HEALTH TECHNOLOGY

DTO Doctors Technology Office
A GPSC initiative

ELECTRONIC ASSETS MANAGEMENT GUIDE

Summary

This guide helps private practice clinics in managing their IT infrastructure in order to support their privacy and security policies. By understanding and maintaining the technology tools at your practice, you can reduce the risk of a privacy breach and the burden of managing that risk.

Why Clinics Need to Manage Their Electronic Assets

Maintaining a clear and up to date summary of clinic IT infrastructure is vital to support the privacy and security of personal health information. It allows a clinic to identify security vulnerabilities, plan and budget for the maintenance and upgrading of technology, as well as support the auditing requirements for access to clinical information systems.

Guiding Principles

1. A clinic should maintain a list of current information systems and software applications. The list includes product name and version and is updated when any change occurs. See the *Electronic Device Inventory List* and *Electronic Software Inventory List* attached.

2. A clinic should maintain a log of all IT service activity on devices or clinical information systems. The list includes service date, support staff, and basic description of work done and is updated when any service is performed. See *IT Activity Log* attached.

Asset Management Tools

The following templates provide a basic framework for tracking hardware and software inventory as well as IT service access to the clinic systems.

Electronic Device Inventory List

Use this template to track all of the hardware at the clinic which may provide access to personal information or the local network. Common items tracked are computers, mobile devices, and networked medical devices.

Assign each device a name and asset number (or use device serial #) and additionally document its type, operating system version, physical location or responsible owner, and any important notes about the device.

Software Inventory List

Use this template to track all of the software at the clinic which may have access to personal information or that is required to support the business. Common software to consider are the EMR and any additional software add-ons, anti-virus, computer operating systems, accounting and productivity software such Microsoft Office.

Document the software name, update schedule or frequency, # of licenses or other subscription details, associated hardware where the software resides (use electronic inventory list device names or asset #), and any important notes about the software.

IT Activity Log

Use this template to track all IT activity (remote or local) where personal information may be accessed such as computer workstations or other networked devices. Include all IT activity both internal and external and retain at least 2 years of records. Document the date of the service, name of staff or external contractor, confirmation of non-disclosure agreement, approval of clinic security lead, and basic description of the service performed.

Related Materials

Physician Office IT Security Guide	User-friendly guide focusing on key safeguards for private practices to ensure their compliance with regulatory requirements. Concise (35 pages) reference for technical terminology and concepts.

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.

For more information, guidance, or support contact:

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

Electronic Device Inventory List

Page #: Last Updated:

Device Name (e.g., Desktop001 or Samsung02)	**Device Type** (e.g., Desktop Notebook, Tablet)	**OS/Version** (e.g., Windows 10, macOS Mojave)	**Serial or Asset Tag #**	**Location or Owner**	**Notes** (Approximate purchase date, sufficient resources left, etc.+)

Software Inventory List

Page #: Last Updated:

Software Name	**Update Schedule** (eg. automatic, daily, manual)	**# of Licenses**	**Subscription Type**	**Associated Devices** (electronic device names or asset #s where software is installed)	**Notes** (eg, any relevant info; software purpose, costs, special considerations)

IT Activity Log

Page #:

Date (DD/MM/YY)	Staff/Company Name	Nondisclosure read/signed (Y/N)	Security Lead (Y/N)	Details