld from the specified individuals and CCCH.

Limiting Collection

1.26. CCCH employees will limit the collection of PHI to only the information that is required to fulfill the purposes that were identified to clients before collection.

1.27. Employees will be trained to recognize when de-Identified or aggregate data will fulfill the purposes for the collection of PHI.

1.28. When requesting PHI from other health care providers, employees will make their requests specific so that they do not receive more PHI than is required to meet the request.

1.29. The Privacy Officer or a delegate will regularly review the scope and nature of data elements collected by CCCH to determine if collection of PHI by programs is appropriately limited.

Limiting Use and Disclosure

1.30. CCCH employees will limit their use and disclosure of PHI to only those activities and disclosures that fulfill the purposes that were identified to clients before collection.

1.31. The Privacy Officer will ensure that CCCH employees are trained to disclose no more PHI than is required to fulfil the purpose of the disclosure.

1.32. CCCH employees are required to use or disclose de-identified or aggregate data instead of PHI where such data will support the purposes for which the PHI was collected.

Limiting Retention

1.33. The Privacy Officer will ensure that CCCH retains PHI only for the time period required to fulfill the purposes for which the information was collected, or as authorized or required by legislation.

1.34. The Privacy Officer will ensure that retention and disposal schedules for PHI in the custody of CCCH are maintained.

1.35. PHI that is no longer required by CCCH for its identified purposes will be securely destroyed or rendered irretrievable to prevent unauthorized access to the information.

Openness

1.36. The Privacy Officer will ensure that CCCH makes available to the public information regarding its privacy policies, procedures and safeguards.

1.37. Its regional partners, to ensure consistency in communications with clients.

1.38. The Privacy Officer will ensure that a plain-language summary of CCCH's privacy policies and procedures is posted on its public-facing web site.

1.39. The Privacy Officer will make available to the public on request print versions of all privacy-related information which it has posted to its public website.

1.40. The Privacy Officer will ensure that her or his contact information is published and readily accessible on CCCH's public website and other client communication materials.

1.41. All communications regarding CCCH's privacy and security program will be reviewed annually by the Privacy Officer to ensure currency of the information.

Privacy Incident Management

1.42. The Privacy Officer will ensure that CCCH employees have received training in supporting the containment, resolution and investigation of privacy and security incidents within CCCH.

1.43. For every confirmed privacy incident, the Privacy Officer will manage the execution of procedures to:

- contain the incident;
- determine the nature and scope of the incident;
- work with any relevant stakeholders to resolve and investigate the incident;
- notify affected clients regarding the incident;
- evaluate the cause(s) of the incident and conduct remediation activities as required.

Safeguards

1.44. The Privacy Officer will ensure that appropriate information security safeguards have been deployed within CCCH to protect PHI from unauthorized collection, use or disclosure, including:

- administrative safeguards such as training and awareness activities.
- technical safeguards such as encryption of PHI.
- Physical safeguards such as locked cabinets for paper records.

Access and Correction

1.45. CCCH will provide client with access to his or her record of PHI where lawful and appropriate, by providing a report of the PHI it has collected about the client.

1.46. The Privacy Officer will review and respond to all access and correction requests, according to CCCH's *Access* and Corrections Policy and associated procedures.

Privacy Inquiries and Complaints

1.47. CCCH will accept inquiries and complaints regarding CCCH's privacy program and CCCH privacy practices from any individual or CCCH.

1.48. The Privacy Officer will review and respond to all privacy inquiries and complaints, according to CCCH's *Privacy Inquiries and Complaints Policy and associated procedures*.

2. Privacy and Security Governance and Accountability Policy

Purpose To ensure that CCCH has in place an appropriate privacy and security governance and accountability framework to support its compliance with its privacy obligations, and decision-making regarding the objectives and management of its privacy program.

Applicability This policy applies to all CCCH employees responsible for privacy governance within CCCH.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Board of Directors and Executive Director approve this policy.

Policy

2.1. CCCH will have a privacy and security governance structure that distributes accountability and responsibility for privacy and security to the appropriate Individuals and bodies.

2.2. The following individuals and bodies comprise the privacy and security governance structure at CCCH:

- Executive Director
- Senior Management Team
- Privacy Officer
- Privacy and Security Committee

Accountabilities

2.3. The Executive Director will have overall accountability for protecting privacy and security at CCCH, and will approve CCCH's privacy and security policies on the recommendation of the Board of Directors.

2.4. The Executive Director is accountable for ensuring that CCCH has implemented a privacy and security program to support the compliance of employees with CCCH’s privacy and security policies and procedures.

2.5. The Senior Management Team will receive regular reporting on the performance of the privacy program from the Privacy Officer, and provide guidance on the resolution of privacy issues.

2.6. The Privacy Officer will be responsible for ensuring that the CCCH complies with its privacy obligations as defined In PHIPA, other relevant legislation, and its own privacy policies.

2.7. The Privacy Officer will be responsible for establishing and managing CCCH's privacy program, through which CCCH's privacy policies are translated into day-to-day operations and procedures.

2.8. The Privacy Officer will delegate responsibility for ensuring that third party service providers are compliant with the privacy terms of their agreements to CCCH Coordinators responsible for contracting the service providers.

2.9. The Privacy and Security Committee will be responsible for regular review of CCCH's privacy and security policies and procedures, and for making recommendations for amendments to the policies, procedures, or the overall policy framework.

2.10. The Privacy and Security Committee will be responsible for oversight of privacy and security risk management within CCCH.

2.11. All CCCH employees and, where applicable, third party service providers will be responsible for compliance with CCCH's privacy and security policies and procedures.

Responsibilities Senior Management Team

2.12. The Senior Management Team will have a standing item on its agenda for privacy and security which includes the following items, where relevant:

- privacy complaints
- privacy and security incidents
- results of privacy assessments, audits, and threat and risk assessments
- recommendations for changes to CCCH privacy policies and procedures
- Any other privacy issues

Privacy Officer

2.13. The Privacy Officer will be appointed by the Executive Director and will be responsible for:

- preparing the Annual Report on Privacy and Security
- acting as the point of contact for, and managing, privacy inquiries and complaints, and access and correction requests made under PHIPA and FIPPA.
- acting as the point of contact for, and managing, the containment, resolution and investigation of privacy and security incidents
- coordinating and managing CCCH's privacy program
- directing privacy assessments and audits
- managing risk mitigation activities as defined in CCCH's privacy risk management plan
- preparing privacy agenda items for meetings of the Senior Management Team
- convening and chairing regular meetings with the Privacy and Security Committee
- ensuring that CCCH's Human Resources staff have delivered privacy and security training to all employees as needed
- provide privacy advice and guidance to all CCCH employees on an as-needed basis.

2.14. The Privacy Officer will report to the EXECUTIVE DIRECTOR.

2.15. The Privacy Officer will ensure that CCCH's privacy and security governance and accountability framework, including the privacy organizational chart, is posted on CCCH internet site (or otherwise made available to employees), and included in privacy and security training.

Privacy and Security Committee

2.16. The Privacy and Security Committee will meet on a quarterly basis to review and/or discuss:

- progress of risk mitigation activities documented in CCCH's privacy risk management plan
- any recommendations deriving from privacy impact assessments, privacy audits, and threat and risk assessments
- privacy or security incident management activities, and related recommendations
- proposals to update or amend the privacy and security policies and procedures

2.17. The Privacy and Security Committee will review and approve privacy audit plans developed by the Privacy Officer.

2.18. The Privacy and Security Committee will have representation from CCCH’s Program Managers.

Annual Report on Privacy and Security

2.19. The Annual Report on Privacy and Security will provide reporting on:

- training and awareness efforts
- third party service provider agreements (new agreements, changes to agreements)
- audits and compliance, including privacy impact assessments, privacy and security audits and any related recommendations, and the status of their implementation
- incident management, including privacy inquiries and complaints, privacy and security beaches (if any),related recommendations, and the status of their implementation
- recommendations for changes (if any},to privacy and security policies and procedures

2.20. The Annual Report will be reviewed by the Senior Management Team before being forwarded to the Executive Director for approval.

3. Privacy and Security Training and Awareness Policy

Purpose To ensure that employees have received sufficient training to ensure that CCCH is able to comply with its privacy obligations as defined in legislation, and with recognized standards and best practices in privacy management.

To ensure that CCCH employees are provided with initial orientation to CCCH's privacy program at the start of employment, and with on-going privacy awareness training.

Applicability This policy applies to all CCCH employees and third party service providers.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Chief Executive Officer approves this policy.

Privacy and security training

3.1. CCCH will provide all employees with privacy and security awareness training when starting employment.

3.2. Content for privacy and security training will be developed by the Privacy Officer or a delegate, in consultation with program managers, or will be reviewed and approved by the Privacy Officer before delivery if she or he has not developed the content.

3.3. CCCH employees will complete privacy and security refresher training every X years, or upon significant legislative or policy changes.

3.4. The Privacy Officer will determine privacy training requirements for third party service provider employees based on a review of a service provider's existing privacy training.

3.5. No CCCH employee or contractor, or employee of a third party service provider, will receive access to PHI until s/he has completed required privacy and security training.

Privacy training topics

3.6. Privacy and security awareness training will be developed to support compliance of employees with CCCH's privacy and security policies and procedures, and with the CCCH Code of Conduct.

3.7. To support employee compliance with CCCH's privacy obligations, the Privacy Officer will ensure that privacy training addresses:

- appropriate use and disclosure of PHI to support the delivery of health care, and the conditions under which PHI may be disclosed with regional health care partners;
- practices for appropriately accessing PHI and for limiting the use and disclosure of PHI;
- information management practices that support the security of PHI;
- guidelines on the identification, reporting and containment of privacy incidents and breaches

Role-based privacy and security training

3.8. CCCH will provide role-based privacy and security training to support employees in meeting CCCH's privacy obligations.

3.9. The Privacy Officer will consult with program managers on an ongoing basis to determine role-based training needs.

3.10. The Privacy Officer will review all role-based privacy and security training before it is delivered to its intended audiences.

3.11. The Privacy Officer will ensure that role-based training Is delivered within twenty business days of the date that an employee or contractor assumes her or his duties at the CCCH that require the role-based training.

Third party service providers

3.12. The Privacy Officer will ensure that third party service providers are contractually obligated to provide their employees with privacy and security training that addresses the service provider's privacy and security obligations to CCCH.

Privacy and security awareness and culture

3.13. The Privacy Officer will ensure that managers promote and foster a culture of privacy and security awareness with employees.

Review of training materials

3.14. All privacy and security training and awareness materials and content will be reviewed by the Privacy and Security Committee:

- annually
- upon a significant change to a CCCH program or information system, or the introduction of a new program or information system.
- Upon a change in application legislation that will have a significant impact on CCCH business or clinical processes.

3.15. Any proposed changes to CCCH privacy and security training will be approved by the Executive Director on the recommendation of the Privacy Officer. The changes to the training will be made by the Privacy Officer.

Documenting and tracking delivery of privacy and security training

3.16. The Privacy Officer will log the completion of all privacy and security training, and will use the training log to determine refresher training requirements, and compliance with this policy.

4. Privacy Incident Management Policy

Purpose To ensure that CCCH employees understand their responsibilities for monitoring for and identifying privacy incidents, and for managing the resolution of such incidents.

Applicability This policy applies to all CCCH employees.

Responsibility The Privacy Officer develops, maintains and reviews this policy.

The Chief Executive Officer approves this policy.

Policy Definitions

4.1. A privacy incident is an event occurring within a CCCH program or system that places the privacy of personal health information at risk, and that is attributable to the actions of one or more individuals, to electronic system failures, or to malicious software (e.g., virus, worm).

4.2. A privacy breach is an incident that involves the unauthorized collection, use, disclosure, modification or destruction of PHI.

4.3. Privacy incidents or breaches will include, but not be limited to, the following:

- a contravention, through the actions of a CCCH employee or contractor, of the privacy rights of an individual
- a contravention of CCCH privacy policies and procedures
- a contravention of CCCH's Code of Conduct, if the contravention is related to personal health information
- a contravention of privacy-related terms and conditions in agreements with third party service providers
- a circumstance where personal health information is subject to unauthorized access, use, or disclosure or unauthorized copying, modification or disposal

Policy

4.4 CCCH will respond to and resolve all privacy incidents and breaches according to documented privacy incident management procedures maintained by the Privacy Officer.

4.5. The Privacy Officer will ensure that privacy and security general awareness training includes guidance on identifying privacy incidents and breaches.

4.6. The Privacy Officer will notify all CCCH clients whose PHI was subject to incident or breach in as timely a manner as possible.

4.7. CCCH's documented procedures for incident management will include detailed procedures for

- intake and documentation of incident reports
- containment and resolution of incidents and breaches
- notifications of affected clients
- incident investigation

4.8. CCCH employees will be trained to notify the Privacy Officer as soon as reasonably possible after a potential or actual incident or breach has been identified.

4.9. The Privacy Officer will evaluate the notification from the employee or contractor, and implement appropriate containment and resolution activities.

Investigation and follow-up

4.10. The Privacy Officer will conduct an investigation of each privacy or security incident that affects PHI in the custody of the CCCH.

4.11. The Privacy Officer will monitor the implementation of any recommendations in the incident investigation report intended to address the causes of the incident.

Third party service provider obligations

4.12. Third party service providers will be obligated, through their agreements with CCCH

- to immediately notify CCCH if the third party service provider detects or is responsible for a privacy incident or breach;
- to assume incident management responsibilities where required to support CCCH in addressing privacy incidents.

Incident: ***Incident report intake***

Management

4.13. Procedure: On receipt of a notification regarding a privacy incident, the Privacy Officer will:

- collect details regarding the incident from the employee who has reported the incident.
- document all available details regarding the incident
- instruct the employee who reported the incident to take reasonable measures to contain the incident if possible
- notify the privacy representative of any third party service provider with involvement in the incident

Containment and resolution

4.14. To contain the privacy incident, the Privacy Officer will:

- confirm the scope of PHI subject to the incident
- determine and conduct appropriate containment measures, and delegate containment measures to employees or third party service providers as needed

4.15. Containment and resolution measures should ensure that no further unauthorized access to, and use, disclosure or disposal of PHI occurs.

4.16. The Privacy Officer will update documentation about the incident with any details about the incident determined during containment and resolution of the incident.

4.17. The Privacy Officer will ensure that the privacy incident is resolved by confirming that the cause of the privacy Incident has been determined and addressed by CCCH employees.

4.18. The Privacy Officer will document the cause of the incident.

Notification

4.19. To notify the clients whose PHI was subject to breach, the Privacy Officer will:

- determine with relevant program managers the appropriate manner in which to conduct the notifications, based on managers' understanding of client expectations, and the severity of the incident {i.e., by phone, when the client next visits CCCH, etc.)
- prepare Privacy Incident Notification Forms for each affected client
- notify the affected clients in the manner determined in consultation with management

Incident investigation

4.20. To conduct the incident investigation, the Privacy Officer will complete, and document in an Investigation report, the following activities:

- collection of relevant information regarding the incident
- assessments of the information collected
- documentation of findings and recommendations

4.21. The Privacy Officer will send the completed investigation report to the Executive Director for review and approval.

4.22. When the Executive Director has approved the report, the Privacy Officer will implement the recommendations in the investigation report, and monitor the progress of Implementation on a monthly basis until completed.

5. Safeguards Policy

Purpose To ensure that CCCH has deployed effective safeguards to protect the privacy and security of personal health information in its custody.

Applicability This policy applies to all CCCH employees.

Responsibility The Privacy Officer develops, maintains and reviews this policy

The Chief Executive Officer approves this policy.

Policy

5.1. CCCH will safeguard PHI in its custody, or for which it has been given responsibility by another custodian, against:

- theft or loss;
- unauthorized use or disclosure;
- unauthorized copying , modification or disposal.

5.2. The Privacy Officer will ensure that CCCH has deployed information security safeguards at all sites of CCCH, including

- physical security measures protecting servers and physical IT infrastructure (locked server rooms with environmental controls)
- network security measures, including firewalls and anti-malware measures
- encryption of PHI at rest and in transit where appropriate
- implementation of internal network layers and endpoint security measures

5.3. The Privacy Officer will ensure that all paper records of PHI are subject to physical security safeguards, including storage in locked cabinets.

5.4. The Privacy Officer will provide training to employees in implementing administrative information security procedures, such as maintaining workspaces, ensuring that paper documents containing PHI are shredded when no longer required, etc.

5.5. The Privacy Officer will ensure that all electronic health information systems used by CCCH to retain PHI are subject to access controls, so that access to the PHI can be provided only to authorized employees.

5.6 CCCH employees will be trained on the creation of strong passwords for all electronic health information systems, and for all devices and services requiring passwords.

5.7. CCCH will encrypt portable or removable media (e.g., USB memory) that its employees use to store PHI.

5.8. CCCH will encrypt mobile computing devices (i.e., laptops and tablets) issued to employees.

5.9. CCCH will encrypt the smartphones that it issues to its employees.

5.10. CCCH employees will be permitted to use their own smartphones to carry out their job responsibilities if the smartphone has been encrypted by CCCH.

5.11. Employees who use their own smartphones to carry out their job responsibilities will sign an agreement with CCCH authorizing retrieval of and access to the smartphone by CCCH as required to address any privacy or security incident involving the use of the smartphone.

5.12. Employees will not store PHI on any portable device that is not encrypted.

Acceptable use of technology

5.13. CCCH employees will send PHI by email:

- only to recipients within CCCH's network
- to external email recipients only if the PHI Is protected by encryption

5.14. CCCH will not download or retain PHI in any form (including emails, attachments, SMS messages, photographs, sound or video files, etc.) onto any device that was not issued or approved by the CCCH.

5.15. CCCH employees will be required to have explicit approval from their managers to retain PHI on their smartphones, outside of PHI sent or received by email.

5.16. CCCH employees will:

- not leave smartphones and mobile computing devices used to carry out their job responsibilities unattended
- securely store smartphones and mobile computing devices when not in use
- not use automatic login procedures (such as password saving) on smartphones and mobile computing devices.

5.17. CCCH employees who work remotely will:

- transfer PHI retained on smartphones and mobile computing devices to CCCH's internal network on a regular basis
- delete PHI from smartphones and mobile computing devices when retention on the devices is no longer required.

5.18. CCCH employees who work remotely will not access and view PHI on smartphones or mobile computing devices in settings where the PHI can be viewed by individuals who are not authorized to view it (e.g., coffee shops, public transit, etc.)

5.19. CCCH employees will use unsecured email, or SMS or MMS messaging, to communicate with clients only if a client has consented to be contacted and to communicate with the employee in this manner.

6. Policy on Limiting Access to Personal Health Information

Purpose To ensure that the access of CCCH employees to personal health information is appropriately limited.

Applicability This policy applies to all CCCH employees.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Chief Executive Officer approves this policy.

Policy

6.1. CCCH maintains procedures and guidelines, including its Code of Conduct, which is intended to appropriately limit the access of employees to PHI.

6.2. Procedures to limit access to PHI are based on the "need-to- know" principle, which means that the access of employees to PHI will be limited only to that information they require to do their jobs at CCCH.

6.3. CCCH employees will be prohibited from accessing and using PHI collected from clients with whom they have no clinical relationship, unless such access is authorized by consent, or under applicable legislation.

6.4. The Privacy Officer will ensure that CCCH managers document the scope and purpose of access to PHI of each of their employees. This documentation will be conducted on onboarding or change of employment, and the documentation will be retained by the Privacy Officer.

6.5. CCCH employees are prohibited from accessing and using PHI if other information (e.g.,. de-identified and/or aggregate information) will serve the identified purpose for which the employee or contractor intended to access the PHI.

6.6. The Privacy Officer will audit the access of employees to PHI on a regular basis, according to the provisions of CCCH's Privacy Audit Policy.

---

7. Policy on Retention, Transfer and Disposal of Personal Health Information

Purpose To ensure that CCCH employees appropriately retain personal health information, and that this information is securely transferred and disposed of as required.

Applicability This policy applies to all CCCH employees.

Responsibility The Privacy Officer develops, maintains and reviews this policy

The Executive Director approves this policy.

Policy

7.1. Retention periods for all repositories of PHI will extend for only as long as the PHI is required to fulfill the purpose for which it was collected, or as required or permitted by law.

7.2. The Privacy Officer will ensure that CCCH maintains inventories of all repositories of PHI in any form (paper, electronic).

7.3. Inventories of PHI will include a retention schedule for each repository of PHI that has been documented.

7.4. Client health records created for the purpose of providing health care will be retained by CCCH:

- for adult clients, for 10 years after the client's discharge or last visit, or the client's death
- for clients who are minors, for 10 years after the client's 18th birthday (whether alive or deceased)

7.5. All repositories of PHI will be retained in a secure manner according to the requirements of CCCH’s Safeguards Policy.

7.6. CCCH employees will be assigned as data stewards for each repository of PHI identified in CCCH's inventory, and will be responsible ensuring that repositories of PHI are appropriately safeguarded.

7.7. CCCH will specify retention periods and secure disposal procedures for all paper records of PHI that are scanned into the CCCH's electronic systems for use and/or retention.

7.8. CCCH will ensure that all transfers of PHI within the CCCH, or to service providers, are secure, including electronic transfers of data, and transfers of physical records, such as paper files.

7.9. The Privacy Officer will ensure that a log of all transfers of PHI to third party service providers is maintained.

7.10. CCCH employees will be required to transfer or delete PHI from portable devices (e.g. laptops, tablets) and portable media (e.g., USB drives) once the purpose for retaining the PHI on the device has been fulfilled.

Disposal of Records

7.11. The Privacy Officer will ensure that CCCH follows documented procedures for secure disposal of records of PHI, so that the records are disposed of through processes that make the reconstruction of the records impossible.

7.12. CCCH employees will be required to dispose of paper records of PHI using designated and locked bins clearly marked for this purpose.

7.13. CCCH employees will be required to maintain CDs, USB keys and hard drives intended for destruction separately in a designated and locked bin clearly marked for the secure retention of records of PHI, pending their secure disposal.

7.14. Third party service providers that have been contracted by the CCCH to securely dispose of records of PHI in any form will be contractually required to provide CCCH with certificates of destruction for all records of PHI of which they dispose.

8. Execution of Agreements with Third Party Service Providers Policy

Purpose To ensure that CCCH executes agreements with third party service providers that include appropriate privacy and security provisions.

Applicability This policy applies to CCCH's relationships with third party service providers in which the providers will have access to personal health information in the course of providing services to CCCH.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Chief Executive Officer approves this policy.

Policy Agreements prior to access to personal health information

8.1. CCCH will execute agreements with all third party service providers for services before providing the third party service provider with access to PHI, or to environments where employees of the service provider may have access to PHI.

Key terms in agreements

8.2. Third party service providers with access to personal health information will be subject to the same conditions, where applicable, as CCCH employees regarding the handling of personal health information.

8.3. The Privacy Officer will ensure that agreements with a third party service providers that have access to PHI:

- describe the purposes and associated services for any access (including incidental access) of service provider employees to PHI;
- identify the service provider's privacy responsibilities related to the services provided;
- obligate the service provider to meet all obligations in CCCH privacy policy that apply to the activities of the service provider employees;
- specify privacy and security terms for the exchange of information between CCCH and the service provider;
- Include the right of CCCH to audit the service provider to ensure that specified privacy and security safeguards and service delivery terms have been implemented as required in the agreement with the service provider.

Provisions regarding controls in agreements with third party service providers

8.4. The Privacy Officer will ensure that provisions addressing the following controls and related procedures are included in agreements with third party service providers where relevant to protect the privacy of PHI:

- physical protection controls
- protection against malicious software
- controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during, the agreement
- restrictions on copying and disclosing information,
- privacy and security awareness training provided by the service provider for all service provider employees
- change management procedures for software and systems
- access control policies and procedures that indicate

    - all reasons for access to systems and to personal health information by agents of the third party service provider
    - permitted access methods
    - user authorization methods
    - the requirement to maintain a list of all users with access to the system and to personal health information
    - a process for revoking access rights

Execution of agreement

8.5. CCCH managers or employees responsible for procurement of services will notify the Privacy Officer when they intend to contract the services of a third party service provider.

8.6. The Privacy Officer will provide standard privacy and security provisions for agreements with third party service providers to CCCH managers or employees responsible for procurement of services from service providers.

8.7. CCCH managers or employees responsible for procurement of services will execute the agreement with the third party service provider, and notify the Privacy Officer that the agreement has been executed.

Review of agreements

8.8. The Privacy Officer will review CCCH's templates for third party service provider agreements on an annual basis to ensure consistency with CCCH privacy policy.

Log of third party service provider agreements

8.9. The Privacy Officer will log the execution of all agreements with privacy and security provisions.

9. Privacy Risk Management Policy

Purpose To ensure that privacy risks within CCCH have been identified, documented, and appropriately managed.

Applicability This policy applies to all CCCH employees responsible for the assessment and review of CCCH privacy program.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Executive Director and Board of Directors approve this policy.

Policy Privacy risk management

9.1. The Privacy Officer will maintain an inventory of privacy risks identified within CCCH.

9.2. The inventory of identified risks will include:

- assessment of each risk and its potential negative impact on the safeguarding of PHI and PI
- the ranking of the risk
- the approved approach for mitigating the risk, the schedule for implementing the approach, and the employees responsible for implementation

9.3. The Privacy Officer will ensure that managers within the CCCH have received training and resources to support their identification and reporting of privacy risks.

9.4. The Privacy and Security Committee will review the privacy risk inventory on a regular basis to assess newly identified risks, and to review progress on mitigation of existing risks.

Privacy impact assessments (PIAs)

9.5. CCCH will conduct privacy impact assessments to identify the privacy risks that an initiative, program or technology solution poses to PHI that will be collected, used and/or disclosed through the initiative.

9.6. All PIAs conducted by CCCH will include an inventory of the privacy risks identified as a result of the assessment.

9.7. CCCH employee responsible for conducting the PIA will communicate the finalized inventory of privacy risks from the PIA to the Privacy Officer.

9.8. PIAs will not be conducted where existing programs or systems are changed or new programs or systems are implemented, if no personal health Information is involved.

10. Privacy Audit Policy

Purpose To ensure that the compliance of CCCH employees with privacy policies and procedures is audited on a regular basis, and that any privacy risks identified as a result of the audit are documented and appropriately mitigated.

Applicability This policy applies to all CCCH employees.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Board of Directors and Executive Director approve this policy.

Policy

10.1. The Privacy Officer will ensue that regular privacy audits are conducted within CCCH according to an annual privacy audit plan.

10.2. The Privacy Officer is responsible for developing the annual privacy audit plan.

10.3. The annual audit plan will be reviewed by the Privacy and Security Committee, and approved by the Executive Director.

10.4. The privacy audit plan will be developed to review and audit:

- employee and contractor access to PHI
- employee and contractor compliance with CCCH's privacy policies and procedures.

10.5. The privacy audit plan will include both administrative and technical auditing activities.

10.6. The privacy audit plan will be implemented by CCCH managers, who will report the results of the audit to the Privacy Officer.

10.7. All privacy risks identified in the course of executing the privacy audit plan will either be addressed immediately by the Privacy Officer, or entered into CCCH's privacy risk inventory.

10.8. All activities conducted to complete the privacy audit plan will be logged by the Privacy Officer.

---

11. Access and Corrections Policy

Purpose To ensure that CCCH responds to requests for access to records of personal health information, and makes corrections to these records if required.

Applicability This policy applies to CCCH employees with privacy program responsibility.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Chief Executive Officer approves this policy.

Policy

11.1. The Privacy Officer will maintain procedures for responding to and fulfilling a request from an individual for access to her or his records of PHI, and for correction of the records.

11.2. The Privacy Officer will post and maintain information about these procedures on CCCH's public-facing web site.

11.3. CCCH is authorized under PHIPA to deny access and correction requests under specific conditions.

11.4. The Privacy Officer will acknowledge an individual's request for access to or correction of her or his records of PHI within ten business days.

11.5. The Privacy Officer will fulfill the request for access or correction within thirty calendar days of receipt of the request, if there are no grounds for denying the request.

11.6. The Privacy Officer will correct or amend an individual’s records of PHI if the Individual has sufficiently demonstrated that the records are inaccurate or incomplete.

11.7. The Privacy Officer will provide an individual with a reason for denying request for access or correction if it is determined that denial is warranted, and is authorized under PHIPA.

11.8. The Privacy Officer will record or document an individual's disagreement regarding the denial of her or his request for access or correction to PHI.

---

12. Privacy Inquiries and Complaints Policy

Purpose To ensure that CCCH appropriately responds to privacy- related complaints and inquiries.

Applicability This policy applies to CCCH employees with privacy program responsibility.

Responsibility The Privacy Officer develops maintains and reviews this policy.

The Board of Directors and Executive Director approve this policy.

Policy

12.1. The Privacy Officer will accept inquiries and complaints from individuals regarding its privacy practices and the privacy safeguards it has deployed to protect PHI.

12.2. The Privacy Officer will maintain procedures for receiving, managing and investigating complaints, inquiries and other feedback.

12.3. The Privacy Officer will post and maintain information about these procedures on CCCH's public-facing web site.

12.4. The Privacy Officer will acknowledge receipt of a privacy-related inquiry or complaint within ten business days of receipt of the inquiry or complaint.

12.5. The Privacy Officer will determine if an investigation into a privacy- related complaint is required after reviewing the details of the complaint.

12.6. If an investigation is required, the Privacy Officer will provide the individual or CCCH that submitted the complaint with an outcome of the investigation within 30 business days of the receipt of the complaint.

12.7. If a complaint investigation indicates that a privacy incident has occurred, the Privacy Officer will address the incident through the CCCH's privacy incident management procedures.

12.8. The Privacy Officer will log the receipt of and response to all privacy Inquiries and complaints.

---

13. Privacy and Security Tip Sheet

Meeting CCCH's Privacy Obligations

To meet your privacy obligations as an employee of CCCH, you should:

- **Carry out your job responsibilities according to CCCH's privacy policies**
- **Talk to your manager or Privacy Officer if you have any privacy related concerns or questions**

Limiting Collection of PHI

To ensure that you appropriately limit your collection of PHI, you should:

- **Only collect the information you require to meet the purposes of your collection**
- **Review all PHI you collect about clients from other sources (hospitals, etc.) and keep only the information you need**

Sending PHI Securely

To transmit or deliver PHI securely, you should:

- **Verify contact information before sending PHI by phone, email, fax, courier, etc.**
- **Only email PHI to an external recipient if it is encrypted or if the client approves the sending of PHI using unsecured email**
- **Include a cover sheet when faxing PHI indicating that the fax contains PHI and is intended only for the indicated recipient**
- **Remove all documents from fax machine when you have finished faxing them**

Obtaining Knowledgeable Consent

CCCH relies on posted client notices to inform clients of the purposes for collection use and disclosure of the PHI.

However, if you believe that a client does not understand the purposes for which we will disclose his or her PHI, you should:

- **Verbally remind the client of our purposes for sharing his or her PHI with other health care providers**
- **Document any such conversations in the clients chart**

Limiting Use and Disclosure of PHI

To ensure that you appropriately limit the use and disclosure of PHI, you should:

- **Only access PHI when you must do so to fulfill your job duties**
- **Not access the PHI of any client to whom you are not providing our services**
- **Only disclose PHI required to fulfill the purpose of the disclosure and do not provide more information than is required**

Storing PHI Securely

To securely store PHI, you should:

- **Store all paper files containing PHI in locked cabinets or cases**
- **Lock files and laptops containing PHI in the trunk of your car when offsite when you are not using the files, or out of plain sight in your locked car**
- **Encrypt PHI stored on mobile computing devices (laptops, tablets, smartphones) and password protect the devices**
- **Store files containing PHI on laptops or tablets for only as long as the data is required for use on the laptop or tablet**

Managing and Accessing PHI Securely

To securely manage PHI in your work space, you should:

- **Not leave any materials containing PHI unattended at your desk and lock these materials in cabinets when leaving your desk unattended**
- **Dispose of paper materials containing PHI in designated shredding bins, not in blue recycling bins**
- **Password protect your computer when you leave it unattended**

To access PHI in a secure manner, you should:

- **Not remove paper files containing PHI from locked cabinets or briefcases for any longer than they are required**
- **Not access and view PHI in busy or high traffic areas within CCCH or access and view PHI in busy public spaces where it could be seen (such as public transit)**

What is Privacy Incident?

Privacy incidents are events that involve the unauthorized

- **Collection, access use or disclosure, OR**
- **Retention, modification or destruction**

of PHI in the custody of CCCH.

Incidents can be caused by CCCH employees, by individuals external to CCCH or by third party service providers.

Incidents may also be the result of technical issues and failures such as malware attacks. These events can be inadvertent or deliberate and even malicious.

Responding to Client Privacy Inquiries

If a client has privacy concerns or requests access to his or her records of PHI, you should:

- **Indicate to the client that the Privacy Officer will accept questions and complaints about privacy practices as well as client requests for access to or correction of client records of PHI**
- **Inform the client that contact information for the Privacy Officer is available as well as forms that the client can print and complete to submit privacy questions**

What should you do if you cause or discover and incident?

If you have caused or discovered a privacy incident, you should:

- **Take reasonable steps to contain the incident if possible**
- **Immediately notify the Privacy Officer either by phone or email, provide the Privacy Officer with details regarding the incident and answer any questions**
- **Take further measures to contain the incident if directed by the Privacy Officer**
- **Notify your manager and provide him or her with details regarding the incident**
- **Cooperate with your manager and the Privacy Officer to provide support in further containing, resolving and investigating the incident**