

Huron Perth Healthcare Alliance	
HR Policies and Procedures	Original Issue Date: October 01, 2001
Confidentiality	Review/Effective Date: July 31, 2019
Approved By: Director, Human Resources	Next Review Date: July 31, 2021

This is a CONTROLLED document for internal use only.

Any documents appearing in paper form are not controlled and should be checked against the document (titled as above) on the file server prior to use.

Preamble:

All Huron Perth Healthcare Alliance employees or affiliates (see **Definition**) may have access to confidential information by virtue of their employment or affiliation with the Alliance.

The Alliance recognizes the individual's right to privacy in relation to personal or personal health information (PHI) and its obligation to ensure the privacy and confidentiality of all personal or personal health information under its control, regardless of format (e.g. written, electronic or verbal).

Health care workers are held to the highest standard of ensuring the privacy and confidentiality of our patients' personal health information.

It is unethical and unlawful for any Alliance employee or affiliate to access, use, discuss or disclose the personal or personal health information of any patient, Alliance staff or affiliate to anyone except through the course of performing their express role.

Breaches of privacy and confidentiality may result in serious consequences for an Alliance employee or affiliate, including loss of trust or reputation, loss of access to information systems, embarrassment, discipline up to and including termination of employment or affiliation, reporting to and discipline by professional associations/colleges, legal action and fines up to \$100,000 for individuals.

Policy:

All reasonable measures must be taken to ensure that sensitive information is collected, accessed, used and disclosed only in circumstances necessary and authorized for patient care, research or education or as necessary in the conduct of the business of the Huron Perth Healthcare Alliance facilities and/or programs.

Circumstances appropriate for access to and disclosure of sensitive information:

i) regarding personal information (patient, staff, visitor) include:

- When necessary for the care of the patient
- For continuity of care
- When authorized by the person the information is about
- For research or education authorized by an appropriate body
- For purposes of quality improvement projects or within the Quality of Care Committee process
- If authorized by law (e.g. court order or subpoena)
- For an authorized person to contact next of kin and/or Substitute Decision Maker

ii) regarding corporate information

- If necessary for the purposes of conducting business
- If authorized by law (e.g. court order, subpoena, statutory authority)

HPHA is part of the broader healthcare system and employees or affiliates may have access to PHI from another organization, such as Alexandra Marine and General Hospital (AMGH) in Goderich through the shared Meditech system, Clinical Connect and PACs. Accessing information from another provider should only be done in the course of providing direct care to the patient. Alliance employees and affiliates will protect an individual's privacy and confidentiality by adhering to the following:

- **DO** follow the '**need to know**' rule by accessing only the information that is required as part of employee or affiliate's role in the Alliance, e.g. health care providers access patient information for those patients to whom they are assigned or for whom they are providing care.
- **DO** access only the records that are relevant to the care provided or the patient's current condition when the patient or others are not able to provide the information required
- **DO** respect patient information of a sensitive nature including nature and cause of illness, treatment options under consideration, reactions of the patients, financial status, conditions of the patient's home or domestic situation
- **DO** make every effort to discuss confidential information out of the range of others that do not need to know, e.g. do not discuss confidential information in public areas in the hospital such as corridors, elevators, cafeteria
- **DO** discuss sensitive information with patients in a low voice or an area where others cannot overhear, if possible
- **DO** wear an identification badge at all times and ensure the identifying information is visible
- **DO** check the identification badge or question anyone that does not appear to have authority to access, use or disclose personal or personal health information
- **DO** ensure that, when authorization has been granted for the removal of the original records from the premises (e.g. taking chart to court) or when copies of confidential information are provided for removal from the hospital (e.g. for the physician to take to their office), they are secured against loss, theft or unauthorized access
- **DO** log off a computer when it is unattended so that others cannot access confidential information
- **DO** place all paper records containing personal health or other confidential information in the locked "Shred-it" (Cintas-Documents Security Confidential Paper Collection Stations) boxes that are located throughout the Alliance
- **DO** inform the Manager/Program Director or the Chief Privacy Officer when an employee or affiliate witness or suspect anyone breaching the privacy and confidentiality of an Alliance patient, employee or affiliate
- **DO** inform patients or others that ask, how they or the Alliance protect their privacy or confidentiality
- **DO** check with the Manager/Program Director or the Chief Privacy Officer if employee or affiliate is unsure of any information as it relates to privacy or confidentiality

- **DO** review and understand the privacy and related policies as they relate to the individual's role (listed below).
- **DO NOT** acknowledge personal health information that is learned through performing one's role to a patient, e.g. if you process an acquaintance's lab results and learn that she is pregnant, **DO NOT** congratulate her the next time you see her unless of course, she tells you of her pregnancy herself.
- **DO NOT** discuss personal health information that you learned of outside of work when you are at work as others may assume you learned of this through your role or a co-worker and are breaching privacy/confidentiality
- **DO NOT** disclose that you saw a patient or visitor, or discuss confidential information, with anyone that does not need to know, including other employees or affiliates, at home or in public places outside the hospital
- **DO NOT** call patients in waiting rooms or other public areas by their first and last name (see [Calling Patients in Waiting Room Policy](#))
- **DO NOT** leave confidential information in unattended or unsecured locations where it may be accessed by unauthorized persons, e.g. lock confidential hard copy information in a cabinet or room
- **DO NOT** take original records containing confidential information that are the property of the Alliance from the premises, unless authorization has been granted
- **DO NOT** send personal health information in Outlook emails without authorization (see [Using Email to Send Personal Health/Patient Information Policy](#))
- **DO NOT** share computer passwords with anyone
- **DO NOT** store any PHI on any computing devices (PC's, laptops, USB drives, CD's, smartphones etc.). Staff/Affiliates require express written approval from the HPHA IT Department. Those who are permitted to store PHI for portability purposes must contact the IT Department for application of encryption software on all computing devices.
- **DO NOT** provide care to or access records for patients that are relatives or known to you if there is someone else that can do this.
- **DO NOT** use bed/status board for non-legitimate purposes, e.g., seeing how busy another unit is or to see if you know someone on another unit

Providing Care to a Family Member or Friend

In some instances healthcare providers, especially those working in small communities, may be required to care for a family member, friend or acquaintance as part of their role. These situations should be limited to circumstances in which no other care providers are available. The patient should be stabilized and, if possible, care transferred. If a healthcare provider's partner/family member is admitted to an agency where the healthcare provider is providing care or services, they must make every effort to ensure that alternative care arrangements are made. Until alternative arrangements are made, however, the healthcare provider may provide care. If it is not possible to transfer care, the following factors must be considered.

- Input from the patient. A client may feel uncomfortable receiving healthcare services from someone with whom he/she has or had a personal relationship.
- Self-awareness/reflection. Carefully reflect on whether professionalism and objectivity in caring for the patient can be maintained, and whether this relationship interferes with meeting the patient's needs. Also, ensure that providing care to a family member or friend will not interfere with the care of other patients, or with the dynamics of the health care team. The situation should be discussed with colleagues and leader before making a decision.
- Maintaining boundaries. When providing care for a family member, friend or acquaintance:
 - be aware of the boundary between professional and personal roles;
 - clarify that boundary for the client;
 - meet personal needs outside of the relationship; and
 - develop and follow a plan of care.
- Confidentiality. It is important not to disclose information about a patient to other family members and/or friends without the patient's consent, even after the provider-patient relationship has ended.

Definitions

Affiliates: individuals who are not employed by the organization but perform specific tasks at or for the organization, including professionals with privileges (e.g. physicians), students, volunteers, contractors or contractor employees who may be members of a third-party contractor or under direct contract to the organization, and individuals working at the organization, but funded through an external source.

Personal Health Information: oral or recorded information that identifies or could identify an individual and:

- relates to physical or mental health
- includes family history as it is reflected in the record of personal health information
- identifies the healthcare provider
- relates to payments or eligibility for healthcare
- relates to donation of body part or bodily substance
- includes the health number
- identifies Substitute Decision Maker
- includes any identifying non-health information

References:

http://www.cno.org/globalassets/docs/prac/41033_therapeutic.pdf - August 2017

Privacy Related Policies

1. [Acceptable Use of Computers/Electronic Resources](#)
2. [Audits of Electronic Personal Health Information](#)
3. [Calling Patients in Waiting Rooms](#)
4. [Information System Remote Access](#)

5. Information System Access
6. Media Relations & Public Statements
7. Patient Access to Personal Health Information
8. Patient Request for Correction to Personal Health Information
9. Photography, Sound Recording and / or Videotaping of Patients
10. Police Requests for & Disclosure of Personal Health Information
11. Privacy Policy
12. Privacy Breach of Patient Health Information
13. Potential Privacy Breach Investigations
14. Protection of Electronic Information
15. Records Retention, Storage and Destruction
16. Restricting Disclosure of Patient Health Information ("lock-box")
17. Release of Personal Health Information
18. Request For Information For Program Planning / Quality Assurance / Utilization Purposes
19. Research Request For Participation
20. Telephone Messages
21. Transmission of Personal Health Information by Fax
22. Using Email to Send Personal Health/Patient Information Policy

Confidentiality Agreement

I understand and agree:

- to abide by the above-mentioned statements for the duration of my employment or affiliation with the Alliance and after this ceases
- breaches of privacy and/or confidentiality are serious offences and may result in disciplinary action up to and including termination of employment or affiliation with the Alliance, reporting to and discipline by professional associations/colleges, legal action and fines up to \$100,000 for individuals.

Name (please print)

Signature

Date