CHATHAM-KENT Health Alliance

CKHA POLICY and PROCEDURE

Title:	Privacy Policy		**Document Number:** HTI-1-009
Approved by:	Senior Leadership Team	**Date Revised:**	April 2, 2020
Policy Owner:	Chief Privacy Officer	**Date of Origin:**	October 6, 2003

BACKGROUND

In compliance with Ontario's privacy legislation, the Chatham-Kent Health Alliance (CKHA) intends to self-regulate, to the fullest extent possible, based on the Personal Information Protection and Electronic Documents Act (PIPEDA) fair information principles.

COMPETENCIES

This policy applies to all staff and affiliates who work on behalf of the Chatham-Kent Health Alliance, including independent health care practitioners, contracted individuals, researchers, solicitors, students and volunteers.

INDEX

POLICY

It is the policy of CKHA to protect the privacy and confidentiality of patient personal health information (PHI) as required by law. This applies regardless of the format of the information (i.e. verbal, written or electronic). The goal of this policy is to facilitate the protection of the privacy, confidentiality, and security of patient PHI held by CKHA and to facilitate the use of that information to improve both the quality of care for patients and the effective use of CKHA's health care resources.

If a CKHA staff member or affiliate has received any health care services or treatment at CKHA, he/she is considered a patient in the context of this document and his/her PHI is subject to the same policies and procedures as that of all CKHA patients. Exception is provided for health care services administered under the direction of The Occupational Health, Safety and Wellness Department, the documentation of which is not subject to this policy, but it shall be treated as confidential and breaches shall be subject to disciplinary action, up to and including termination of employment.

This policy was developed within the context of relevant Federal and Provincial Law. Subject to a few exceptions, if there is conflict between provisions in this policy and those in another policy of CKHA, this policy prevails unless this or the conflicting policy specifically provides otherwise. No contract or agreement that contravenes this policy may be executed or entered into by anyone to whom this policy applies. Questions or complaints from the public should be directed to the Chief Privacy Officer.

Audits of the use of PHI will be conducted by the Health Records Department and TransForm Shared Services under the direction of the Chief Privacy Officer to ensure that confidentiality and privacy are maintained.

Violations of this policy will be reviewed and addressed. All individuals shall report breaches of confidentiality of information, whether inadvertent or intentional, in the RL6 system and to their direct supervisor to ensure a prompt remedy of the occurrence (see Breach of Confidentiality). Effective reporting aids in identifying process or systemic issues that may occur in multiple areas if not identified and addressed. If the breach of confidentiality is found to be

serious, disciplinary action may be taken, up to and including revocation of privileges or dismissal from employment or other relationship with CKHA.

Personal Health Information Privacy Principles
This policy balances individuals' right to privacy with respect to their own PHI with the legitimate needs of persons and organizations providing health care services to access and share this information. CKHA has developed this policy and related procedures based on the following principles, adapted from the Personal Information Protection and Electronic Documents Act (PIPEDA) fair information principles for the protection of personal information. Most privacy legislation in the world is based on these ten privacy principles. CKHA applies these principles to verbal, electronic or written PHI used for treatment, other health care services and research.

Accountability
CKHA is responsible for the PHI under our control and has designated individuals (Chief Executive Officer and Chief Privacy Officer) who are accountable for compliance at all hospital sites.

CKHA complies with the Personal Health Information Protection Act (PHIPA) by:

- Implementing policies and procedures to protect your PHI, and all other confidential information including information relating to patients, staff and affiliates. (Affiliates include physicians, students, volunteers, researchers and contracted individuals who are not paid by CKHA but have a working relationship with the Hospital);
- Responding to complaints and inquiries;
- Educating our staff and affiliates about privacy policies and practices.

Identifying Purposes
CKHA will identify the purposes for which PHI is collected at or before the time of collection. These purposes will be conveyed by means of the CKHA website. The primary purpose to collect, use and share PHI is to deliver patient care. CKHA also uses PHI for administrative purposes, research, teaching, statistics, fundraising and to comply with legal and regulatory requirements. Persons collecting PHI will explain to patients the purposes for which the information is being collected.

Consent for the Collection, Use, and Disclosure
If PHI is being used by CKHA staff/affiliates to provide or assist in providing health care to registered patients of CKHA, it is reasonable to imply that the patients or Substitute Decision Makers (SDM) have consented to this use. However, if a patient refuses to consent to a specific use, consent cannot be implied and the refusal must be respected. Patients have the right to know why we are collecting their information and how it is being used. Patients also have the right to withdraw their consent at any time, unless the collection, use or sharing is required or permitted by law.

Limiting Collection
CKHA will not collect PHI indiscriminately. Both the amount and the type of information collected will be limited to that which is necessary to fulfill the purposes identified at the time the information is collected. PHI is collected by CKHA primarily for providing or assisting in providing health care.

Limiting Use, Disclosure and Retention
PHI may be used only for the purposes for which it was collected, except with consent or as required by law. The information is retained only as long as necessary, and securely destroyed in accordance with legislation and CKHA's policies, guidelines and procedures.

Under statutory requirements set out by the Ontario Hospital Association, PHI of adult inpatients and outpatients is stored for a minimum of 10 years after discharge or death. PHI of pediatric patients is stored for a minimum of 10 years after the patient's 18th birthday (see Public Hospitals Act/ADM-1-013: Records Retention).

In compliance with PHIPA and the Public Hospitals Act, records may be moved bi-annually to a secure offsite storage-holding company. Documentation of offsite storage records must be archived and retrievable by the responsible department Director and/or Manager. If required, access to records stored offsite can be arranged by contacting the Manager of Health Records.

Ensuring Accuracy
CKHA will make every effort to ensure the PHI the Hospital holds is accurate, complete and up-to-date. Patients have the right to challenge the accuracy of the information.

If a patient wishes to challenge the accuracy and/or completeness of the information and have it amended, they must provide a written request outlining the additional or amended information to be included as part of the permanent health record. If CKHA disagrees with the content of the amendment, a statement of disagreement will be completed and attached to the health record.

Ensuring Safeguards
CKHA applies security safeguards appropriate to the sensitivity of PHI to aim to protect it against loss, theft, unauthorized access, disclosure, copying, use, or modification, regardless of its format. Protection may include physical measures (e.g. locked filing cabinets and restricted access), organizational measures (limiting access on a "need-to-know" basis), and technological measures (use of passwords, encryption and audits). New and current staff and affiliates are required to complete privacy and confidentiality education annually and sign a confidentiality agreement as a condition of employment or affiliation. Contracted agents are bound to privacy and confidentiality as a condition of the contract.

Openness about Policies and Practices
CKHA makes information about their privacy policies and practices available by means of posted policies at registration points and other public areas as well as on the CKHA website. Information provided includes:

- contact information for the hospitals' Chief Privacy Officer and/or delegate, to which complaints or inquiries can be forwarded;
- the process for a patient to access his/her PHI held by CKHA;
- a description of the type of PHI held by CKHA, including a general description of its use, and common examples of how the information may be shared.

Individual Access to Own Personal Health Information
Upon request, within a reasonable time and at a reasonable cost (as outlined by the Fee Schedule for Personal Health Information Request), an individual will be informed of the existence of his/her PHI and will be given access to it. They can challenge its accuracy and completeness and have it amended as appropriate.

Exceptions to providing access will be limited and specific. This may include information that is prohibitively costly to provide, refers to other individuals, cannot be disclosed for legal, security or proprietary reasons, and/or is subject to solicitor-client or litigation privilege. An individual must provide sufficient information to permit CKHA to identify the existence of PHI, including details of third-party recipients.

Challenging Compliance
An individual will be able to challenge CKHA's compliance with its policies and privacy law to the Chief Executive Officer and/or Privacy Office delegates. CKHA has procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of PHI. CKHA will investigate all complaints. If a complaint is justified, CKHA will take appropriate measures including, if necessary, amending their policies and practices.

Confidential Information
CKHA has a legal and ethical responsibility to protect the privacy of patients, their families, clients, staff and affiliates, and to ensure confidentiality is maintained. Confidentiality is defined as not divulging, releasing or revealing information without the express consent of the patient and/or Substitute Decision Maker to individuals not within the "circle of care" of the patient.

CKHA considers the following types of information to be confidential:

- Personal information and PHI regarding patients and their families;
- Personal information, PHI, employment information, and compensation information regarding staff and affiliates; and
- Information regarding CKHA operations, which are not publicly disclosed by CKHA (e.g. unpublished financial statements, legal matters, quality of care etc.).

This policy applies whether this information is verbal, written, electronic, or in any other format.

In addition to standards of confidentiality which govern Regulated Health Professionals, staff and affiliates are bound by CKHA's responsibility to maintain confidentiality. CKHA expects staff and affiliates to keep information which they may learn or have access to because of their employment or affiliation, in the strictest confidence. It is the responsibility of every staff and affiliate:

- To become familiar with and follow CKHA policies and procedures regarding the use, collection, disclosure, storage and destruction of confidential information.
- To collect, access and use confidential information only as authorized and required to provide care or perform their assigned duties.
- To divulge, copy, transmit or release confidential information only authorized and needed to provide care or perform their duties.
- To safeguard passwords or any other users' codes to access computer systems and programs and to assume full responsibility for activity undertaken using their security codes/passwords. This includes using access only to perform their role and not to use access on the behalf of another individual to review PHI at the request of another party.
- To identify confidential information as such when sending e-mails or fax transmissions and to provide direction to the recipient if they receive a transmission in error.
- To discuss confidential information only with those who require this information to provide care or perform their duties and never within range (hearing or seeing) of others who should not have access to this information.
- To continue to respect and maintain the terms of the Confidentiality Statement after an individual's employment and/or affiliation with CKHA ends.

Confidentiality Statement

It is a condition of employment/privileging contract/association that staff and affiliates review this policy and sign the Confidentiality Statement before receiving access to information or records, or performing any duties at CKHA (access CKHA's Confidentiality Statement Form here).

Confirmation of the successful completion of the education program and the signed Confidentiality Statement will be kept on the individual's file in:

- Human Resources Department for staff
- Volunteer Services for volunteers
- Departmental Managers/Directors offices under whose supervision students, contract staff, vendors or consultants are working if not coordinated by a separate Department (i.e. any individual employed by third-party organizations who are performing work at CKHA on a temporary basis)
- Medical Affairs for physicians, residents, medical students, dentists, and midwives

Managers must review any department specific information or procedures related to confidentiality with new CKHA staff and affiliates.

It is the responsibility of CKHA to ensure that all Affiliation Agreements with educational institutions include provisions outlining the obligation to ensure that students and faculty abide

by CKHA's standards of confidentiality/policies and that the standard confidentiality requirements have been included in the Affiliation Agreement.

Breach of Confidentiality

A breach of confidentiality includes any inadvertent or intentional collection, use and/or disclosure of PHI, whether verbal or written, in breach of this policy. Staff and affiliates of CKHA have the right and responsibility to report a breach of confidentiality without fear of reprisal for doing so.

Staff and affiliates must report suspected breaches of confidentiality, or practices within CKHA that compromise confidential information, in the electronic Patient Safety Reporting system and to their Departmental Manager or Direct Supervisor. If the Manager is the individual suspected of the breach, staff and affiliates may contact the Chief Privacy Officer directly.

Department Managers, in conjunction with Human Resources and/or Quality/Risk Management and with the support and guidance of the Chief Privacy Officer, depending on personnel involved, will investigate alleged breaches of confidentiality. If allegations are substantiated, the individual may be subject to disciplinary action up to and including termination of employment/contract or loss of privileges or affiliation with CKHA, reporting to the individual's professional College, and/or civil action/criminal prosecution.

Request to View Personal Health Information (PHI)

Standard Access

The record of PHI created, acquired or maintained, regardless of the medium (verbal, written, visual or electronic) or location for a registered patient of the organization will be under custody and control of the Health Information Custodian (HIC). The personal information and PHI contained in the record is owned by the patient and must be kept confidential. Individuals (or appropriate SDM) have a right of access to records of their own PHI, except if access could result in serious harm to any person or the identification of a person who provided information in confidence.

Inpatient Records

For **an inpatient** who requests to view his/her own chart, access to the personal health information will be executed in the presence of the Patient and/or Patient Representative, Physician, Unit Manager or designated member of the Health Records team as determined by the Chief Privacy Officer.

Direct all requests for a copy of an original inpatient/outpatient health record by a patient or third party (e.g. family member, lawyer, etc.) to the Health Records Department

Charges for copies of patient information will be applied as outlined in the Fee Schedule for Personal Health Information Request. Fees may be waived on compassionate grounds by the Manager of Health Records.

Discharged Records
A discharged patient or client who is mentally capable to examine his/her health record, or can consent to disclosure of his/her health record must complete a Consent to Disclose Personal Health Information form and return it to the Health Records Department.

If access is approved to view all or part of the health record, the Patient Relations Specialist or Director of the patient unit will schedule an appointment for viewing. This will occur in a confidential area. During the appointment the patient/SDM may make their own notes.

Placing a Restriction (Lock Box) on Your Record
Patients have a right to restrict access to their record. This can be done at the point of registration or, to the extent possible, at any time during or after their visit (see CKHA's Lock-Box Request form). When restricting access after registration, it is the patient's responsibility to notify other system administrators that enable a shared electronic patient record, such as Clinical Connect.

CKHA restricts personal access to psychiatric patient records under the authority of the Mental Health Act (refer to MHA, R.S.O. 1990, Chapter M.7- sec. 35 and 36).

Release of Information – Health Records
Disclosure or Copy of Personal Health Information Including Restrictions
Disclosing or copying of PHI must comply with legislative requirements, professional standards and the procedures outlined in this policy. PHI may only be disclosed or copied by the organization from which it originated, i.e. CKHA must not disclose or copy records that exist in either paper or electronic format that originated from a visit/admission from another organization unless under specific exceptions, and only by the Health Records Department. In accordance with legislation, CKHA has 30 days to complete release of information requests.

Agents of CKHA are not authorized to provide a patient and/or third parties with a copy of a patient health record. All PHI disclosed or copied will be carried out through the Health Records Department, excluding PHI required for the purpose of continuing patient care. Faxing patient information should only be done on an urgent basis for the purpose of continuing care (see Ensuring Safeguards).

A Consent to Disclose Personal Health Information form permits the disclosure of PHI that has already been created, collected, or maintained on or before the date that the consent is signed. An **original signed** consent is required, except when the request is made by an organization that falls within the patient's circle of care.

The Consent to Disclose Personal Health Information form must include:

- Name of patient (or legal designate) authorized to release information
- Name of Hospital/Site
- Description of the information being requested

- Name of agency receiving the information
- Date range of personal health information requested
- Signature of patient (or legal designate)
- Signature of witness
- Date authorization signed (within 6 months of request)

For more information on disclosing PHI, refer to HTI-1-010: PRIVACY: Disclosure of Patient Information.

Mental Health Records
If the request is to access or obtain a copy of a **Mental Health client** record, the Health Records Department will acquire appropriate consent and will follow guidelines for approval of the request.

For client requests, Health Records requires the attending health care practitioner or delegate to approve requests within 5 business days.

If a decision is made to refuse the request, the custodian will sever the record and provide access to or a copy of the rest of the chart. CKHA will refuse an individual's request to personal health information if there is a significant likelihood of substantial adverse effects on the physical or mental health of the client or of harm to a third party. Additionally, access to a client health record may be refused for reasons permitted by law, which include:

- access is likely to result in harm to the treatment or recovery of the client or,
- access is likely to result in injury to the mental condition of a third person, or bodily harm to a third person.

The Health Records Department is responsible for notifying the client (or delegate) that his/her request has been refused.

No Consent is required in the following specified circumstances:

- For those involved in a patient's Circle of Care, provided the PHI disclosed is reasonable and for the purposes of providing health care.
- To contact a relative or most appropriate individual if the patient is injured, incapacitated or ill and is unable to give consent personally.
- Disclosures related to risks i.e. DUTY TO WARN: If the custodian believes on reasonable grounds that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons. **Consult Quality/Risk Management/Chief Privacy Officer prior to disclosure.** (See PTS-2-017: Identification, Documentation and Reporting of Child Abuse and Neglect)
- Disclosures for health or other programs: Communicable Diseases to the Chief Medical Officer of Health. **Consult Infectious Disease Practitioner.**
- Disclosures for proceedings: on receipt of a Warrant, Summons, or Subpoena. **Consult Risk Management/Chief Privacy Officer.**

- Disclosures Complying with Mandatory Legislated Disclosure Requirements: Mandatory Gunshot Wound Reporting, Family & Children's Services Act (a child in need of protection)
- Disclosure for planning and management of the health system, e.g. prescribed entity such as Cancer Care Ontario
- For monitoring health care payments: Minister of Health
- Disclosures for analysis of the health system
- Deceased patient:
    - For the purpose of identifying the individual
    - For the purpose of informing any person whom it is reasonable to inform in the circumstances of;
    - The fact the individual is deceased or suspected to be deceased
    - The circumstances of death; where appropriate
    - To the spouse, partner, sibling or child of the individual if the recipients of the information reasonably require the information to make decisions about their own health care or their children's health care

If unsure, contact: QUALITY/RISK MANAGEMENT/CHIEF PRIVACY OFFICER/HEALTH RECORDS/MANAGER/DIRECTOR

Disclosure Fees

Fees may apply as set out in the regional Local Health Integration Network (LHIN) fee schedule (see Appendix A), in compliance with Health Order HO-009 of the Information and Privacy Commissioner of Ontario. A pre-payment of the applicable fee must accompany a request.

Research, Education and Quality Assurance

This section of the policy establishes standards for staff and affiliates regarding their access to PHI for research, education, and quality assurance purposes. This policy applies to all PHI compiled in the organization's health records, regardless of the medium or storage location.

This section does not apply to:

- The use of PHI for direct patient care, legal, or other purposes (see References); and,
- Aggregate PHI (de-identified data) sought by staff and affiliates solely to prepare a research protocol or clinicians who wish to review their own individual patient records for the same purpose.

Only authorized staff and affiliates who have completed corporate Privacy and Confidentiality Education and signed a Confidentiality Statement may access PHI for research, education, and/or quality assurance purposes. Authorized staff and affiliates who access PHI for these purposes are responsible for safeguarding, disclosing and disposing of PHI in accordance with corporate policies on privacy, confidentiality, data security, release of information and applicable privacy legislation.

Electronic records may only be viewed for research, education and/or quality assurance purposes in the Health Records Department or in other departments in which authorized staff and affiliates have access to the Electronic Patient Record (EPR) system. There are situations where remote access can be arranged in select circumstances in conjunction with the Health Records Department.

Photocopies of hard-copy health records and/or the reproduction of health records in any other format must not be made without the authorization of the Manager of Health Records (or delegate) in the Health Records Department.

Regular and Ad Hoc audits are conducted to ensure compliance with this policy.

Education Purposes
Authorized staff and affiliates may access the organization's PHI for the evaluation of patient care or for internal clinical education purposes involving staff and affiliates. Identifiable patient information is used for internal teaching purposes only where necessary. PHI may be used by authorized staff and affiliates for external education purposes, provided no identifiable patient information is disclosed.

Authorized staff and affiliates include members of the physician, dental and midwifery staff, allied health staff and students assigned to the organization. Authorized staff and affiliates accessing the EPR for education purposes must document the reason for their access within each patient's EPR using the "comments" button.

Authorized staff and affiliates accessing hard-copy health records for education purposes must:

- Submit a Request for Access to PHI for Research, Education and Quality Assurance to the Manager or designate in Health Records;
- Present their Hospital ID badge, or other acceptable personal identification, at the time a request to review/provide access to electronic health records for education purposes at no cost. If copies are required in unique situations, this must be reviewed with the Health Records Manager.

Quality Assurance Purposes
With the knowledge and permission of management, the Manager of Health Records or the Chief Privacy Officer, staff and affiliates may access PHI to determine quality assurance or quality improvement of hospital programs/services. Health Records provides access for quality assurance purposes at no cost. Authorized staff and affiliates accessing hard-copy health records for quality assurance purposes must:

- Submit a Request for Access to PHI for Research, Education and Quality Assurance to the Manager or designate in Health Records.
- Present their Hospital ID badge, or other acceptable personal identification at the time a request to review/retrieve a hard-copy health record is made.

- Authorized staff and affiliates accessing the EPR for quality assurance purposes must document the reason for their access within each patient's EPR using the comments section.

Research Purposes
Staff and affiliates may access the organization's PHI for research purposes provided that:

- The research plan is approved by the Ethics and Research Committee (ERC).
- A member of the research team submits a Research Application Package to the Chair of the ERC and to the Program Director for the area the study will occur.

All PHI requirements are included in the application submission process. Member(s) of the research team must present their CKHA ID badge, or other acceptable personal identification, at the time a request to review/retrieve a health record is made.

PHI may be disclosed to a researcher only if the ERC has approved the project or program. The ERC will specify that the researcher is required to obtain written consent to the disclosure of PHI for the purposes of the project or program from the individuals to whom the information relates.

A letter of approval from the ERC and any required consent forms are required for individuals wishing to use PHI as part of any research protocol and must be presented to the Health Records Department. Depending on the nature of the request for information, a consult regarding the retrieval of the information may need to be scheduled with the Health Records Department. A list of researchers that will be accessing PHI is required and all researchers and/or assistants must sign a confidentiality agreement with CKHA.

When a health record is transmitted or copied for use outside the facility for the purpose of research, academic pursuits or the compilation of statistical data, the name of and any means of identifying the patient will be removed and a signed statement of confidentiality shall be obtained from the recipient of the information that she/he will not disclose the name of or any means of identifying the patient and will not use or communicate the information or material in the health record for a purpose other than research, academic pursuits or the compilation of statistical data.

Students
Students of all clinical professions, who in training at CKHA for an official period of training, may have access to the health records on clinical units, in clinic, or within programs and services, as necessary for their training, at the discretion of their Supervisor and Program Staff. Students accepted by CKHA are considered to be part of the health care team. Students must have signed a Confidentiality Statement prior to commencement of their placement and are bound by the same practices and principles as staff.

For students to gain access to health records other than those located on the nursing unit/program/clinic, a written request giving the name of the patient and the Master Patient Index (MPI) number, verifying the student's status and clinical involvement, signed by the student's supervisor is required. This request is to be presented to Health Records who will then authorize access to the specific record.

Consent and Capacity Board Hearings
In a proceeding before the Consent and Capacity Board, all parties shall be given an opportunity to examine and copy any documentary evidence that will be produced and any report whose contents will be given in evidence in accordance with the Health Care Consent Act (section 76(1) & (2)). Upon notification of the hearing, the nursing station shall make the appropriate arrangements for the patient/client to view his/her health record if requested by the patient/client. Lawyers (acting for a current inpatient) may examine the health record on the unit/program/clinic. If a lawyer requests photocopies of the health record, staff will comply with procedures for photocopying health records.

Rights Advisor/Lawyer
The Rights Advisor shall only be granted access to patient/client information, which is necessary to perform his/her routine duties (e.g. legal status, treatment status information etc.). Refer all requests for PHI from lawyers, including telephone calls, for access to health records to the Health Records Department.

Media Requests
Any release of information to the media must be in compliance with the media relations practices of the Communications Department and all inquiries from the media regardless of their nature should be immediately referred to the Communications Department (see ADM-2-039: Media Request for Patient Condition).

After hours, the "most responsible" registered nurse or Administrator-on-Call may release a one-word condition update to the media provided the reporter already has the patient's full name and the patient or SDM has given consent. These updates include good, fair, serious, critical and still being assessed.

Verbal/Telephone Requests
Basic hospital information (location and phone number) will be given out upon a request that identifies the patient by name as being a patient at CKHA unless the patient has instructed, upon admission/registration that this information not be disclosed. In this case, the patient will be flagged as confidential and appear highlighted on patient census inquiry functions and documented in the patient chart indicating that no information will be released.

Fundraising
In general, custodians are only permitted to collect, use or disclose PHI for non-health-care-related purposes with the express consent of the individual in question. However, Ontario

Privacy Legislation provides special rules for fundraising. It provides that the collection, use or disclosure of an individual's name and mailing address (or the name and mailing address of a SDM, if applicable) for fundraising may take place with the implied consent of the individual in question, as long as the following requirements are met:

- That the collection, use or disclosure of PHI for fundraising purposes is only permitted where the fundraising relates to the charitable or philanthropic purpose related to the custodian's function;
- That implied consent may only be inferred where the custodian has provided, or has made available, notice to the individual at the time an individual receives health care, informing that individual of the custodian's intention to use or disclose the information for fundraising purposes, along with the information on how the individual can easily opt out in your notices, signs or brochures;
- That the individual had not opted out within 60 days from the time the notice had been provided to him or her;
- That all solicitations contain an easy opt-out from any further solicitations; and
- That no solicitations contain information about an individual's health care or state of health.

Opt-out processing is coordinated by Admitting.

Release of Information to Law Enforcement Agencies

Information becomes known to hospital staff and affiliates simply by virtue of being the patient's healthcare provider. All information that becomes known by virtue of this healthcare relationship with the patient is to be treated as personal health information. In most cases, information cannot be released unless there is **patient consent or specific legal authority** (warrant, court order, or subpoena). Where there is a warrant, court order, or subpoena, only the PHI that is ordered to be disclosed can be shared.

Situations where information can be shared are outlined below. When in doubt, and in any urgent situation, always contact your manager, Risk Manager, Chief Privacy Officer, After-hours Supervisor or the Administrator-on-Call (if after hours).
(Note: If child is a ward of Children's Aid Society (CAS), consent will be from CAS).

Location and Condition of Patient

PHIPA allows disclosure of the fact an individual is a patient at CKHA and disclosure of his/her general health status (e.g. good, fair, serious, critical or still being assessed) and his/her location in the facility, unless the patient has indicated they object to such disclosure. If the patient is not currently in the hospital, staff and affiliates can direct callers to the Health Records Department.

Significant Risk of Serious Harm to Other(s)

PHIPA also allows disclosure of PHI where the hospital has reasonable grounds to believe that disclosure is necessary to eliminate or reduce a significant risk of serious bodily harm to a person or group of persons.

Threat to Staff or Patient/Visitor Safety
If a patient or visitor is perceived to be a threat to staff or others' safety, police can be called for assistance and the name of the patient, location and situation can be given to the police to assist them as they respond. PHI is not to be part of the information released unless it is pertinent information to the threat.

Coroner Investigations
When police are investigating on behalf of a coroner, staff and affiliates are required to cooperate with those investigations in consultation with the Chief Privacy Officer and Risk Manager, After-hours Supervisor or the Administrator-on-Call (if after hours). It is important to document the name of the officer and the incident number. If the investigation includes a warrant for a copy of any part of the record, it must be referred to the Health Records Department for proper procedure for release and verification of the conditions of the warrant.

Warrant for Arrest on Discharge
When police have indicated they have a warrant to arrest the patient on discharge or they have reasonable grounds to arrest, disclosure of the date/time of the patient's discharge is permitted. Document the officer's badge number, police incident number and the disclosure on the health record. Ask the officer to provide a copy of the warrant and place it on the chart. The arrest should not take place on the patient unit/floor – contact Security for additional support.

Warrant for Health Record Information
Copies and release of any information from the health record must occur in the Health Records Department as per policy with a warrant or a signed consent. If the request for information is outside of regular business hours, contact the After-hours Supervisor or Administrator-on-Call (if after hours).

Police Presence in the Department

Requests from Police to Interview Patient
The immediate medical needs of the patient in the hospital take precedent over an officer's request to interview a patient. After the immediate medical needs of the patient are taken care of, advise the patient the police would like to speak to them and arrange for the interview to take place in a private place, if possible. The discussion will be between the police and the patient, staff or affiliates should not be a witness to the conversation.

If staff/affiliates have reason to believe a patient is under arrest in the Emergency Department, staff/affiliates should request the reason for the law enforcement agent's attendance at the hospital, as well as their badge and incident number; document this in the chart.

Requests to Photograph Patient
If the police take pictures of the patient, this is to be documented in the chart with the police badge and incident number. Staff/affiliates are not to be photographed, nor other patients.

Vicinity of Police Presence
If the patient is under arrest or correctional facility incarceration, police or correctional officer will be present and may wish to remain with the patient. If at any time the police presence interferes with the provision of care or treatment, staff and affiliates have the right to ask police to leave the treatment room.

If the patient has been brought in for assessment under the Mental Health Act, the police will remain with the patient until the hospital has taken care and control of the patient.

If the patient is deceased, the police officer may need to remain within the vicinity and/or line of sight of the patient.

The nurse is to document in the chart the reason the officer gave for needing to be present, along with badge and incident number.

Unless the officer identifies a legal reason such as the above, staff and affiliates can request that police step out of the clinical area and show them an appropriate area to wait, or make arrangements to call them back when the patient can meet with the officer. If the officer needs access to a desk or telephone, staff and affiliates should identify an area outside the clinical desk to maintain privacy and department workflow.

Requests to Interview Staff
All police requests for statements or interviews with staff and affiliates must be referred to the Risk Manager through Police Services. In an emergency where there is a risk of serious harm, the presenting or calling officer should be directed to the Risk Manager, After-hours Supervisor or Administrator-on-Call (if after hours).

If a police officer requests personal information of staff or affiliate, only their name, date of birth and work address should be provided. Personal contact information does not have to be given. Document the officer's badge and incident number and the circumstances.

Service (Delivery) of Subpoena(s)
Staff and affiliates are not required to give their home address information to police for the purpose of contacting them as future witnesses. Staff and affiliates are instructed to give their name, date of birth, work address and work extension. The police department has been requested to contact the Risk Manager to arrange a time for staff or affiliates to be served a subpoena to appear as a witness. The Risk Manager will assist the staff or affiliate with preparation for the court date. If a subpoena includes the request for the staff or affiliate to

bring copies of the record or notes to refer to, only the Health Records Department can provide that to the court.

Police Requesting to View/Seize Hospital Surveillance Tapes

In the absence of an appropriate warrant, police cannot view or seize hospital surveillance tapes without the request first being reviewed with the hospital Risk Manager and Chief Privacy Officer or Administrator-on-Call (if after hours). It is important to balance the privacy rights of all of our patients with our desire to assist the police. In an emergency situation, police should be directed to the Risk Manager and Chief Privacy Officer, After-hours Supervisor or Administrator-on-Call (if after hours). Release of video surveillance follows Freedom of Information processes, which allow 30 days to comply with requests.

Search and Seizure if a patient is under arrest

Police have a right (without a patient's consent) to examine or seize patient clothing or belongings if they are:

- acting as a representative of the Coroner,
- in possession of a valid arrest warrant or the patient is arrested, or
- under specific emergency situations.

In the above circumstances, staff and affiliates should assist police officers and make every effort to document the items which were taken by police; ask police for a receipt.

Seizure of Evidence if Patient is Under Arrest

Police have the authority to remain with an arrested patient and obtain evidence if a patient is under arrest. Without consent, a medical practitioner cannot perform a procedure solely for the purpose of obtaining evidence for police. When providing medically indicated treatment, objects or substances obtained or collected during the procedure can be provided to police.

Inquiries from Police about Unidentified Patients

When the police call or attend CKHA asking if there are any patients in the facility/Emergency Department with specific injuries (e.g. "anyone with a chemical burn") or coming from specific situations (e.g. "anyone from an accident on Highway 401"), this information cannot be disclosed without patient consent.

If staff and affiliates are comfortable speaking to the patient, they can ask whether the patient consents to the release of information. If there is no consent, police should be advised their request has been directed to the most responsible staff in attendance (e.g. your manager, Risk Manager, After-hours Supervisor or the Administrator-on-Call [if after hours]).

Protecting Confidential Information

Every effort should be made to ensure that PHI is not inadvertently disclosed to persons who are not otherwise entitled to receive such information. Subject to the reasonable limits described below, recorded and non-recorded PHI should never be discussed, displayed or left in any area where others not entitled to do so can hear or view the information.

Information Technology Security – General

CKHA is supported by a third party Information Technology company and Regional partner, TransForm Shared Service Organization (TSSO) that supports the operations of CKHA's information technology infrastructure.

The following policy topics are addressed in TSSO policies:

- Information Security Policy
- Information Management Policy
- Privacy and Security Incident Management
- Sample Network Access Request Form

CKHA Information Technology Policies:

(Refer to the following CKHA Policies located on the online Policy Database- Medworxx)

- COM-1-020: Appropriate Use of Email
- COM-1-014: Wireless and Portable Devices Security
- COM-1-016: Corporate Use of Social Media
- PEO-1-072: Personal Use of Social Media
- COM-1-013: Authorized Use of Computer Equipment

Electronic Information

CKHA staff and affiliates are responsible for protecting PHI stored on computerized media. CKHA retains the exclusive rights to all computer assets and information that reside on: CKHA's mainframe processing systems, CKHA's systems residing on local area networks, enterprise networks and/or stand-alone microcomputers, and CKHA's voicemail system.

Users should not leave a workstation unattended while a file/document containing PHI is displayed or open, with the exception of computers in a restricted area where no unauthorized persons can view the information. To secure PHI, users must password-protect encrypted files, use screen savers and log-off when leaving a workstation unattended. Staff and affiliates must not access applications containing PHI using login credentials that are not their own. The user should first log-out and let the second user log-on. Passwords are never to be shared. Contact TSSO Service Desk, for instructions.

Access to computerized patient information will be granted in accordance with CKHA's policies and procedures and access levels established. This access will be confined to information required for performance of duties.

E-mail and Fax Transmissions

When sending confidential information (both inside and outside CKHA), e-mail and fax cover sheets must contain the following confidentiality statements:

Fax Transmissions CONFIDENTIALITY CAUTION:

- The enclosed information is confidential and privileged only to the individual to whom it is addressed and should not be distributed, copied, or disclosed to any unauthorized

persons. If you have received this communication in error, please notify the sender immediately by telephone and mail the original message to us at our cost.

Ensure all CKHA fax machines are located in a private and secure location that is only accessible to authorized personnel. Whenever possible, confidential information should be delivered through telephone, courier, inter-office mail or Canada Post. PHI is only to be faxed when it is absolutely necessary to do so and must include a Fax Transmission Form to Disclose Personal Health Information.

E-mail Transmissions CONFIDENTIALITY STATEMENT:

- This email transmission may contain confidential or legally privileged information that is intended only for the individual or entity named in the email address. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution, or reliance upon the contents of this email is strictly prohibited. If you are not the intended recipient, please notify the sender immediately by return email and delete this message and any attachments from your system.

When sending/transmitting confidential information, all CKHA staff/affiliates are responsible for:

- Selecting the most secure method of sending physical (hard copy) and electronic confidential information.
- Complying with corporate faxing guidelines to reduce risk of faxing to incorrect recipients.
- De-identifying, encrypting or using secure file transfer to send confidential information to a recipient outside the organization's secure network. In an e-mail that is being sent/forwarded/copied externally, the patient's PHI should never appear within the e-mail. Instead, senders will use only the health record number and the patient's initials.
- Not using e-mail to send confidential information to a recipient outside CKHA's secure e-mail system or ONE-Mail system.
- Designating e-mails sent within the secure e-mail system, which contain confidential information, as confidential by typing "confidential" in the subject line of the e-mail and applying the confidential status under "send options".
- All e-mail correspondence at CKHA that involves identifiable patient care or sensitive information may be sent only using an address on the CKHA or ONE-Mail address book.

Transportation/Mail

If patient information is being physically transported/mailed within the building, it must be done in a secure manner, which ensures that PHI is not visible and that no information may be dropped or lost. When PHI is being couriered between sites, it must be placed in blue bags to ensure confidentiality at all times.

It is CKHA's policy that no patient's original health record may be taken from CKHA by any hospital staff/affiliate or independent health care practitioner, except as required by subpoena, court order or statute. There are no exceptions to this policy. For cases where an urgent and

immediate transfer is required, information from the health record is to be faxed ahead of the patient's transfer or copied and sent with transport team. The original chart is not to leave the building.

If a Coroner or officer acting under the authority of the Coroner, a copy MUST be made or the chart scanned in Health Records prior to leaving the building.

Telephone and Cellular Telephones
Given that the cellular telephone network may not be secure, such that there is the possibility of conversations being intercepted, a regular telephone should be used whenever possible for the discussion of PHI. If discussing PHI, the telephone must not be used when others not entitled to hear that information are present.

Storage
PHI that is kept outside of the Health Records Department is subject to the same policies as if it was stored in the Health Records Department. Health records must always be stored in the Department unless the health record is still active and remains in use for visit. Health records must be stored in a secure area when not in use. The health record should not be left in unattended areas accessible to unauthorized individuals.

Photocopying
If any part of the legal health record or any PHI, regardless of format or storage location is photocopied in Health Records or on the unit, the same policies on confidentiality and privacy apply to the copy as if it was the original. In addition, the following information must be documented in the record: name of individual or facility to receive information; specific reports/notes photocopied; date photocopied; and name of individual responsible for the photocopying.

- If the patient is still an inpatient on a patient unit and information is requested to be photocopied for continued medical care, unit clerks will make the photocopies and send/fax the copies upon validation of proper consent.
- If the photocopies of the health record are for use outside CKHA, Health Records staff will do the photocopying except for patient transfers.
- Finance staff may request copies from the Health Records Department to allow processing of health care insurance billing for requests from non-resident patients who have given their consent.

Audits
Security audits will be performed regularly and upon request to determine whether there has been a violation of privacy through inappropriate access to electronic patient information. It is the responsibility of all users of CKHA computer information systems to use electronic systems ethically, legally, and in a manner consistent with the Mission, Vision and Values of CKHA.

All individuals who have access to PHI are responsible for ensuring that the information is kept confidential and for protecting patients' privacy according to the guidelines outlined in this policy. Disciplinary action will be implemented if individuals access PHI inappropriately.

Regular Audits
Regular audits will be conducted and reviewed by the Privacy Team (Chief Privacy Officer, Manager of Health Records and Strategy & Privacy Assistant) and on a randomly selected group of patients. This includes random accounts, random search users, random staff and affiliates who are patients in the organization and others as determined by the Privacy Team (and/or delegates).

Ad Hoc Audits
Audits can be requested by a member of the Executive or Senior Leadership Team, Quality/Risk Management, Human Resource Department, Physician Leader or Patient Representative on behalf of a patient (including staff and affiliates who are patients), who believes patient information may have been inappropriately accessed. Please contact the Chief Privacy Officer or a member of the Privacy Team if an ad hoc report is required.

Audit requests and results are treated confidentially by all staff involved. The request must include the patient name, a unique identifier (MRN #/Acct # if known), birth date, approximate time period of access in question or specific visit, and a brief explanation of the suspected violation including the name of the user suspected of the breach.

Audits are for internal purposes only. Audits may also be performed in conjunction with regional systems and auditing requirements of regionally shared systems. This includes audit processes outlined in all regional data sharing agreements. They will be conducted in a confidential manner.

Disposal of PHI
CKHA is responsible for ensuring that all confidential information is securely maintained as required by the PHIPA. Destruction of confidential information must be done in a manner which protects and safeguards the contents of this information and the interests of patients, employees, affiliates and agents.

CKHA uses the services of contracted third party affiliates for all of the organizations confidential waste management.

All information that is deemed to be confidential in nature and requires shredding will be placed in consoles marked "Shred-it" that are strategically located in departments throughout the organization. The designated shredding company will be on site weekly to shred any confidential information from the consoles and provide a receipt of shredding to Housekeeping. Receipts are maintained by Housekeeping.

When confidential consoles become too full and require emptying prior to pick up, Housekeeping will be notified. The Housekeeping Department will arrange to have the console emptied and stored in a locked secured area until the shredding company makes its weekly run.

It is the responsibility of each department to properly identify confidential information and ensure that it is placed in the appropriate container for shredding. Departments need to be aware of appropriate legislation with respect to record retention and destruction to ensure that information being shredded meets appropriate timelines.

Confidential Information Requiring Shredding

- Health Care Information – Patient Care Record, Diagnostic Imaging CD's, Patient-Related Administrative Information such as Schedules, Registers, Census Reports
- Quality Assurance Information – Incident Reports, Minutes, Q.A. Reports, Evaluations, Letters
- Business Information – Financial data such as pay roll - Personnel Records, Appraisals
- Employee Health Records
- Any Other Information Deemed Confidential - This includes all personal identifiers

Non-Paper Data Storage Items

- Items include: VHS tapes, films (reel) tapes, paging system tapes, memory cards/sticks, digital camera disks, CD Roms, DVD's, cassette tapes, dictation tapes, photographic images/negatives, impact printer ribbons or cartridges. Clearly label items as "Confidential".
- Items that cannot be placed in "Shred-it" will be transported by Housekeeping to a designated locked storage room for pick up by the applicable service provider.
- After every service call a Certificate of Destruction is given to Housekeeping management.
- All confidential waste will be stored in a locked, secure area.

PROCEDURE

Identifying and Managing a Privacy Breach

This section provides information and direction to Supervisors/Managers when they identify or are made aware of a potential or actual privacy breach.

PHIPA requires the organization, as a HIC, to take reasonable measures to protect PHI against unauthorized access, use or disclosure. Rapid action in response to an actual or potential privacy breach is part of a Supervisor's/Manager's responsibility for protecting patient's PHI.

Identifying a Privacy Breach

A privacy breach occurs whenever:

a) PHI is lost or stolen, or
b) PHI is accessed, disclosed, copied or modified without authority, or
c) Disposal of PHI has occurred in an insecure manner, or

d) In any other situation where any employee, physician, volunteer or affiliate has contravened, or is about to contravene the PHIPA.

A privacy breach can occur via verbal or written communication, by phone, e-mail, fax, electronic means or any other medium. A privacy breach can be actual, potential or suspected.

1. Privacy Breach – Actual

Includes, but is not limited to accessing patient PHI when it is not required to provide care to a patient or in the performance of work duties, for example:

a) directly accessing one's own electronic health record without following the process set by Health Records
b) accessing the health record of an employee, family member, friend, or any other person for whom you do not have a requirement to view information in order to provide care or perform work duties
c) accessing any patient information (e.g. address, date of birth, next of kin, etc.) of an employee, family member, friend, or any other person for whom you do not have a requirement to view the information in order to provide care or perform work duties

Disclosing patient information

a) without the appropriate consent, e.g. to a lawyer or insurance company
b) to another employee or affiliate who does not require access to the information to perform his or her job functions
c) by discussing within hearing range of other people who do not require access to the information to perform his or her job functions
d) by emailing, faxing or mailing to the wrong recipient
e) by posting to a social networking site, e.g. blog

Leaving patient information in unattended or unsecured locations where it may be accessed by unauthorized persons, for example:

a) leaving patient reports, charts, or worksheets that contain patient-identifying information in a public area
b) leaving access to electronic patient information unattended on an open log-in
c) storing electronic patient-identifying information on portable information devices or insecure drives, e.g. hard drives that have not been encrypted
d) theft of electronic devices that contain patient-identifying information
e) loss of hard copy records or other patient-identifying information

2. Privacy Breach – Potential

Occurs when an individual's PHI is at a high risk of being accessed, used or disclosed inappropriately. A potential privacy breach includes, but is not limited to situations in which:

a) A patient alerts the Supervisor/Manager or the Privacy Officer that a staff member or affiliated individual may have accessed information about him or her inappropriately
b) A patient requests additional security measures for his or her PHI e.g. requests for anonymity and requests for patient information to be lock boxed. Contact Health Records and/or the Chief Privacy Officer for any request from a patient to restrict access to information.

3. Privacy Breach – Suspected

Occurs when there has been an allegation of a privacy breach, but the allegations have not yet been substantiated or refuted by investigation.

Steps in the Management of a Privacy Breach

The Office of the Information and Privacy Commissioner of Ontario (IPC) has directed HIC's, such as hospitals, to take the following steps when they identify or are made aware of a potential or actual privacy breach. Some steps have been added or amended to support internal systems and structures e.g. RL6.

Note: Depending on the type of privacy issues, these steps may not all occur, may not be sequential and could occur concurrently.

1. **Contain the breach or secure the PHI to reduce the likelihood of a breach**
   This step may include engaging other departments, Supervisors and Managers.
2. **Enter the breach and corresponding information into the RL6 System**
   This step triggers a notification to the Chief Privacy Officer and helps ensure all potential, suspected or actual breaches are recorded.
3. **Investigate the potential/actual breach and evaluate the risks associated with the breach**
   This step may include:
   a) Evaluating risks associated with a privacy breach.
   b) Creation of a privacy incident response team.
   c) Outcomes for employees, physicians, volunteers and affiliates.
4. **Notification of those affected by the breach**
   This step may include:
   a) Notifying patients affected by the privacy breach.
   b) Notifying the IPC
5. **Managing the risk of future breaches**
   This step may include reducing the risk of future breaches.

Some actions are common to most privacy breach scenarios and may be referred to in each scenario. Depending on the type of breach, these actions may occur at varying steps in the investigation.

Severity Categories for Privacy Breaches

Notify Chief Privacy Officer and Risk Management for Categories 3 to 5; Notify Corporate Communications for Category 5

Category	Description
1	• Isolated incident- non-identifiable health information • Inadvertent breach using Electronic Patient Record (viewing of a previous screen due to incomplete system log-out by user) • Faxed information to wrong recipient – non-identifying, non-confidential single incident
2	• Faxed report to wrong recipient – PHI of a single patient
3	• Faxed report to wrong recipient – PHI of multiple patients • Unintentional breach or release of sensitive PHI of a single patient or PHI of multiple patients due to theft or loss of files, computer or portable information storage or computer device
4	• Intentional unauthorized access of PHI of a single patient or multiple patients without further release to other parties
5	• Deliberate release of patient, employee, affiliate or organizational confidential information to the media or other parties • Deliberate use or release of patient, employee, affiliate, organizational confidential information for personal gain or malice • Potential for fine or penalty under the PHIPA and its regulations

Criteria for Engaging Other Departments

Depending on the type and severity of the breach, a Supervisor/Manager must contact the Chief Privacy Officer as soon as reasonably possible for breaches in the "Categories of Severity for Privacy Breaches" of a rating of 2-5

1. The Supervisor/Manager must notify the Administrator-on-Call if:
   a) The breach carries a high risk, where the PHI must be immediately secured or the risk of re-occurrence is high, and/or
   b) The Supervisor/Manager is made aware of the breach during off-duty hours.
2. If the Administrator-on-Call is contacted, the Chief Privacy Officer must also be contacted at the earliest reasonable time. The Chief Privacy Officer will advise, coach and mentor on the need to notify or engage other Management, based on the criteria for each Department:
   a) Risk Management
   b) Communications
   c) Human Resources
   d) Information Technology
   e) Medical Affairs
   f) Security
   g) Other personnel as necessary, depending on the breach.

Criteria for Notifying Risk Management of a Privacy Breach:

1. A patient or a representative of the patient indicates the intent to sue CKHA or contact a lawyer, or
2. The information is highly sensitive and may not only identify the name of the patient, e.g. a high profile patient, but also nature of the information, or
3. The quantity of information breached is considerable, e.g. large amount of information pertaining to a single patient, or a large number of patients due to theft/loss, or
4. External parties are investigating the breach, e.g. law enforcement agency, a professional College under the Regulated Health Professions Act (RHPA), the media, etc., or
5. Disciplinary action by CKHA is a probable outcome, or
6. Media interest is likely, e.g. the breach is a newsworthy story (see Media Requests), or
7. A patient or staff/affiliate involved in the investigation indicates that he or she will contact the media, or
8. An MP, MPP or a LHIN is involved or has been notified of the breach.

Criteria for Notifying Corporate Communications of a Privacy Breach:

Notify Corporate Communications regarding a privacy-related incident when:

1. The incident is a level 5, or
2. A law enforcement agency is a part of the investigation, or
3. Disciplinary action by CKHA is a probable outcome, or
4. A person involved in the investigation indicates intent to contact the media; or
5. A reporter from the media might be interested in covering the story (e.g. newsworthy)

Criteria for Engaging Human Resources in the Management of a Privacy Breach:

Whenever an employee or affiliate is under the investigation and/or is alleged to have breached privacy.

Criteria for Engaging Medical Affairs in the Management of a Privacy Breach:

1. Whenever a Professional Staff member (physician, dentist), medical student or privately hired physician secretary is under investigation and/or is required to speak to a Manager/Supervisor regarding a breach, or
2. In the case of an employed physician secretary and if discipline is a probable outcome discuss with a Medical Affairs representative if Medical Affairs presence is warranted during the interview.

Criteria for Engaging Ethics and Research Committee:

1. Whenever the information breached was collected and/or used for research purposes.
2. Whenever an employee or affiliate involved in the breach was engaged in research activities.

Evaluating the Risks Associated with a Privacy Breach

To determine which steps are immediately necessary, it is essential to first assess the risks associated with the breach.

Consider the following factors (*Note: The risk escalates when multiple factors are involved)*:

1. What kind of PHI is involved? Risk escalates if sensitive information is involved. Although all PHI is confidential and may be considered sensitive to the patient, information that may be considered more sensitive includes, but is not limited to information pertaining to:
   a) Mental health
   b) Sexual assault
   c) Communicable diseases, e.g. HIV
2. Has information been used for personal reasons or disclosed to others either in the organization or outside the organization? Disclosure increases risk. Disclosure to a non-health information custodian, e.g. to a private home, business, or to an individual who is not a health care provider, carries even greater risk.
3. What is the cause of the breach? Is there a risk of an ongoing breach or further exposure?
4. Approximately how many patients are affected by the breach?
5. Are they patients of CKHA? For example, if an employee or affiliated individual has accessed information inappropriately on patients who were not at CKHA at the time of the access, the Privacy Officer must notify and work with the other organization to ensure compliance with our requirements under PHIPA.
6. Is the information encrypted or otherwise not easily exploited? The IPC has stated: "When encryption is implemented properly, it renders PHI safe from disclosure."
7. Can the information be used for fraudulent or otherwise harmful purposes?
8. What harm might CKHA suffer as a result of the breach, e.g. loss of trust, loss of business, loss of assets or other financial exposure?

Creation of a Privacy Incident Response Team

Depending on the risks associated with the breach, any of the parties involved in the breach may request that all parties meet to:

1. Facilitate the investigation
2. Identify and manage risks associated with the breach, including risk related to:
   a) reputation of the organization
   b) patient trust
   c) media
   d) legal
3. Collaborate on determining next steps/actions

Outcomes for Staff and Affiliates

On completion of the investigation, the Manager and/or Supervisor, in collaboration with the Chief Privacy Officer and Human Resources or Medical Affairs (depending on which type of individual is involved) determines the most appropriate outcome for staff or affiliate. In rare circumstances, legal may also be involved in this step of the process. Possible outcomes include one or more of the following:

   a) education

b) verbal warning
c) written suspension
d) suspension
e) termination of relationship/placement

The following are examples of factors that may be considered when determining the outcome. Consult your Human Resource or Medical Affairs representative if disciplinary action is a probable outcome.

1. Severity of the breach
2. Level of risk to the patient, staff, affiliate and/or CKHA
3. History of work performance or any prior discipline. Note the time lapse between disciplinary infractions and the staff or affiliate's tendency to respond favorably to discipline subject to applicable collective agreement provisions
4. Years of service
5. Staff or affiliate's response to and cooperation with the investigation
6. Whether staff or affiliate understand the concept of privacy and confidentiality and understands the seriousness, impact and possible consequences of the breach
7. Provision of professional College standard

Notifying Patients Affected by a Privacy Breach

The Chief Privacy Officer will advise Managers/Supervisors about CKHA's legal requirement to notify:

1. A patient or incapable patient's SDM, if the patient's information has been lost, stolen or accessed without authority,
2. Another organization, if the actual or potential breach involves an employee from another organization, or a patient's PHI is from another organization,
3. Other groups, based on legal, professional or contractual obligations,
4. Police, if the breach may reasonably be considered to result in significant harm to the patient or a third party,
5. The Information and Privacy Commissioner of Ontario

How to Notify a Patient/SDM Affected by a Potential or Actual Privacy Breach

Notification of a patient/SDM may be done verbally or in writing depending on the following factors:

1. The availability of the patient/SDM - if the patient is in hospital at the time of notification, or coming into hospital in the near future, it may be appropriate for the physician, Supervisor/Manager or the most appropriate Regulated Health Professional who has a clinical relationship with the patient, e.g. Social worker, Psychologist to notify the patient in person, and
2. The relationship with the patient – if a physician, Supervisor/Manager, or a Regulated Health Professional has an established clinical relationship with the patient, it may be appropriate to notify the patient in person.

The Chief Privacy Officer has collaborated with the IPC to develop notification letters and outlines for verbal notification and will act as a resource in the notification. The aim of notification is to be open and honest and address any questions or concerns the patient may have. Notifications should include the following information:

1. The fact that a privacy breach occurred and a description of the breach
2. The elements of personal information involved, i.e. exactly what information is potentially accessible to others as a result of the breach
3. The steps the organization has taken to mitigate the harm and reduce the risk of re-occurrence,
4. Advice to affected patients on what they can do to further mitigate the risk of harm, i.e. to consult the Ministry of Health and Long Term Care for an audit of the use of their health card, or to obtain a new health card.

When responding to a patient's questions following notification of a breach, either in person, or when a patient calls in response to a notification letter, the information that may be provided includes:

1. The name of the staff member or affiliate if requested by the patient
2. The department/area where the staff member or affiliate is/was employed or affiliated
3. That the staff member or affiliate received disciplinary action however details of the disciplinary action are not disclosed. Assure patients that CKHA takes these matters very seriously and the issue has been addressed with the staff member or affiliate
4. Details about the patient's information that was accessed (e.g. in an ADT breach) or potentially available to others (e.g. laptop theft) as part of the breach. Details about how the breach occurred may be provided. For example, that the staff member or affiliate searched the ADT system by patient name and would have had access to demographic information and visit history, that the staff member or affiliate opened the patient's ADT record, and what information could have been accessible, e.g. demographic information, laboratory and diagnostic imaging results and notes, Clinic notes, discharge summaries, that were dictated using the organization's central dictation system and posted to the ADT system.
5. Managers/Supervisors can forward detail inquiries about access to the ADT systems to the Chief Privacy Officer.

Patients often ask if they are at risk for identity theft as a result of the breach, and whether their social insurance number (SIN) was accessed. Inform the patient that their SIN is not routinely collected. The only time SIN is collected is for the first visit of a workplace injury and usually a WSIB Claim # for all subsequent visits is required.

Notifying the Information and Privacy Commissioner of Ontario (IPC)

The Chief Privacy Officer will notify the IPC as needed by:

1. Preparing a de-identified summary of the issue. When applicable, the summary will indicate that the organization took disciplinary action against the staff member or

affiliate, without indicating the specific action. If the IPC is made aware of the specific disciplinary action, it would be required to disclose this to the patient, if requested.
2. De-identifying any written communication with the patient.
3. Staff and affiliates must participate annually in the hospital's Privacy and Confidentiality e-learning education program.
4. Confirmation of the successful completion of the education program and the signed confidentiality agreement will be kept on the individual's file in:
   a) Sending these document to the IPC
   b) Liaising with the IPC for any follow up

Reducing the Risk of Future Breaches

Depending on the severity of the breach, any of the parties involved may initiate a review of the breach with an aim to reduce the risk of re-occurrence. If applicable, the group may recommend steps to reduce the risk of re-occurrence. These steps may include:

1. Changes to processes, polices or procedures
2. Additional education and training for users related to PHI and their accountabilities to protect patients' privacy rights
3. Reviewing and enhancing the program or department's security measures to protect PHI

Conducting this type of review will result in continuous improvement to the PHI environment in the area and strengthen the privacy culture within the organization.

DEFINITIONS

Affiliate: Individuals who are not employed by Chatham Kent Health Alliance (CKHA) but perform specific tasks at or for CKHA, including appointed professionals e.g. physicians/dentists, students, volunteers, researchers, contractors, or contractor employees who may be members of a third-party contract or under direct contract to CKHA and individuals working at CKHA, but funded through an external source.

Appropriate Access: Access to health information is based on "the need to know" and circle of care guidelines (see IPC Circle of Care) to provide current and direct patient care or to perform one's duties and in alignment with established security level policies for systems. Personal health information may be used only under the following conditions:

- **For Direct patient care** – the health care provider may access health information when they are involved in the direct and current care of the patient. Access to health information is limited to that information which is required to fulfill this purpose.
- **Research** – personal health information may be used for this purpose once the Study is approved by the Ethics and Research Committee and the designate CKHA representative; however, all patient identification must be removed prior to presentation or publication of any results.
- **Education** – personal health information may be used in education rounds for teaching purposes providing no identifiable information is disclosed. Identifiable patient information will be used only where necessary for clinical education purposes.

- **Quality Assurance** – personal health information will be used to ensure that the quality of care and services provided to patients is of the highest quality.
- **Patient's Personal Use** – a patient generally has a right to access his or her health information through the organizations release of information office in the Health Records Department.
- **As Required by Law** – personal health information may be accessed and/or released as required by law.
- **For Performance of One's Duties** – personal health information may be accessed as required by individuals to perform their job duties.
- **Other uses** – when used for purposes other than those stated here, personal information may be accessed only by persons designated by the individual or the individual's legally authorized representative through a properly executed consent through the Health Records Department. Other uses can also include authorized access by Quality/Risk or Human Resources or designated management staff to ensure compliance with this policy and legislation.

Circle of Care: Is not defined in PHIPA, but refers to those in the health care team who are actually involved in the care or treatment of a particular patient**.**

Confidentiality: Means the moral, ethical, professional and employment obligation to protect the information entrusted to individuals.

Disclose/Disclosure: The Personal Health Information Protection Act (PHIPA) refers to release or making available of personal health information to another person, (other than patients or their substitute decision-makers) organization or health information custodian. It does not mean the use of the information.

Express/Informed Consent: Consent is informed if the patient received information about:

- Why the information is being requested
- The expected benefits of the release
- The implications of the release (e.g. used against him/her)
- Likely consequences of not releasing (e.g. warrant could be used)
- Person received responses to his/her inquiries

Express consent can be verbal or written. If verbal, this must be documented in the chart.

Health Information Custodian (HIC): Defined by PHIPA and for the purposes of Chatham Kent Health Alliance means any person or organization who controls other people's personal health information as part of their role as a hospital under the Public Hospitals Act, a private hospital under the Private Hospitals Act, a psychiatric facility under the Mental Health Act or an independent health facility under the Independent Health Facilities Act.

Health Record: Means the capture of personal health information (PHI) acquired or maintained within the organization, regardless of the medium (verbal, written, visual, electronic,

microfilm/microfiche), and is the property of the Health Information Custodian. The PHI contained in the Health Record is owned by the patient and is considered confidential. It consists of all PHI accumulated in the following:

- Hard-copy health records or charts housed in Health Records or designated alternative locations (e.g. Radiology)
- Electronic Patient Record (EPR)
- Diagnostic images and reports, lab specimens and reports, photographs, videos, sound recordings, microfilm or microfiche
- Departmental databases that maintain PHI

Implied Consent: Permits you to conclude from surrounding circumstances that a patient would reasonably agree to the collection, use or disclosure of the patient's PHI.

Inappropriate Access: Inappropriate access occurs when an individual accesses PHI when they are not providing care for the patient and none of the appropriate access circumstances apply. Inappropriate includes, but is not limited to, accessing patient information for personal interest including one's own personal health information or that of a family member or colleague without submitting a request through the Health Records department.

Law Enforcement Agency: For the purpose of this policy includes Ontario Provincial Police (OPP), Royal Canadian Mounted Police (RCMP), Canadian Military Services, and municipal Police Services (CKPS).

Most Responsible Practitioner (MRP): For the purpose of this policy the MRP may be a physician/dentist/midwife or other Regulated Health Professional who would have knowledge of the patient and the potential risks related to disclosure of the PHI.

Patient Identifying Information: Means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. Patients do not have to be named for information to be considered identifying. Information is identifying if an individual can be recognized using it, or when it can be combined with other information to identify an individual. Anonymous or de-identified personal health information cannot be linked back to the individual either directly or indirectly.

Patient/Substitute Decision Maker: Or **Patient/SDM** refers to the patient (if the patient is capable of making a decision with respect to the collection, use and disclosure of his or her personal health information) or the patient's Substitute Decision Maker (SDM) (if the patient is incapable with respect to the collection, use and disclosure of his or her personal health information).

Personal Health Information (PHI): Defined by PHIPA as oral or recorded identifying information about someone that relates to:

- an individual's physical or mental health, or family health history, or

- health care an individual receives, including who provided the health care, or
- a plan of service for an individual under the Long-Term Care Act, or
- an individual's eligibility for health care payments or the payments made for an individual's health care, or
- an individual's donation of any body part or bodily substance or anything derived from testing or examining a donated body part or bodily substance

Personal Health Information also includes:

- an individual's health number
- anything that identifies an individual's Substitute Decision Maker
- anything that identifies an individual and that is contained in a personal health record

Personal health information does not include records maintained for human resources purposes.

Personal Information: Information about an identifiable individual, but does not include the name, title or business address or business telephone number of a staff member or affiliate of an organization.

Quality Assurance: Refers to activities that involve the use of personal health information to improve or maintain the quality of care or to improve or maintain the quality of any related programs or services of Chatham-Kent Health Alliance.

Record: Means an information record in any form or media, including written, printed, photographic or electronic format.

Subpoena: An Order of a Court (writ) that requires a **person** to be present at a certain time and place to testify and/or produce documents in the control of the witness or suffer a penalty. A subpoena is used to obtain testimony from a witness at both depositions (testimony under oath taken outside of court) and at trial.

Substitute Decision Maker (SDM): Is defined as a person who is:

- at least 16 years of age, unless he or she is the incapable patient's parent
- capable with respect to the treatment
- not prohibited by court order or separation agreement from having access to the incapable patient or giving or refusing consent on the incapable patient's behalf
- available, and willing to assume the responsibility of giving or refusing consent

In descending order or priority, an incapable patient's SDM may be:

- the incapable patient's "**guardian of the person**", if the guardian has authority to give or refuse consent to the treatment
- the incapable patient's "**attorney for personal care**", if the power of attorney confers authority to give or refuse consent to treatment
- the incapable patient's "**representative**" appointed by the Consent and Capacity Board, if the representative has authority to give or refuse consent to the treatment
- the incapable patient's **spouse** or **partner**

- a **child or parent (custodial)** of the incapable patient, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent to the treatment in the place of the parent
- a **parent (who has only a right of access)** of the incapable patient
- a **brother or sister** of the incapable patient
- **any other relative** of the incapable patient.

Third Party Information: In relation to a patient's health record, means personal information about an identifiable individual or individuals, other than the patient.

Warrant: An official document, signed by a judge or other person in authority, commanding police to perform specified acts.

LINKS

Legislation

Personal Health Information Protection Act
Personal Information Protection and Electronic Documents Act
IPC Circle of Care
Public Hospitals Act
Private Hospitals Act
Mental Health Act
Independent Health Facilities Act
CKHA Patient and Family Guide

Policies/Procedures/Guidelines

COM-1-004: Capacity Assessment Guidelines for Inpatients
PTS-3-107: Mandatory Reporting of Gunshot Wounds Act
PTS-2-017: Identification, Documentation and Reporting of Child Abuse and Neglect
COM-1-014: Wireless and Portable Devices Security
COM-1-016: Corporate Use of Social Media
PEO-1-072: Personal Use of Social Media
ADM-1-013: Records Retention
ADM-2-039: Media Request for Patient Condition
COM-2-001: Access to Information under FIPPA
COM-1-020: Appropriate Use of Email
COM-1-013: Authorized Use of Computer Equipment
HTI-1-010: PRIVACY: Guidelines for Disclosure of Patient Information
COM-2-003: Preservation of Forensic Evidence
COM-1-005: Specimens for Blood Alcohol – Police Requests Only
PTC-2-020: Illicit Drugs: Handling of Suspected

Forms

Confidentiality Statement

Consent to Disclose Personal Health Information
Lock-Box Request Form
Ethics and Research Committee Application Form
Fax Transmission Form to Disclose Personal Health Information

REFERENCES

Bluewater Health. Bluewater Health Privacy of Personal Health Information. (2003, December). Retrieved from http://bwh.bluelemonmedia.com/uploads/AboutUs/pdfs/privacypolicy.pdf

Coroners Act, R.S.O. 1990, c. C.37. (2018, May 7). Retrieved from https://www.ontario.ca/laws/statute/90c37

Criminal Code, R.S.C. 1985, c. C.46. (2018, December 3). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-46/

Erie Shore Health Care. ESHC Privacy Policy. (2014, December 14). Retrieved from http://www.erieshoreshealthcare.ca/images/document_render.pdf

Health Care Consent Act, S.O. 1996, c. 2, Sched. A. (2018, May 8). Retrieved from https://www.ontario.ca/laws/statute/96h02

Hotel-Dieu Grace Healthcare. HDGH Privacy Policy (2009, June). Retrieved from https://www.hdgh.org/uploads/PatientsandVisitorsMain/HDGH%20Privacy%20Policy%20November%202016.pdf

London Health Sciences Centre. LHSC Privacy Policy. (2018). Retrieved from https://www.lhsc.on.ca/privacy/privacy-policy

Mental Health Act, R.S.O. 1990, c.M.7. (2015, December 21). Retrieved from https://www.ontario.ca/laws/statute/90m07

Nursing Act, 1991, S.O. 1991, c. 32. (2017, December 30). Retrieved from https://www.ontario.ca/laws/statute/91n32

Personal Health Information Protection Act 2004, S.O. 2004. c. 3, Sched. A. (2018, May 7). Retrieved from https://www.ontario.ca/laws/statute/04p03

PIPEDA fair information principles. (2018, January). Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

Public Hospitals Act, R.S.O. 1990, c. P. 40. (2017, December 12). Retrieved from https://www.ontario.ca/laws/statute/90p40

Windsor Regional Hospital. WRU Privacy Policy. (2016, September 1). Retrieved from https://www.wrh.on.ca/uploads/Common/Document/WRH%20Privacy%20Policy.pdf

Appendix A – Fee Schedule

Fees for Personal Health Information Request	Amount/Rate
Application Fee (Non-refundable) (Patient/Third Party/Substitute Decision Maker)	$33.90 (includes HST & first 20 pages) 50% additional surcharge applies to all requests required within 72 hours
Additional photocopies and computer printouts	$0.25 per page + HST
Imaging provided on CD-ROMS (excluding continuing care)	$10.00 for each CD-ROM
Off-Site Retrieval Fee (additional)	$20.00
Chart Viewing	$20.00 for each 30 minute period Copy charge additional (see copy charges above)
Circle/Continuing Care (requests faxed to office)	No Charge
Proof of Birth Letter	Free up to first birthday (regular fee applies after 1 year)

H.S.T. applies to all fees above
$30.00 non-refundable administrative fee for cancelled requests

Last Update: July 2016