

Practice Education Guidelines for BC Privacy and Confidentiality

July 2021

Intent / Purpose

- Identify the required expectations of Post-Secondary Institution (PSI) Students and Educators for safeguarding and protecting the privacy of Health Care Organization's (HCO) Clients and Workers.
- Outline the responsibilities of the PSIs and HCOs for protecting the privacy and maintaining the confidentiality of personal and business information in the custody or under control of the HCO which might be accessed during the course of a practice education experience.

Definitions

Also refer to: [Standard Terms and Abbreviations](#)

<i>Academic Works</i>	"Works created and submitted by students for evaluation in accordance with course and program requirements, including master's and doctoral theses." ¹ Includes quizzes, essays, reports, film, video, photographs, artistic projects, and any other assignments. ²
<i>Breach of Privacy/Confidentiality</i>	a) "...unauthorized access to or collection, use, disclosure, or disposal of personal information. Such activity is "unauthorized" if it occurs in contravention of the <i>Personal Information Protection Act</i> or part 3 of the <i>Freedom of Information and Protection of Privacy Act</i> " ³ The loss, theft, intentional or inadvertent unauthorized collection, use, disclosure, storage, or disposal of personal information in the custody or control of HCOs. ⁴ b) Unauthorized access to or use, disclosure, or disposal of any information about the business, affairs, or operations of the HCO which is not generally known or available to the public.
<i>Confidentiality</i>	The duty of someone who has received confidential information in trust to protect that information and disclose it to others only in accordance with permissions, rules or laws authorizing its disclosure. ⁵
<i>Confidential Information</i>	...all data, information, and material relating to the [HCO] and its services, staff, contractors, service providers, or [the people who receive care or service (clients)], whether or not it is stored in written, electronic or any other form, that students or [PSI] staff receive, in connection with [a practice education experience], including: (i) personal information about [HCO] staff and [clients], (ii) health records, (iii) any information about the business, affairs, or operations of the [HCO] which is not generally known or available to the public ⁶

¹ University of Waterloo. (January 2020). *Records Management: TL40 – Student Work, Examinations & Theses [DRAFT]*. Retrieved March 11, 2021 from <https://uwaterloo.ca/records-management/news-watclass-updates/updated-records-classes-retention-schedules-drafts/tl40-student-work-examinations-theses-draft>

² Ibid.

³ Office of the Information & Privacy Commissioner for British Columbia. (March 2012). *Privacy Breaches: Tools and Resources*. Page 3. Retrieved April 5, 2019 <https://www.oipc.bc.ca/guidance-documents/1428>

⁴ Provincial Health Services Authority. (2012). *IA_020 Privacy and Confidentiality Policy*. Vancouver, BC. Retrieved March 21, 2021 from <http://www.phsa.ca/Documents/PrivacyandConfidentiality.pdf>

⁵ Canadian Nurses Association. (2003). Privacy and Health Information: Challenges for Nurses and for the Nursing Profession. *Ethics in Practice for Registered Nurses, November 2003*, page 3. Retrieved April 5, 2019 from https://www.cna-aic.ca/~media/cna/page-content/pdf-en/ethics_pract_privacy_health_nov_2003_e.pdf?la=en

⁶ Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*. Retrieved October 27, 2020 from <https://www.hcpp.org/?q=node/17>

Practice Education Guidelines for BC Privacy and Confidentiality

<i>Confidential Business Information</i>	"Any information about the business, affairs, or operations of the [HCO] which is not generally known or available to the public" ⁷ "...includes but is not limited to: draft correspondence; financial forecasts not yet made public; some third party business information typically supplied in confidence; specific contract language; legal opinions prepared for the health authority; some quality improvement information; ongoing labour relations issues not yet resolved; negotiations carried on or for the public body." ^{8, 9, 10}
<i>Data Steward</i>	"Refers to a public body that has ultimate responsibility for a given data source. In practice, an individual is typically named as having the authority to approve or reject research requests involving that data, typically called 'the / a Data Steward.' " ¹¹ Those within HCOs responsible for ensuring that the use or disclosure of HCO data is done in a way that protects client personal information and fulfills HCO responsibilities to the FIPPA. Example: Health Records department
<i>Destroy/Destruction (Secure)</i>	Ways to prevent sensitive or personal information on records from being retrieved or reconstructed a) Physical record: cross shredding or placing in marked confidential shredding containers b) Electronic record: ¹² - completely erase through overwriting using overwriting software (deleting the file or reformatting does not completely erase the data) - expose to a powerful magnetic field (degaussing) - shred, pulp, incinerate, pulverize (CD ROMS, DVDs, SD cards, tapes, etc.)
<i>Encrypt/Encryption</i>	"The process of protecting personal information by encoding data into an electronic form that can only be read by the intended authorized recipient." ¹³
<i>Health Record</i>	"...confidential compilation of pertinent facts of an individual's health history, including all past and present medical conditions, illnesses and treatments, with emphasis on the specific events affecting the patient during the current episode of care." ¹⁴
<i>'Need to know' and 'Least Privilege' Principles</i>	"The "need to know" principle states that authorized users of a system should only have access to the minimum amount of [personal] information that is necessary to perform their duties within a public body or an organization. The "least privilege" principle requires that each authorized user in a system be granted the most restrictive access privileges needed for performing authorized tasks. The principles are reflected in privacy law but not always expressly stated." ¹⁵
<i>Perpetuity</i>	Continuing forever, everlasting ¹⁶
<i>Personal Identity Information</i>	"any personal information of a type that is commonly used, alone or in combination with other information, to identify or purport to identify an individual" ¹⁷

⁷ Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*. Retrieved October 27, 2020 from <https://www.hcpp.org/?q=node/17>

⁸ Interior Health Authority. (2021). *Privacy Frequently Asked Questions*. Retrieved February 28, 2021 from <https://www.interiorhealth.ca/YourStay/PrivacyRightsConfidentiality/Pages/PrivacyFAQs.aspx>

⁹ Vancouver Island Health Authority. (n.d.). *Legislation in BC – FAQs*. Retrieved March 4, 2021 from <https://www.islandhealth.ca/about-us/accountability/information-stewardship-access-privacy/legislation-bc>

¹⁰ Government of British Columbia. (2019). *Freedom of Information and Privacy Protection Act [RSBC] Chapter 165: Division 2.21 Disclosure harmful to business interests of a third party*. Retrieved February 28, 2021 from https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi

¹¹ PopulationDataBC. (n.d.). *Glossary of Terms: Data Steward*. Retrieved March 21, 2021 from https://www.popdata.bc.ca/data_access/glossary#d

¹² Information and Privacy Commissioner of Ontario. (2018). *Technology Fact Sheet: Disposing of Your Electronic Media*. Retrieved on April 13, 2019 from <https://www.ipc.on.ca/wp-content/uploads/2018/03/fs-tech-disposing-of-your-electronic-media-003.pdf>

¹³ Doctors of BC, College of Physicians and Surgeons of BC, Office of the Information and Privacy Commissioner. (August 2017). *BC Physician Privacy Toolkit: A guide for physicians in private practice (3rd ed.)*. Pg. 63. Retrieved March 7, 2021 from <https://www.oipc.bc.ca/guidance-documents/1470>

¹⁴ Health Information Management. (2019). *What is a Health Records?* Retrieved August 27, 2019 from <http://www.himconnect.ca/patients/commonly-asked-questions/what-is-a-health-record>

¹⁵ Doctors of BC, College of Physicians and Surgeons of BC, Office of the Information and Privacy Commissioner. (August 2017). *BC Physician Privacy Toolkit: A guide for physicians in private practice (3rd Edition)*. Pages 65-66.

¹⁶ Perpetual [Def. 1]. (n.d.). In *Merriam-Webster Online*, Retrieved April 5, 2019 from <https://www.merriam-webster.com/dictionary/perpetual>

¹⁷ Government of British Columbia. (2019). *Freedom of Information and Privacy Protection Act [RSBC] Chapter 165, Schedule 1*. Retrieved April 5, 2019 from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_07

Practice Education Guidelines for BC Privacy and Confidentiality

<i>Personal Information</i>	"recorded information about an identifiable individual other than contact information" ¹⁸ "information about an identifiable individual's health and includes information about the individual's health care providers, health numbers (such as care card number) and insurance." ¹⁹ Examples: demographic data, psychosocial history, family history, financial or personal situation, identification numbers, marital status
<i>Privacy</i>	"(1) physical privacy is the right or interest in controlling or limiting the access of others to oneself; (2) informational privacy is the right of individuals to determine how, when, with whom and for what purposes any of their personal information will be shared. A person has a reasonable expectation of privacy in the health-care system so that health-care providers who need their information will share it only with those who require specific information" ²⁰
<i>Record/Recording</i>	Noun: Any confidential information that is recorded in some way "Under FIPPA, a 'record' includes books, documents, maps, drawings, photographs, letters, vouchers, papers, and any other thing on which information is recorded or stored by graphic, electronic, mechanical, or other means." ²¹ Examples: email, text message, CD/DVD, USB/SD memory device, microfiche, computer file, data management systems, mobile device, camera, or "even heard by word of mouth" ²² (i.e. subjective data).
<i>Safeguards / Security</i>	Measures used to protect information (how information is accessed, used, and disclosed – and by whom) <ul style="list-style-type: none">- Physical safeguards: use of locked cabinets, locating devices with data away from public areas- Administrative safeguards: development and enforcement of policies around who can access personal information- Technical safeguards: use of computer passwords, non-sharing of passwords, firewalls, anti-virus software, encryption, and other measures to protect from unauthorized access, loss, or modification^{23, 24}
<i>Transitory Records</i>	"...records of temporary usefulness that are not an integral part of an administrative or operational record series, that are not regularly filed with standard records or filing systems, and that are only required for a limited period of time for completion of a routine action or the preparation of an ongoing record." ²⁵ "Transitory records are records of temporary usefulness that are needed only for a limited period of time in order to complete a routine action or prepare a final record. As with all records, they can exist in any format or medium (paper or electronic), and can be created and shared using a variety of technologies...All confidential (including restricted) transitory records should be securely destroyed." ²⁶ Examples of transitory records: worksheets, rough notes, informational material, convenience copies, and returned academic works

¹⁸ Government of British Columbia. (2019). *Freedom of Information and Privacy Protection Act [RSBC] Chapter 165, Schedule 1*. Retrieved April 5, 2019 from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_07

¹⁹ BC Freedom of Information and Privacy Association. (March 2011). *Definitions – Personal health information*. Retrieved March 7, 2021 from <http://www.healthinfoprivacybc.ca/home/definitions>

²⁰ Canadian Nurses Association. (2017). *CNA Code of Ethics for Registered Nurses*. Page 25. Retrieved April 4, 2019 from <https://www.cna-aic.ca/en/nursing-practice/nursing-ethics>

²¹ Office of the Information & Privacy Commissioner for British Columbia. (October 2015). *Guide to Access and Privacy Protection under FIPPA*. Page 7. Retrieved April 5, 2019 from <https://www.oipc.bc.ca/guidance-documents/1466>

²² National Health Service. (October 2019). *POL_1010 Confidentiality Policy*. Corporate Information Governance. Version 5.0. Page 5. Retrieved March 21, 2021 from <https://www.england.nhs.uk/publication/confidentiality-policy/>

²³ Office of the Information & Privacy Commissioner for British Columbia. (2015). *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*. Pg. 36-37. Retrieved March 4, 2021 from <https://www.oipc.bc.ca/guidance-documents/1438>

²⁴ Government of Canada. (2014). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS (2018), Chapter 5, Privacy and Confidentiality Key Concepts, Security*. 5C-Article 5.3. Retrieved March 4, 2021 from https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html

²⁵ Government of British Columbia. (n.d.). *Transitory Records (schedule 102901)*. Retrieved February 28, 2021 from <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules/special-schedules/transitory-records>

²⁶ University of the Fraser Valley. (n.d.). *Transitory Records Schedule*. Para. 5. Retrieved February 28, 2021 from <https://www.ufv.ca/secretariat/records-management/official-record-schedules/transitory-records-schedule/>

Practice Education Guidelines for BC Privacy and Confidentiality

Practice Education Guidelines

All parties involved in practice education share the responsibility for protecting the privacy and maintaining the confidentiality of information learned during the course of a practice education experience.

All confidential information accessed by PSI Students and Educators during a practice education experience is the property of the HCO.²⁷

HCOs and PSIs, and their Workers, Educators, and Students, as well as Contractors/Vendors involved in practice education experiences, are subject to the provisions of applicable laws and standards of practice that protect privacy and confidentiality, including:

- [Freedom of Information and Protection of Privacy Act \(FIPPA or FOIPPA\)](#)²⁸
- [Personal Information Protection Act \(PIPA\)](#)²⁹
- [E-Health \(Personal Health Information Access and Protection of Privacy\) Act](#)³⁰
- the requirements of Educational Institution Affiliation Agreement³¹, service agreements (see [Educational Institution Affiliation Agreement Template; PEG Contractor/Vendor Practice Education Experiences](#)), professional- or discipline-specific 'code of ethics', 'codes of conduct', and/or practice standards.

PSI Students and Educators, HCO Workers, and/or Contractors/Vendors, as researchers, conducting research involving HCO Workers or Client as part of the practice education experience also:

- are bound by the Tri-Council Policy Statement on the Ethical Conduct for Research Involving Humans (Canada)³² and The First Nations Principles of OCAP® (Ownership, Control, Access, and Possession)³³
- could require entering into a separate information-sharing agreement (refer to HCO and PSI Research Ethics Boards)³⁴

²⁷ Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*. Retrieved October 27, 2020 from <https://www.hcpp.org/?q=node/17>

²⁸ Government of British Columbia. (2019). *Freedom of Information and Protection of Privacy Act [RSBC] Chapter 165*. Retrieved February 28, 2021 from https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi

²⁹ Ibid. (2020). *Personal Information Protection Act [SBC 2003] Chapter 63*. Retrieved November 3, 2020 from https://www.bclaws.ca/civix/document/id/complete/statreg/03063_01

³⁰ Ibid. (2020). *E-Health (Personal Health Information Access and Protection of Privacy) Act [SBC 2008] Chapter 38*. Retrieved March 4, 2021 from https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_08038_01

³¹ Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*.

³² Government of Canada. (2018). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2018)*. Retrieved March 4, 2021 from https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html

³³ First Nations Information Governance Centre. (2021). *The First Nations Principles of OCAP®*. Retrieved March 4, 2021 from <https://fnigc.ca/>

³⁴ Government of Canada. (2018). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS (2018), Chapter 5, Privacy and Confidentiality Key Concepts, Security*. 5C-Article 5.3. Retrieved March 4, 2021 from https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html

Practice Education Guidelines for BC Privacy and Confidentiality

PSI Educators and Students **only take part** in a practice education experience **after**:

- The individual has **completed** the HCO relevant **education** on information privacy and confidentiality; **and**
- The individual has **signed** the HCO Confidentiality Undertaking agreement in a method approved by the HCO.³⁵

The HCO or PSI retains the completed/signed Confidentiality Undertaking agreements according to all legal, regulatory, and accreditation requirements, as well as HCO record retention policies. (Can be as long as 10 years beyond the practice education experience based on the period of time the HCO is required to retain the Client's health record under the Hospital Act Regulation).³⁶

PSI Students and Educators access, collect, use, and disclose HCO confidential information:

- based on the 'need to know' and 'least privilege' principles
- with the highest degree of anonymity possible in the circumstances
- according to HCO policies and procedures

Continued access to HCO confidential personal and/or business information depends on PSI Students and Educators keeping information confidential both inside and outside the practice education setting.

Records/recordings obtained **for HCO Client health care** or **HCO business purposes** during the course of a practice education experience:

- remain the property of the HCO
- cannot leave the HCO practice education setting on the PSI Student's or Educator's person or personal electronic device
- can only be transmitted internally using HCO or government secure email networks, externally using an approved email network as an attachment using industry-standard encryption, or by using the HCO secure file sharing service
- can only be transmitted to those involved in HCO health care or service based on the 'need to know' and 'least privilege' principles
- cannot be retained by the PSI Student or Educator

³⁵ Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*. Retrieved October 27, 2020 from <https://www.hcpp.org/?q=node/17>

³⁶ Government of British Columbia. (2019). *Hospital Act Regulation: Destruction of health record documents*. Retrieved April 5, 2019 from http://www.bclaws.ca/civix/document/id/complete/statreg/121_97#section14

Practice Education Guidelines for BC Privacy and Confidentiality

For recordings of HCO Clients for academic purposes:

- The HCO Practice Education Coordinator is informed of and obtains approval from the HCO privacy officer for the activity before the practice education experience begins.
- The HCO Client's written consent is retained in the Client's health record.
- Students:
 - Make every effort to use the least identifiable personal HCO Client or Worker information in academic works.
 - Secure and only share the recording with the PSI Educator via an approved HCO and PSI methods.
 - Use industry-standard encryption for digital-based recordings, such as:
 - as an encrypted and password protected attachment through the PSI or HCO email system
 - in an encrypted and password protected mobile storage device
 - a secure file sharing service³⁷

Regardless of whether obtained for HCO Client health care, HCO business purposes, or academic purposes, recordings cannot be posted on social networking sites or anywhere else on the internet regardless of the privacy settings.

PSI Educators, who retain Student academic works, securely store and/or destroy Student academic works containing any personal HCO Client or Worker personal information and/or confidential HCO business information according to the PSI records management protocol for transitory, temporary, and permanent records.

Students, who have academic works returned after grading, remove and securely destroy all content containing any personal HCO Client or Worker personal information and/or confidential HCO business information.

PSI Students and Educators securely destroy all confidential transitory records created during the course of a practice education experience as soon as the usefulness of the records has ended.

Example: Rough notes made throughout the day relevant to the care or service of HCO Clients used for entry into the HCO Client's permanent record.

³⁷ University of British Columbia. (n.d.). *Guard it: Preventing a Privacy Breach – What are the recommended methods for sharing UBC data?* Retrieved March 4, 2021 from <https://privacymatters.ubc.ca/share-files-securely#what-are-the-recommended-methods-for-sharing-ubc-data>

Practice Education Guidelines for BC Privacy and Confidentiality

Using the same principles as would apply to Client privacy and confidentiality:

- HCO and its Workers respect and protect the privacy and confidentiality of the PSI Students and Educators.
- PSI and its Students and Educators respect and protect the privacy and confidentiality of the HCO Workers.

Any HCO Clients' or Workers' private and confidential information or HCO confidential business information:

- learned by PSI Students or Educators during a practice education experience shall be kept confidential in perpetuity
- used or disclosed by the PSI Student or Educator outside the context of a practice education experience constitutes a breach of privacy or confidentiality

In cases where there is a discrepancy between PSI and HCO policies, standards, guidelines, and/or protocols around preserving confidentiality, the more restrictive applies.

Any breach, unintended or otherwise, by PSI Students/Educators or HCO Workers is investigated and acted on according to both the HCO and PSI policies and protocols.

During a breach investigation, all parties involved:

- make every effort to recover any confidential or personal information
- cooperate with the breach investigation
- comply with requests for evidence and documentation when requested
- identify opportunities to improve processes and prevent future breaches

Failure of the PSI, Educator, and/or Student to maintain in perpetuity the privacy and confidentiality of personal information/records or recordings of HCO Clients and/or business information/records of HCOs, no matter how it is obtained, will result in action by the HCO, such as:

- suspending or excluding the PSI Student or Educator, either temporarily or permanently, from the practice education experience
- working with the PSI to address the breach through mediation or arbitration
- taking legal action against the PSI and/or the Educator/Student
- terminating the Educational Institution Affiliation Agreement (see [Educational Institution Affiliation Agreement Template](#))

Practice Education Guidelines for BC Privacy and Confidentiality

Failure of any HCO Worker to maintain in perpetuity the privacy and confidentiality of personal information/records or recordings of PSI Students and/or Educators, no matter how it is obtained, will result in action by the PSI, such as:

- removing the PSI Student or Educator, either temporarily or permanently, from the practice education experience
- working with the HCO to address the breach through mediation or arbitration
- taking legal action against the HCO and/or the Worker
- terminating the Educational Institution Affiliation Agreement (see [Educational Institution Affiliation Agreement Template](#))

Roles, Responsibilities and Expectations

Post-Secondary Institutions

- Collaborate with the HCOs to make sure systems, processes, and policies are in place for the legitimate secure movement of confidential information between the PSI and the HCO.
- Provide education to Students in ways to reduce inadvertent privacy/confidentiality breaches, including:
 - legal and ethical obligations in maintaining privacy and confidentiality
 - risks of using communication technologies such as email, video tools, social media platforms, photo or video sharing sites
 - standards and practices for ensuring assignments that do not uniquely identify HCO Clients or Workers
 - current practices for transferring, securing, and storing paper and digital-based academic works
 - methods for timely and secure destruction of transitory records and academic works created during the practice education experience that contain confidential personal HCO Client or Worker information or HCO business information
- Take steps to ensure that PSI Educators and Students are aware of, understand, and practice according to the signed terms and conditions related to Privacy and Confidentiality stated within the Educational Institution Affiliation Agreement (see [Educational Institution Affiliation Agreement Template](#)).
- Facilitate the process for Educators and Students to access, understand, and sign the HCO Confidentiality Undertaking agreement.
- Securely submit or retain the HCO Confidentiality Undertaking agreements according to the HCO-specific policy.

Practice Education Guidelines for BC Privacy and Confidentiality

- Ensure the requirements for academic works related to practice education experiences are structured to limit the use of Client materials and recordings, and what is used follows HCO consent and confidentiality policies.
- Employ safeguards (policies and practices) to protect HCO personal and/or confidential information obtained during the course of a practice education experience to ensure it is collected, used, stored, disclosed, transferred, and securely destroyed by Students and Educators appropriately.
- Review at least annually the use of communication technology (such as learning management systems and social media platforms) and traditional educational processes used by Educators and Students to ensure they are not placed at risk for breaching privacy and confidentiality obligations to the HCO.
- Should any breaches or potential breaches of privacy or confidentiality by a Student or Educator occur:
 - Immediately disclose the breach to the HCO
 - Cooperate with any investigation done by the HCO.
 - Return or facilitate the return of any HCO health records or confidential information held by Students or Educators.

PSI Educators

- Review the HCO policies on privacy and confidentiality before the practice education experience.
- Complete HCO education on privacy and confidentiality as per HCO requirements ([*PEG Orientation On-Site Post-Secondary Institution Educators*](#)).
- Confirm understanding of responsibilities by signing the HCO's Confidentiality Undertaking agreement using the method approved by the HCO.
- Reconfirm the HCO's Confidentiality Undertaking on a regular basis as defined by the HCO requirements.
- Adhere to the HCO's policies concerning the collection, use, disclosure, retention, and disposal of personal and business information.
 - Collect, use, disclose, retain, and dispose of all HCO personal information as defined by relevant legislation, HCO and PSI policies, and professional practice standards.
 - Ensure both own and Students' access to HCO personal and business information is authorized by the HCO and only for the purposes of the practice education experience based on the 'need to know' and 'least privilege' principles.

Practice Education Guidelines for BC Privacy and Confidentiality

- Only share with Students relevant HCO Client or business information needed for learning purposes during the practice education experience.
- When engaging in any form of communication (verbal or written, in-person or electronic) about HCO Clients or Workers, ensure the discussion is in a private location, is respectful, and does not identify those persons unless necessary and appropriate based on the 'need to know' and 'least privilege' principles.
- Ensure Students use the least amount of identifying information possible (such as personal identifiers) when submitting academic works.
- Securely destroy all confidential transitory records created during the course of a practice education experience as soon as the usefulness of the records has ended.
- Ensure graded academic works containing any confidential HCO Client or Worker person information/records or recordings, or confidential HCO business information is either:
 - retained according to the PSI records management protocols, or
 - returned to the Student with directive to be securely destroyed
- Immediately report, using HCO protocol:
 - any breach or potential breach of privacy or confidentiality
 - any practices within the HCO that compromise or have the potential to compromise private or confidential information
- Take part in any HCO or PSI breach investigations as required.

Students

- Review the HCO policies on privacy and confidentiality before the practice education experience.
- Complete HCO education on privacy and confidentiality as per HCO requirements ([PEG Orientation – Students](#)).
- Confirm understanding of responsibilities by signing the HCO's Confidentiality Undertaking agreement using the method approved by the HCO.
- Hold all private and confidential information observed or gathered during the course of a practice education experience in the strictest confidence in perpetuity.
- Adhere to the HCO's policies concerning the collection, use, and disclosure of personal information as defined in the FIPPA and HCO policies on the use of **social media**.
- Adhere to the HCO's policies concerning the collection, use, disclosure, retention, and disposal of personal and business information.

Practice Education Guidelines for BC Privacy and Confidentiality

- Collect, use, disclose, retain, and dispose of all HCO personal information as defined by relevant legislation, HCO and PSI policies, and professional practice standards.
- Only collect, access, use, or disclose personal and/or business information authorized by the HCO and only for the purposes of the practice education experience based on the 'need to know' and 'least privilege' principles.
- Use safeguards to protect personal, confidential, and sensitive information in any medium (digital and paper-based):
 - Protect **passwords** to any HCO electronic system (such as the electronic medical record). Do not share password with anyone. Do not use another person's password under any circumstances.
 - When engaging in any form of communication (verbal or written, in-person or electronic) about HCO Clients or Workers, ensure the discussion is in a private location, is respectful, and does not identify those persons unless necessary and appropriate.
 - Share only relevant HCO Client and/or business information from the practice education experience with fellow Students and PSI Educators for learning purposes (such as during PSI Educator-led debriefings, reflective journals, or assignments).
 - Securely destroy all confidential transitory records as soon as the usefulness of the records has ended.
 - Use the least amount of identifying information as possible (such as personal identifiers) when submitting assignments (such as case studies, care plans, and presentations).
 - Do not download personal HCO Client or Worker information, or HCO business information onto any portable electronic device (such as laptops, tablets, smart phones, USB/SD memory devices/cards) unless it is encrypted and done with the permission of a HCO data steward or HCO policy.
 - Do not print, photograph, video, or photocopy any part of the HCO Client's health record or any communication tools with Client information (such as whiteboards).
 - Only use approved PSI and/or HCO **email systems** for the transferring of private and confidential information and use industry-standard encryption. Do not use or auto-forward to unsecure or unapproved email systems (such as Gmail or Hotmail).

Practice Education Guidelines for BC Privacy and Confidentiality

- When taking recordings of HCO Clients:
 - For the sole purposes of it becoming a component of the **health record** (such as documenting a Client's condition and tracking progress of treatment), only do so if:
 - it is within Student's role and expectations (see [PEG Student Practice Activities, Limits, and Conditions](#)),
 - it is with the Client's expressed verbal consent (see [PEG Consent for Student Involvement in Health Care](#)),
 - it uses an HCO electronic device, and
 - it can be done according to HCO policy
 - For the purposes of academic work, education, or research, only do so if:^{38, 39}
 - it is within Student's role and expectations (see [PEG Student Practice Activities, Limits, and Conditions](#)),
 - it is with the Client's expressed written consent obtained by the HCO Supervisor and retained in the Client's health record (see [PEG Consent for Student Involvement in Health Care](#)),
 - every effort is made to conceal the Client's identity,
 - the recording can be stored securely,⁴⁰
 - the electronic device used allows for secure transfer of the recording using industry-standard encryption,⁴¹ and
 - it can be done according to both HCO and PSI policy
 - Regardless of whether the recording is for the Client's health record or academic work, explain to the HCO Client:^{42, 43}
 - how the recording will be stored,
 - how the recording will be secured,
 - how identifying features and information will be protected or removed,
 - who will have access to the raw and transcribed recording,
 - if the recording will be used for educational purposes, and

³⁸ School of Social Work. (2017). *Master of Social Work Practicum Manual*. Renison University College affiliated with the University of Waterloo. Page 27. Retrieved June 28, 2019 from https://uwaterloo.ca/school-of-social-work/sites/ca.school-of-social-work/files/uploads/files/msw_practicum_manual_2017-2018_2.pdf

³⁹ The General Medical Council. (March 2013). *Making and using visual and audio recordings of patients*. Retrieved March 14, 2021 from <https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/making-and-using-visual-and-audio-recordings-of-patients/recordings-made-for-research-teaching-training-and-other-healthcare-related-purposes>

⁴⁰ University of British Columbia. (March 2020). *Guard it: Preventing a Privacy Breach - Information and Security Guideline: How to Encrypt Files Using Common Applications*. Retrieved March 7, 2021 from <https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/How%20to%20Encrypt%20Files%20using%20Common%20Applications%20Guideline.pdf> on <https://privacymatters.ubc.ca/share-files-securely>

⁴¹ Ibid.

⁴² Research Ethics Board. (2017). *Guidelines for Obtaining Consent and Assent*. Ryerson University. Page 8. Retrieved June 28, 2019 from <https://www.ryerson.ca/content/dam/research/documents/ethics/guidelines-for-obtaining-assent-and-consent.pdf>

⁴³ School of Social Work. (December 2020). *Field Education: The critical bridge between social work education & practice – BSW Field Education Manual*. Memorial University. Pg 36-39. Retrieved March 21, 2021 from https://www.mun.ca/socialwork/field/BSW_Field_Education_Manual.pdf

Practice Education Guidelines for BC Privacy and Confidentiality

- if and when the recording will be destroyed.
- Remove and securely destroy **assignments** or content within assignments containing any personal HCO Client information⁴⁴/records⁴⁵, HCO Worker personal information/records, or HCO business information once assignments have been completed and graded.
- Immediately report, using HCO and/or PSI protocol:
 - any breach or potential breach of privacy or confidentiality
 - any practices within the HCO that compromise or have the potential to compromise private or confidential information
- Take part in any HCO or PSI breach investigations as required.

Health Care Organizations

- Collaborate with the PSIs to make sure systems, processes, and policies are in place for the legitimate and secure movement of confidential information between the HCO and the PSI.
- Make HCO privacy, confidentiality, and related policies available to PSIs, Students, and Educators.
- Communicate any changes in policies and protocols to PSIs regarding access, use, and disclosure of private and confidential information.
- Take reasonable steps to ensure that HCO Educators and Workers involved in practice education are aware of, understand, and practice according to the signed terms and conditions related to Privacy and Confidentiality stated within Educational Institution Affiliation Agreement (see [Educational Institution Affiliation Agreement Template](#)).
- Ensure the Confidentiality Undertaking agreement addresses privacy and confidentiality aspects unique to practice education and the need to use this information for learning purposes.
- Retain signed Confidentiality Undertaking agreements according to HCO record retention policies.
- Provide reasonable access to Client or business records for PSI Educators to create Student assignments and for Students to carry out those assignments based on the 'need to know' and 'least privilege' principles.

44 Government of British Columbia. (2019). *Freedom of Information and Privacy Protection Act [RSBC] Chapter 165, Schedule 1*. Retrieved April 5, 2019 from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_07

45 National Health Service. (August 2018). *POL_1010 Confidentiality Policy*. Corporate Information Governance. Version 4.0. Page 5. Retrieved April 5, 2019 from <https://www.england.nhs.uk/wp-content/uploads/2016/12/confidentiality-policy-v4.pdf>

Practice Education Guidelines for BC Privacy and Confidentiality

- Collect, use, protect, disclose, retain, and securely destroy PSI Educator and/or Student personal information that is in the custody and control of the HCO **only for**:
 - any purposes related to the practice education experience
 - conducting investigations related to the practice education experience
 - complying with legal requirements
 - the safety of HCO Clients and Workers
- To retain and use any Student record information (such as a pre-practice education experience resume) following the practice education experience:
 - Obtain Student consent.
 - Securely store such information.
 - Securely destroy such information according to HCO records management protocol for transitory, temporary, and permanent records.
- Inform Clients that PSI Students and Educators could have access to and use their personal information for educational purposes, based on the 'need to know' and 'least privilege' principles according to FIPPA.
- Use systems and processes that best support privacy and confidentiality to minimize the risk of privacy and confidentiality breaches involving PSI Students and Educators while in the practice education setting (such as confidential paper shredding and mandatory password access).
- Conduct privacy assessments related to practice education experiences as needed to ensure compliance with HCO policies, share findings with the PSI, and work with the PSI to remedy any gaps in compliance.
- Investigate breaches or potential breaches involving PSI Students or Educators and share findings with the PSI.

HCO Supervisors / Workers

- Protect all Student personal information observed, collected, used, disclosed, shared, or stored during the practice education experience according to relevant legislation, HCO and PSI policies, and professional practice standards.
- When engaging in any form of communication (verbal or written, in-person or electronic) about Students with other HCO Workers or PSI Educators, ensure the discussion is in a private location, is respectful, and does not identify those persons unless necessary and appropriate based on the 'need to know' and 'least privilege' principles.

Practice Education Guidelines for BC Privacy and Confidentiality

References and Resources

- BC Freedom of Information and Privacy Association. (March 2011). *Definitions – Personal health information*. Retrieved March 7, 2021 from <http://www.healthinfoprivacybc.ca/home/definitions>
- Canadian Nurses Association. (2017). *CNA Code of Ethics for Registered Nurses*. Retrieved April 4, 2019 from <https://www.cna-aicc.ca/en/nursing-practice/nursing-ethics>
- Ibid. (2003). *Privacy and Health Information: Challenges for Nurses and for the Nursing Profession. Ethics in Practice for Registered Nurses, November 2003*. Retrieved April 5, 2019 from https://www.cna-aicc.ca/~media/cna/page-content/pdf-en/ethics_pract_privacy_health_nov_2003_e.pdf?la=en
- Columbia University Irving Medical Center. (2019). *Confidentiality, Electronic Media, and Protected Patient Information Required Guidelines: HIPAA and Electronic Medical Record Access*. Columbia University. Retrieved April 13, 2019 from <https://www.ps.columbia.edu/education/student-resources/honor-code-and-policies/school-and-university-policies/confidentiality>
- Doctors of BC, College of Physicians and Surgeons of BC, Office of the Information and Privacy Commissioner. (2017). *BC Physician Privacy Toolkit: A guide for physicians in private practice*. (3rd ed.). Retrieved April 5, 2019 from https://www.doctorsofbc.ca/sites/default/files/ptv3.0_full_document.pdf
- First Nations Information Governance Centre. (2021). *The First Nations Principles of OCAP®*. Retrieved March 4, 2021 from <https://fnigc.ca/>
- Government of British Columbia. (2019). *Freedom of Information and Protection of Privacy Act [RSBC] Chapter 165*. Retrieved April 5, 2019 from https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/96165_00_multi
- Ibid. (2019). *E-Health (Person Health Information Access and Protection) Act [SBC 2008] Chapter 38*. Retrieved April 13, 2019 from http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_08038_01
- Ibid. (2019). *Hospital Act Regulation: Destruction of health record documents*. Retrieved April 5, 2019 from http://www.bclaws.ca/civix/document/id/complete/statreg/121_97#section14
- Ibid. (2020). *Personal Information Protection Act [SBC 2003] Chapter 63*. Retrieved November 3, 2020 from https://www.bclaws.ca/civix/document/id/complete/statreg/03063_01
- Ibid. (n.d.) *Transitory Records (schedule 102901)*. Retrieved February 28, 2021 from <https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/records-management/information-schedules/special-schedules/transitory-records>
- Government of Canada. (2018). *Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS (2018), Chapter 5, Privacy and Confidentiality Key Concepts, Security*. March 4, 2021 from https://ethics.gc.ca/eng/policy-politique_tcps2-eptc2_2018.html

Practice Education Guidelines for BC Privacy and Confidentiality

- Health Care Protection Program. (2008). *Risk Note: Managing Risk in Educational Affiliation Agreements - Educational Institution Affiliation Agreement Template*. Retrieved October 27, 2020 from <https://www.hcpp.org/?q=node/17>
- Health Information Management. (2019). *What is a Health Records?* Retrieved August 27, 2019 from <http://www.himconnect.ca/patients/commonly-asked-questions/what-is-a-health-record>
- Information and Privacy Commissioner of Ontario. (2018). *Technology Fact Sheet: Disposing of Your Electronic Media*. Retrieved on April 13, 2019 from <https://www.ipc.on.ca/wp-content/uploads/2018/03/fs-tech-disposing-of-your-electronic-media-003.pdf>
- Interior Health Authority. (2021). *Privacy Frequently Asked Questions*. Retrieved February 28, 2021 from <https://www.interiorhealth.ca/YourStay/PrivacyRightsConfidentiality/Pages/PrivacyFAQs.aspx>
- National Health Service. (October 2019). *POL_1010 Confidentiality Policy*. Corporate Information Governance. Version 5.0. Page 5. Retrieved March 21, 2021 from <https://www.england.nhs.uk/publication/confidentiality-policy/>
- Office of the Information & Privacy Commissioner for British Columbia. (March 2012). *Privacy Breaches: Tools and Resources*. Page 3. Retrieved April 5, 2019 <https://www.oipc.bc.ca/guidance-documents/1428>
- Ibid. (October 2015). *Guide to Access and Privacy Protection under FIPPA*. Retrieved April 5, 2019 from <https://www.oipc.bc.ca/guidance-documents/1466>
- Ibid. (2015). *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations*. Retrieved March 4, 2021 from <https://www.oipc.bc.ca/guidance-documents/1438>
- Perpetual [Def. 1]. (n.d.). In *Merriam-Webster Online*. Retrieved April 5, 2019 from <https://www.merriam-webster.com/dictionary/perpetual>
- PopulationDataBC. (n.d.). *Glossary of Terms: Data Steward*. Retrieved March 21, 2021 from https://www.popdata.bc.ca/data_access/glossary#d
- Provincial Health Services Authority. (2012). *IA_020 Privacy and Confidentiality Policy*. Vancouver, BC. Retrieved March 21, 2021 from <http://www.phsa.ca/Documents/PrivacyandConfidentiality.pdf>
- Ibid. (2019). *Research Administration & Services: Data Access & Management*. Retrieved April 13, 2019 from <http://www.phsa.ca/researcher/resources-support/data-access-management>
- Rankin School of Nursing. (July 2020). *Policy on Confidentiality of Client Information*. Retrieved March 14, 2021 from https://www2.mystfx.ca/nursing/sites/mystfx.ca.nursing/files/Policy%20on%20Confidentiality%20of%20Client%20Information%20%281%29_0.pdf

Practice Education Guidelines for BC Privacy and Confidentiality

- Research Ethics Board. (2017). *Guidelines for Obtaining Consent and Assent*. Ryerson University. Page 8. Retrieved June 28, 2019 from <https://www.ryerson.ca/content/dam/research/documents/ethics/guidelines-for-obtaining-assent-and-consent.pdf>
- School of Social Work. (2019). *Field Practice Manual*. McMaster University. Pages 48 -49, Retrieved June 28, 2019 from <https://socialwork.mcmaster.ca/resources/field-placements/field-practice-manual.doc>
- School of Social Work. (2017). *Master of Social Work Practicum Manual*. Renison University College affiliated with the University of Waterloo. Page 27. Retrieved June 28, 2019 from https://uwaterloo.ca/school-of-social-work/sites/ca.school-of-social-work/files/uploads/files/msw_practicum_manual_2017-2018_2.pdf
- School of Social Work. (December 2020). *Field Education: The critical bridge between social work education & practice – BSW Field Education Manual*. Memorial University. Retrieved March 21, 2021 from https://www.mun.ca/socialwork/field/BSW_Field_Education_Manual.pdf
- Spector, N., & Kappel, D. M. (2012). Guidelines for using electronic and social media: The regulatory perspective. *Online J Issues Nurs*, 17(3), 1. https://www.researchgate.net/profile/Nancy_Spector/publication/232085596_Spector_N_Kappel_DM_Guidelines_for_using_electronic_and_social_media_the_regulatory_perspective_Online_J_Issues_Nurs_1731/links/02bfe50da6d287566c00000/Spector-N-Kappel-DM-Guidelines-for-using-electronic-and-social-media-the-regulatory-perspective-Online-J-Issues-Nurs-1731.pdf
- The General Medical Council. (March 2013). *Making and using visual and audio recordings of patients*. Retrieved March 14, 2021 from <https://www.gmc-uk.org/ethical-guidance/ethical-guidance-for-doctors/making-and-using-visual-and-audio-recordings-of-patients/recordings-made-for-research-teaching-training-and-other-healthcare-related-purposes>
- Tran, K., Morra, D., Lo, V., Quan, S. D., Abrams, H., & Wu, R. C. (2014). Medical students and personal smartphones in the clinical environment: the impact on confidentiality of personal health information and professionalism. *Journal of Medical Internet Research*, 16(5), e132. Retrieved April 13, 2019 from <https://www.jmir.org/2014/5/e132/pdf>
- University of British Columbia. (n.d.). *Guard it: Preventing a Privacy Breach – What are the recommended methods for sharing UBC data?* Retrieved March 4, 2021 from <https://privacymatters.ubc.ca/share-files-securely#what-are-the-recommended-methods-for-sharing-ubc-data>
- Ibid. (March 2020). *Guard it: Preventing a Privacy Breach - Information and Security Guideline: How to Encrypt Files Using Common Applications*. Retrieved March 7, 2021 from <https://cio.ubc.ca/sites/cio.ubc.ca/files/documents/resources/How%20to%20Encrypt%20Files%20using%20Common%20Applications%20Guideline.pdf> on <https://privacymatters.ubc.ca/share-files-securely>

Practice Education Guidelines for BC Privacy and Confidentiality

University of the Fraser Valley. (n.d.). *Transitory Records Schedule*. Retrieved February 28, 2021 from <https://www.ufv.ca/secretariat/records-management/official-record-schedules/transitory-records-schedule/>

University of Waterloo. (January 2020). *Records Management: TL40 – Student Work, Examinations & Theses [DRAFT]*. Retrieved March 11, 2021 from <https://uwaterloo.ca/records-management/news-watclass-updates/updated-records-classes-retention-schedules-drafts/tl40-student-work-examinations-theses-draft>

Vancouver Island Health Authority. (n.d.). *Legislation in BC – FAQs*. Retrieved March 4, 2021 from <https://www.islandhealth.ca/about-us/accountability/information-stewardship-access-privacy/legislation-bc>

Ventola, C. L. (2014). Social media and health care professionals: benefits, risks, and best practices. *Pharmacy and Therapeutics*, 39(7), 491. Retrieved April 13, 2019 from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4103576/>

Guideline Review History

Version	Date	People Responsible	Brief Description (reason for change)
1	February 2007	Authors/Editors: Carol A. Wilson (BCAHC), Barb Collingwood (BCAHC) Reviewers: Practice Education Committee of the BC Academic Health Council (Grace Mickelson, Chair)	
2	June 2012	Editors: Carrie Edge (FHA) Cheryl Zawaduk (TRU)	Update references to legislation; revise according to new template and language standards, updated references and resources.
3	January 2013	Editors: Carrie Edge (FHA) Cheryl Zawaduk (TRU) Debbie McDougall (BCAHC) Reviewers: All Working Group committee members for confidentiality agreement guidelines.	Review for template and terminology updating. Revision of guidelines related to responsibility for obtaining/submitted confidentiality agreements; inclusion of statement regarding retention of student information post-placement.
4	March 2021	Editor: Carol A. Wilson (PHSA) Reviewers: Judy Lee (KPU) BJ Gdanski (PHSA) Ministry of Health (Allied Health Policy Secretariat and Nursing Policy Secretariat) Ministry of Advanced Education, Skills and Training (Health Education Reference Committee) Health Authority Practice Education Committee	References updated Updated definitions. Clarifies processes. Added details that reflect challenges of technology. Updated to reflect ways of accessing, collecting, using, and disclosing information through technology Included guidelines related to recording of clients for academic purposes Included transitory records. Referred to processes for records management Separated out responsibilities of the PSI Educator and the Student. Added HCO Supervisor/Worker roles and responsibilities