Health PEI

Privacy and Access Odds & Ends: Data Safeguards Edition

Why are Safeguards Important?

- IT'S THE LAW! Personal Health Information (PHI) and Personal Information (PI) are two types of data that we see most often in our work for Health PEI. 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.
- Individuals have a legal right to privacy and our patients have an expectation of confidentiality when accessing our services. The use of effective safeguards is one way we protect their privacy and maintain trust.
- As Health PEI staff, we entrust the organization with our PI, including our contact information, social insurance numbers, and employment history. We expect our employer to keep our information safe and confidential and the use of safeguards helps ensure our information is protected.
- Per the FOIPP Act, other types of data we work with may require protection as well.

How Can **YOU** Help?

- We are all responsible for keeping the data we work with safe. Here are some ways you can help:
    - Familiarize yourself with the best practices in the column on the right and make them a part of your regular routine.
    - Visit the ATIP page on the Staff Resource Centre and review the training videos and other helpful resources related to privacy.
    - Regularly review Health PEI privacy policies and protocols, which can also be found on the Staff Resource Centre.
    - Enter all privacy incidents into the Provincial Safety Management System (PSMS) so they can be managed properly.
    - Consult the ATIP team for guidance anytime at healthprivacy@ihis.org.

BEST PRACTICES

- Save all data to network drives; **NEVER** save data to the hard drive of your computer, such as on the desktop or in the documents or downloads folders.
- If transporting your work computer or paper files to and from different worksites or your home, avoid leaving them in your motor vehicle.
- If you absolutely must leave your work computer or paper files in your motor vehicle for a short time, place them in the trunk, preferably under cover, and ensure all doors are locked.
- When transporting paper files, ensure you've signed them out of the originating facility or keep a record of which files you are transporting.
- When sending information electronically, such as by email or fax, include confidentiality statements, confirm you have the right address or phone number before sending, and confirm receipt.
- Keep office doors, desk drawers, and file cabinets locked.
- Ensure records are not left open on desks or left unattended in boardrooms or other common areas.
- Keep your usernames and passwords confidential and use unique passwords with combinations of letters, numbers, and special characters.
- Utilize privacy screens on your computer monitor or position your screen away from others.
- Lock your computer if you are stepping away from your workstation or set up an automatic timeout.
- Utilize the locked print function when printing to shared printers.
- Discuss sensitive information in private areas.
- Be mindful of the volume of your voice while on the telephone in common areas and use a private setting for calls discussing sensitive information.
- When participating in virtual meetings at home or in open office areas, use a headset.
- If disposing of records containing identifying or sensitive information (with approval from the RIM team), use confidential shredding or other secure destruction.