Health PEI

Data Privacy and Security: January 2025

Safeguards for Health Leaders

Health PEI is responsible for appropriately using and protecting the data we collect, analyze and distribute so that the privacy and confidentiality of patients, clients, residents and employees is maintained.

Nature and Purpose of Data Collection and Analysis

The collection of *personal information (PI)* about Health PEI staff and *personal health information (PHI)* about patients, clients and residents contributes to managing our workforce and to our inventory of health data. Analyses and evaluation of this data provides us with the information necessary to make data-led decisions which improve our health care system.

Governing Legislation

Health PEI safeguards all PI and PHI in its custody and control. The *Health Information Act (HIA)* and the *Freedom of Information and Protection of Privacy Act (FOIPP)* establish rules for the collection, use and disclosure of PHI and PI respectively.

Duties and Responsibilities

Health leaders are responsible for ensuring that patient and employee information is kept safe and confidential; this includes ensuring that staff who have access to data that may include PI and/or PHI (e.g. HR information systems, patient level reports, dashboards, data tables, bed-boards) are aware of governing policies, protocols and best practices. These include the *Privacy and Protection of Personal Health Information* Policy, and the *Privacy Breach and Complaint Management Protocol* (in development). A privacy breach has occurred when PI and/or PHI is collected, used or disclosed without authorization, or is lost or stolen.

Best Practices for Data Collection, Access, Analysis and Distribution

Be familiar with and practice the following key behaviours:

- ✓ Avoid over-collection; only data needed for the intended purpose should be collected
- ✓ Always use de-identified, aggregated or encrypted data when possible; use identifiable data (data from which an employee's or patient's identity may be learned) only when necessary to complete the work
- ✓ Only those staff who require access to PI and PHI for their work should be granted such access
- ✓ Staff who are granted data access must be made aware of governing legislation and privacy best practices

- ✓ Data analyses, reports, etc., should only be shared using secure methods (*i.e.* internal government email, Serv-U application available through ITSS), and only with those who require the information to perform their work
- ✓ Ensure the correct fax number is used when transmitting data/information electronically, and include confidentiality statements

Best <u>Physical</u> Practices for Data Privacy and Security

- ❖ Safeguard PI and PHI when out of the office or facility:
  - Do not leave laptops, phones, electronic media, or paper reports in your motor vehicle
  - When traveling by air do not store your laptop in the overhead bin or in checked luggage
  - Keep a record of data repositories or reports which are being transported
  - Do not take laptops or phones outside of the country unless authorized by IT Shared Services

Report stolen devices (laptops, cell phones, etc.) <u>immediately</u> to police and to ITSS Security by contacting the Service Centre

- ❖ Safeguard PI and PHI in oral form:
  - Use private areas to discuss employee and patient information with colleagues; use low volume and/or white noise when others are nearby
  - Do NOT engage in conversations about patients or their PHI with family, friends, etc., unless there is consent or authorization to do so

- ❖ Safeguard PI and PHI in print form:
  - Keep your computer, desk, file cabinet and office doors locked when you leave the area; do not leave printed information out in the open or unattended
  - Ensure the paper chart or computer monitor is not visible to others when confidential information is displayed; purchase a privacy screen if necessary
  - Place fax machines and printers out of the reach and sightlines of public areas
  - Avoid printing unless absolutely necessary; when printing is required, use the locked print function when printing to shared printers
  - Use confidential shredding /secure destruction (with RIM approval) when disposing of sensitive records

Report any privacy breaches or suspected breaches <u>within 72 hours of occurrence</u> by entering a PSMS incident

Best Virtual (IT) Practices for Data Privacy and Security

- Safeguard passwords:
  - Change your password immediately if you think someone has inappropriately accessed your account, and report the access or suspicion to the *ITSS Service Centre* at *servicecentre@gov.pe.ca*
  - Keep usernames and passwords confidential; never share passwords with anyone, write them down or save them to your internet browser
  - Use strong passwords, ensuring unique letter and number combinations. Preferably use a password manager (available through IT Shared Services)
- Saving, access and distribution:
  - If you must save data locally, save data reports to network drives, never to the desktop or to the document/downloads folder of your computer or work phone. Do not store data files on external electronic media (*i.e.* USB sticks, external hard drives)
  - Try to access reports through one of the web-based analytics platforms (*i.e.* Posit Connect, Business Objects Environment) rather than downloading local report files
  - Do not access sensitive information through your own personal devices
  - Do not send any information to private email addresses (e.g. Gmail, Hotmail or Yahoo)

A written **Data Sharing Agreement (DSA)** is typically required to be in place prior to PI or PHI data sets being shared with an external third party. Such an agreement will clarify the rights and obligations of all parties in a data sharing activity and therefore ensure compliance with the *HIA* and *FOIPP Acts*. **If you are unsure of whether a DSA is in place and/or required, contact the ATIP team**.

Helpful links

Guide to the Prince Edward Island Health Information Act

Information Security Guide for Employees (Government of PEI)

For More Information

Health PEI's **Access to Information and Privacy (ATIP) team** provide training and resources related to privacy and confidentiality across all Health PEI services.
Email: healthprivacy@ihis.org
Phone: 902.569.7734

Health PEI's **Health Analytics team** supports our electronic health systems by providing data products which use aggregated and/or de-identified data.

Email: healthinformation@ihis.org