HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

IT BEST PRACTICES CHECKLIST FOR CLINICS

This checklist is intended for clinic IT staff, vendors, or self-supporting physicians with IT experience to help identify potential security or functionality gaps in their current local clinic IT infrastructure. Areas covered are data (including private patient and staff information), hardware, network, backups and disaster recovery.

DATA

DISASTER RECOVERY

- □ **Business Continuity** – Have a business continuity plan that includes EMR software and non-EMR business-critical data or software.
- □ **Secure Off-Site Backups** – Set up a disaster recovery system using a secure off-site or cloud backup solution. Personal information stored outside of a cloud-based EMR must also be considered.

DATA MANAGEMENT

- □ **Passwords** – Protect all individual user accounts and devices used at the clinic with unique, strong passwords. Passwords for encrypted data being transported anywhere should be sent separately from the data package.
- □ **Encryption** – Encrypt all internal and portable drives that may contain personal information. Specific versions of Windows and the Mac operating system both provide built-in encryption methods which can encrypt hard drives.
- □ **Cloud Hosting** – Ensure all personal health information stored within the cloud is encrypted, password protected, and stored within Canadian boundaries. Review agreements with any cloud hosting vendors to ensure they meet clinic privacy requirements.
- □ **Audit Logs** – Set workstations or servers that allow access to personal information to log access in case it is needed to support a privacy breach or security incident investigation.

HARDWARE

WORKSTATIONS AND SERVERS

- □ **Access Rights** – Use separate Administrator accounts with all other users having limited computer and EMR access specific to their roles at the clinic. All user accounts should be unique.

□ **Hardware Requirements** – Ensure individual workstations and servers exceed the hardware recommended requirements of the EMR software and any other business-critical software used.

□ **Lockouts** – Set automatic lockouts for unsuccessful login attempts and periods of inactivity on all workstations, services and mobile devices.

□ **Monitors** – Install privacy screens for any monitors which may be otherwise visible to unauthorized users.

□ **Servers** – If the practice requires a local server to manage the network, it should be hardened and fully managed by a qualified professional.

□ **Operating System Updates** – Schedule all operating system updates during non-business hours and coordinate with your EMR vendor as needed to ensure there are no conflicts with EMR backup processes.

□ **Log Service Work** – Log all external support access and IT work done at the clinic including date, description of service and person who performed the service.

OTHER HARDWARE

□ **Disposal** – Dispose of all hardware used to store personal health information securely and ensure the physical destruction of old hard drives (including a certificate of destruction for your records). Personal health information should not be stored on obsolete hardware.

□ **Faxes & Printers** – Install printers, fax servers or fax machines in a secure location and ensure clinic is using cover sheets on all faxes to help further protect patient privacy.

□ **Mobile Devices** – If mobile devices are used on the clinic network, the mobile software should be updated regularly. Staff should be trained on appropriate security practices specific to their use.

□ **Hard Copy Data** – Any personal data printed or kept on a hard-copy document (paper) should be shredded and securely disposed of once it is no longer needed.

NETWORK

LOCAL NETWORK

□ **Firewall** – A network firewall should be in place to protect local network and machines (stateful monitoring).

□ **Network Switch** – A programmable 2-layer network switch device (business-grade) is suggested if using the Private Physicians Network (PPN).

□ **Personal Use by Staff** - Non-business use of any software or internet access should be done on a separate local network (provide a dedicated workstation/device for this or make staff use their own devices on separated Wi-Fi).

□ **Physical Access** - Disable network plugs in public areas. All server equipment should be installed in a secure location.

WI-FI NETWORK

□ **Anonymity –** The Service Set Identifier (SSID) of the network should be masked/disguised to hide organization details.

□ **Encryption** - Wi-Fi networks must have at minimum WPA2 encryption with a strong, unique password.

□ **Public Wi-Fi** – Any public Wi-Fi offered must on a separate network and internet connection from the Private Physician Network (PPN) local area network (LAN), if the clinic is using the PPN.

SOFTWARE

BUSINESS SOFTWARE

□ **Antivirus & Malware Protection** – Anti-virus and malware protection programs should be installed and configured to run automatically.

□ **Third Party Software** - Third party business software such as PDF readers or other productivity software should be scheduled for regular updates to address any security vulnerabilities they may otherwise introduce.

□ **Web Browser** - Remove any unnecessary browser add-ons or toolbars and ensure the browser is kept up to date.

DTO Resources

DTO Technical Centre	Doctors Technology Office (DTO) resources to assist with clinic IT management and the staff or vendors that support them.
Physician Office IT Security Education	Doctors Technology Office (DTO) resources for physician office IT security and privacy education including online course materials and templates.
BC Physician Privacy Toolkit	A Doctors of BC toolkit, developed with the Office of the Information and Privacy Commissioner for BC and the College of Physicians and Surgeons of BC, to assist physicians in meeting their obligations under the Personal Information Protection Act (PIPA).

DISCLAIMER

This document provides general guides and approaches only. We strongly recommend that you retain a knowledgeable and qualified professional to regularly assess and maintain your clinic's technology and support your privacy and security policy.

For more information, guidance, or support please contact:

Doctors Technology Office
☎ 604 638-5841
✉ DTOinfo@doctorsofbc.ca
🌐 www.doctorsofbc.ca/doctors-technology-office