Best Practices for Transporting Personal Information (PI) and Personal Health Information (PHI) Outside of the Office

This resource provides public bodies with guidelines when transporting personal information and/or personal health information outside of the office. It outlines administrative, physical and technical safeguards that should be considered in order to protect that information.

APRIL 2020

Office of the
Saskatchewan Information
and Privacy Commissioner

PURPOSE

These best practices are for people who transport personal information (PI) and personal health information (PHI) outside the office or work from home. It is important to remember that all government institution, local authority and health trustee employees have a statutory duty to protect PI and PHI. The duty to protect can be found in section 16 of *The Health Information Protection Act*, section 24.1 of *The Freedom of Information and Protection of Privacy Act*, and section 23.1 of *The Local Authority Freedom of Information and Protection of Privacy Act*. There are three types of safeguards to keep in mind when protecting PI and PHI: administrative, physical and technical. In order to protect PI and PHI, a multi-layered approach is required utilizing a combination of all three types of safeguards.

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards include written policies and procedures, annual training for employees, confidentiality agreements, agreements with Information Management Service Providers (IMSPs), auditing programs, records retention and destruction schedules and access restrictions. The following are some administrative safeguards to consider when transporting PI and PHI outside of the office:

- Ensure you are following your organization's IT Acceptable Use policies.
- Set up periodic audits and reviews of the databases to monitor the databases being used.
- De-identify information wherever possible, including removing information like addresses, names, unique identifiers (i.e. health services number), birthdates, phone numbers, etc., that would help identify the individual.
- Have training that will help employees with identifying emails that may contain malicious links or attachments.
- Make sure you discuss with your family not to go into your workspace and use or view your phone, laptop or computer, and files.
- Understand and follow policies, procedures, and guidelines set up by your organization for using files outside of the office.

PHYSICAL SAFEGUARDS

Physical safeguards are physical measures used to protect PI and PHI and related buildings and equipment from natural and environmental hazards and unauthorized intrusion. Physical safeguards include locked filing cabinets, offices and storage rooms, alarm systems and clean desk policies. The following are some physical safeguards to consider when transporting PI and PHI outside of the office:

- Take the least number of files or documents from the office as necessary to carry out your job duties. Sign out files that you are taking and the purpose, so that supervisors can keep track of it. For example, if you are meeting with three clients outside the office, only take the information from the client files that are needed for you to meet with the client.
- Have secure storage that is approved by your organization for your files that are outside of the office and are being transported from place to place.
- Do not leave files in vehicles unattended.
- Secure workspaces and devices at the end of the day or when not in use. Make sure there is a place where you can have your work and devices locked up.
- Immediately report devices or other work materials that are either lost or stolen to your Privacy Officer and the police if necessary.
- Do not leave laptops, computers, documents, or anything containing sensitive information unattended.
- Make sure no one can see your work or hear you discussing your work while you are out in public or around other people.

TECHNICAL SAFEGUARDS

Technical safeguards are using technology to protect PI and PHI including controlling access to it. Examples include user identifications, passwords, firewalls, and authentication controls, virus scanners and audit capabilities in digital systems. The following are some technical safeguards to consider when transporting PI and PHI outside of the office:

- Use only authorized devices for business use and not personal devices.
- Do not share devices or passwords with other people like family or friends.

- Make sure you have strong passwords for your laptop and mobile devices. If you are unsure about how strong your password is, use this tool to measure the strength of your password: https://www.my1login.com/resources/password-strength-test/.
- Set up multilayers of pop-ups, passwords, and logins to help with authenticating the users for data while working at home. One should have to go through a few layers of logins, and pop-ups to get into different databases.
- If you must save information on your device, make sure that it is encrypted and is deleted from the device when you are done using it and once it is properly saved to your work computer network.
- Use encryption for emails, laptops, and other portable devices.
- Enable the wipe down function of devices that will wipe them down if they are stolen. This is software that allows you to erase all the data from your device so that any confidential information will not end up in the wrong person's hands.
- Do not download other applications or software unless you have the approval from your IT Department or employer.
- Do not click on links or open attachments in emails that you think are suspicious.
- Work with your IT Department to make sure that the device's software is up to date.
- Use only work emails and not personal emails for business use. Keep personal emails totally separate.
- Use firewalls, anti-virus, malware, and spyware software. If you are not sure if these are up to date, check with your IT Department.
- Use only approved means of storing information that has been approved by your employer and IT Department. This could be phones, USB sticks, hard drives, laptops, or remote access to your network drives.
- Lock computers when not in use and log off anytime you are temporarily away from it.

CONTACT INFORMATION

Office of the Saskatchewan
Information and Privacy
Commissioner

1801 Hamilton Street
Suite 503
Regina SK S4P 4B4

Phone: 306-787-8350
Toll Free: 1-877-748-2298
Email: intake@oipc.sk.ca

www.oipc.sk.ca