

Sample Privacy Agreement for Trustees Protection of Personal Health Information

I, _____, as an individual employed by or providing services on behalf of the Trustee organization, (this can include an: employee, practitioner staff member, volunteer, student, contractor, etc.) understand that I may have access to personal health information (PHI) in order to provide services or perform functions related to my job duties.

I understand that *The Health Information Protection Act* (HIPA) provides a duty for trustees, and those working for the trustee, to protect PHI through the implementation and compliance with appropriate safeguards (ex. access restrictions, locked filing cabinets, offices and storage rooms, passwords and encryption).

PHI can be in many different forms (this includes: electronic, printed or spoken form) and is defined by HIPA as:

“With respect to an individual, whether living or deceased: The physical or mental health of the individual; any health service provided to the individual; the donation by the individual of any body part or bodily substance or any information derived from the testing or examination of a body part or bodily substance of the individual including information collected in the course of providing health services or incidentally to the provision of health services to an individual and registration information.”

Examples of the type of PHI I may have access to includes, but is not limited to, information related to an individual’s radiology and lab results, operative reports, patient and family history, prescribed medication, physician’s orders, nursing notes regarding diagnosis, treatment and complications, etc.

As an individual working for the Trustee organization with the ability to collect, use, disclose modify or delete PHI, I understand that I am obligated to adhere to the Trustee organization’s policies and procedures related to the protection of PHI in compliance with HIPA. This includes, but it not limited to the following:

- I understand my obligations under HIPA and the HIPA Regulations to ensure the privacy and security of PHI;
- I understand I must complete privacy training, as directed, and review and sign the most current Trustee organization privacy agreement or any other agreements;
- I understand that HIPA prohibits unauthorized collection, use and disclosure of PHI;
- I will only collect, use, and disclose PHI required to complete my duties on a need-to-know basis, meaning I will only collect, use or disclose information needed for the purposes or services I am providing to the Trustee organization;
- I understand that viewing PHI without a need-to-know is considered an inappropriate use and includes looking up information on myself, my family members, friends, co-workers etc. for any personal reason (ex. curiosity, address list, birthdates);
- I understand that talking about PHI with an external party without a need-to-know, is unauthorized disclosure;

- I understand that talking about PHI with other individuals employed by the Trustee organization without a need-to-know, is unauthorized use;
- I understand that the data minimization principle must be considered when collecting, using or disclosing PHI for an authorized purpose to ensure only the information necessary for that purpose is shared;
- I understand that I need to obtain a patient's consent to disclose information to a third party, unless there is a legislated requirement to disclose without consent;
- I understand that all PHI I gain knowledge of while conducting my job duties for the Trustee organization must not be divulged under any circumstances and will I not discuss about such information in public areas (ex. elevator or washroom) or with any person unless legally entitled to do so;
- If I do not know if the collection, use or disclosure of PHI in a specific circumstance is appropriate, I will seek guidance from appropriate personnel (ex. supervisor, privacy officer)
- I will not in any way divulge, copy, release, sell, loan, review, alter or destroy any PHI except as authorized within my duties with the Trustee organization;
- I understand that I have no rights of custody or control of any PHI held by the Trustee organization;
- I will not dispose of any documents containing PHI in the garbage or recycling, and will ensure secure disposal in accordance to the Trustee organization's retention and destruction policies and procedures;
- I understand that my access privileges to systems, databases or other applications that contain PHI are subject to monitoring/auditing if deemed appropriate by the Trustee organization in order to protect and maintain the integrity of the Trustee organization resources and PHI;

I understand that I am liable for all activity completed under my assigned Trustee organization devices (computers, laptops, smartphones, tablets, etc.), systems (databases, electronic medical records, etc.), login credentials or other tools (access cards, keys, etc.) that have been provided to me, to access PHI for the performance of my job duties and that they must never be shared with others under any circumstance.

- I agree to use the PHI I have access to on the Trustee organization computer or mobile device solely on a need-to-know basis to fulfill my duties with the Trustee organization;
- I will not use my access privileges or devices to disclose PHI, by texting, taking pictures or through the use of social media;
- I will not share or allow another person to use my Trustee organization login credentials or devices which may provide access to PHI and is strictly prohibited;
- I will report any suspicious behavior or unauthorized use of my login credentials or devices and any unauthorized use or disclosure of PHI;
- I will lock or log off my computer and mobile devices immediately when not in attendance;
- If I create or print any documents, I will do so in a location that is secure from unauthorized disclosure and will securely destroy documents in accordance with the Trustee organization policies and procedures, when no longer required;
- I will ensure compliance with HIPA, privacy legislation and Trustee organization policies and procedures if I am required to use an external mobile device (ex. portable device, smartphone, etc.) to store PHI;

- I agree to abide by the Trustee organization policies on acceptable business and personal use of the internet, email and mobile devices;
- I understand that should I be required to remotely access PHI, I will only do so when authorized by the Trustee organization and with necessary safeguards to protect against unauthorized access. I understand that remote access of PHI will be logged and can be subject to monitoring and audit.

Failure to comply with this Agreement, HIPA and the Trustee organization’s policies and procedures, can result in:

- disciplinary action, in accordance with the Trustee organization’s disciplinary policy, including access suspension, employment suspension or termination;
- legal action by affected individuals;
- a complaint forwarded to the individual’s regulatory body;
- an investigation by the Saskatchewan Information and Privacy Commissioner; and/or
- a referral of the matter to the Ministry of Justice, Public Prosecutions Division to determine if an offence has occurred and could result in penalties and fines.

I understand that my obligations to protect PHI that I have gained knowledge of during my employment with the Trustee organization, as outlined in this Agreement will continue after any termination or resignation with the Trustee organization and all PHI must be returned to and remain in the custody of the Trustee organization.

Individual Signature	Department/Position	Date (mm/dd/yyyy)
Witness Name (first, last)	Witness signature	Date (mm/dd/yyyy)