TOP 10 INFORMATION PRIVACY & SECURITY FUNDAMENTALS BEST PRACTICES

1. **ALWAYS lock your screen when you are away from your computer. (“Windows Key + L” or "CTRL+ALT+Delete" then "K”).**

2. **LOCK YOUR SCREEN to make it difficult for casual visitors at your desk and in your office to read the content displayed on your computer monitor.**

3. **Ensure that your computer has a SCREEN SAVER that activates after a predefined time and requires a password to reactivate.**

4. **PASSWORDS should not use acronyms, birthdays, sequential numbers, names of family members or pets, etc. and they should not be written down.**

5. **EVALUATE YOUR SURROUNDINGS when discussing sensitive personal information in earshot of other staff or clients.**

6. **KNOW TO WHOM YOU ARE DISCLOSING INFORMATION; it may be necessary to verify with a third-party or call back using the listed number for that individual or organization.**

7. **DO NOT FORWARD SENSITIVE MATERIALS to your personal email address or email personal information among coworkers in the office.**

8. **NEVER LEAVE your laptop/smart phone or similar items in view in the car or UNATTENDED when travelling.**

9. **IF YOU PRINT SOMETHING, RETRIEVE IT IMMEDIATELY. Do not leave originals in photocopiers or fax machines. All sensitive waste should be placed in secure shredding devices.**

10. **ROUTINELY ASSESS VULNERABILITIES in your environment and help one another become more security conscious by respectfully challenging insecure practices.**

This document is meant as a guide for you to develop you own security best practices.
It is based on a document developed for health service agencies in Ontario and is aligned with the Personal Health Information Protection Act (PHIPA), 2004.