MEDICAL DEVICES AND PERSONAL INFORMATION SECURITY POLICY

1. Introduction

1.1 Purpose

Information Technology, as part of medical devices, personal computers, laptops, tablets, and other mobile computing devices, is increasingly being used in the diagnosis and treatment of patients. As these devices are used in clinical environments, Biomedical Engineering departments are either managing these devices or participating in the management of these devices in collaboration with Information Management Information Services (IMITS) and other technology services. Additionally, personal Information may be acquired, stored or accessed on these devices and hospitals have increasingly become targets for ransomware attacks Biomedical Engineering has a responsibility to ensure reasonable measures are taken to protect these devices and the data against various threats. There may also be times when Biomedical Engineering staff be required to help clinical leadership in providing sample data access logs for helping investigations into inappropriate data access. This policy is written with the understanding that in addition to current technology devices, many legacy clinical devices may require unique methods for securing the device and the personal information stored upon it.

The purpose of this policy is to provide Lower Mainland Biomedical Engineering (LMBME) staff a single reference document for device, data and personal information security.

1.2 Scope

This policy applies to all medical devices that store, potentially store, or transmit any patient information, PC's, laptops, tablets, other computing devices mobile or stationary and data storage devices (such as CD's, DVD's, portable hard drives, USB drives and SD cards) supported by the Lower Mainland Biomedical Engineering departments where the Organization's Information Management Information Technology Services (IMITS) departments do not secure the device and/or the data collected. This policy is intended for all new and legacy clinical devices.

2. Policy/Procedure.

2.1 What Devices to Secure

Determining which clinical devices need to be secured or encrypted may not always be straight forward in the hospital environment where several groups look after desktops and mobile computing devices. While most desktop and mobile computing devices are managed by IMITS, there are a significant number of clinical devices that are supported solely by Biomedical Engineering. Many of these clinical devices are unique in the hospital IT environment and may require unique solutions to secure. Additionally, the STRA & PIA process will help determine what

actions may need to be taken.

Devices found in the hospital environment fall into one of following categories but all of them shall have a Security Threat and Risk Assessment in addition to a Privacy Impact Assessment done prior to their implementation. The categories of devices are:

A. Devices purchased as a part of a medical system: These are Biomedical Engineering's responsibility to secure. Biomedical Engineering may choose to have IMITS and Technology Services to help secure these devices. However, in the best interest of efficient installations and/or expeditious repair turnaround times, Biomedical Engineering shall secure these devices so there is no delay in locking/unlocking a device or decrypting a hard drive.

B. Devices purchased through BCCSS Technology Acquisitions and supported by both IMITS and Biomedical Engineering: These devices typically have one or more clinical applications installed which are managed by Biomedical Engineering. These devices may be secured by IMITS.

However, in the best interest of expeditious repair turnaround times, Biomedical Engineering shall secure these devices so there is no delay in unlocking a device or decrypting a hard drive. Additionally, various applications are managed by Biomedical Engineering, and may require that biomedical technologists have local administrative privileges to apply application updates, add users, back up databases and perform other types of application maintenance.

C. Portable data storage devices: These are to be managed by the party that administers or operates the data acquisition system (typically, Clinical Management). This includes, USB drives used to transfer data (import/export), CD's for delivering data to the end user, backup media (this includes but is not limited to; external hard drives, CD's, DVD's, magneto-optical disk, tape drives, and other media).

2.2 Methods for Securing Personal Information

Securing personal information shall incorporate as many of the following measures as reasonably possible.

2.2.1 Physical Measures

The clinical device shall be physically secured if it does not need to be mobile, this can be via cable lock or other locking device, physically attaching the device to a stationary item

using security screws, or storing the device in a locked cabinet. Should the clinical device need to be mobile during use, if feasible it should be mounted securely on a cart and the cart must be stored in a locked room, locked cabinet, locked with a cable lock or other locking device when not in use. This is important as devices are increasingly capable of wirelessly accessing systems that contain patient information.

2.2.2 Password Protection

Passwords are the most common form of user authentication, meaning it is the most common method by which access to a system is granted. All clinical devices should require a user-id (login) and password to access the operating system. Devices attached to a hospital domain meet this requirement. Devices not being able to fulfill this requirement should be kept under strict clinical staff supervision and in locked room when not in use (eg: Xray/CT rooms, mobile medical imaging devices). Devices not attached to a hospital domain should be setup with a login and password for accessing the operating system.

Where possible, a user-ID and password for the application accessing personal information should be employed. In no circumstances should a password be posted in any printed format.

Passwords should never be set to "never expire" as there should always be an interval set to force a password expiry. However, expiration interval of passwords will need to be balanced against clinical needs and workflow.

A password is the primary method employed to protect personal information therefore, it is vital that strong passwords be used. Passwords must not be predictable or obvious and users must protect the confidentiality of the password. User ID's and passwords may not be shared for any system containing confidential information. Strong passwords can be created using the following criteria:

a) Minimum Length: 12 characters

b) Complexity: Include characters from three of following four categories:

   i) Uppercase letters (A - Z)

   ii) Lowercase letters (a - z)

   iii) Numerals (0 - 9)

   iv) Non alphanumeric special characters (for example:., !, $, #, or %)

v) Composition: Passwords and/or passphrases must not contain repeated characters. Passwords must not be the same as the user name or device name and do not use something easily guessed.

c) Age: Passwords should be changed regularly, at least annually or whenever there is any indication the system or account has been compromised. Passwords must be changed more frequently for systems that cannot enforce the four complexity requirements.

d) History: Users must not reuse previous passwords.

Examples of Passwords:

	Weak passwords
✗	cardiology
✗	123456
✗	password

	Stronger passwords
?	C@rd1ology!296
?	I likE TrumpEts for brEakfast
?	K1ch#N56pain

2.2.3 Vendor Accounts

Many vendors will have accounts for accessing systems for service; all vendor specific accounts must be secured with a strong password. Some default service passwords are searchable in the internet, default passwords must be changed to the standard password set by the LMBME Cybersecurity team. Email bmecybersecurity@vch.ca for setting passwords, accessing the password lists or for exceptions to this policy.

These passwords are confidential and are not to be shared with non-biomed staff. If there is an operational need to disclose the password for a device consult with the LMBME Cybersecurity team (bmecybersecurity@vch.ca) prior to sharing the password to minimize the need to reset all password for that model.

2.2.4 Timeouts and Lockouts

Often users walk away from their computers without locking their computer, shutting down the application or logging out of the computer. Screensavers with a password lock help prevent unauthorized access to personal information by blanking out the screen and locking the computer. Correspondingly, application timeouts help prevent unauthorized access to personal information by locking or shutting down the application.

- Screensavers with a password lock (such as Windows screensaver) blank the screen if user input has not been received for a specified time and require a password to

return to the application.

- Application timeouts lockout or shut down an application if user input has not been received for a specified time. The user will be required to login to the application again to restart the application.

Screensavers and application timeouts shall be no longer than 20 minutes. Ideally, use the shortest timeout possible to balance user experience and security. A very short time-out period can lead to user frustration. A very long timeout period can leave personal information vulnerable to exposure. Screensavers with a password lock and application timeouts should be employed where possible.

2.2.5 Data Encryption

Encryption is the conversion of data into a form that is not easily understood by unauthorized parties. Encrypted data needs to be decrypted to be converted back to a form that is understood. Decryption typically requires a password to enable the decryption process.
Password protection alone is not equivalent to encryption. For example, a password protected Excel document may still be readable using another application however an encrypted document would be garbled or completely unreadable if opened without decrypting.

Full disk encryption (FDE) is the preferred method of data encryption. This means the entire hard drive (or other media such as USB drives, CD's, DVD's, etc.) is encrypted and unreadable even if moved to another PC. The vendor of the medical device should be contacted to determine if FDE can be applied without affecting the function of the device. In cases where FDE is not possible, encryption of just the data files or folders containing personal information should be pursued. Once again, the vendor shall be contacted to confirm that data file or folder encryption is approved.

FDE or data file encryption may not be possible on some devices, in these instances, ensure that proper passwords and timeouts are applied and that the device is physically secured.

Portable data storage devices such as, USB flash drives, external hard drives, CD's, and DVD's have the potential of being lost or stolen. Personal data stored on any portable device shall be encrypted. This includes, USB drives used to transfer data (import/export), CD's for delivering data to the end user, backup media (including external hard drives, CD's, DVD's, magneto-optical disk, tape drives, etc.). If a portable data storage cannot be encrypted it must be stored in a locked cabinet.

2.2.6 Software Security Patches

Implementing Operating System and other software patches and fixes is an important part of maintaining the security of systems. Ensuring systems are patched on a regular basis helps protect against known security threats and vulnerabilities. LMBME shall:

1. Keep systems up to date by implementing patches at a minimum annually or as required.
2. Verify that critical OS patches can be applied before patching. Some vendors validate OS patches and post the approved patches on their websites.
3. Verify that all software patches are authentic and current.
4. Perform STRA activity after a substantial patch or software update has been performed.

2.2.7 Endpoint Detection and Response Software (Anti-Virus or Anti-Malware)

Endpoint Detection and Response (EDR) refers to applications that detect and remediate malware. Malware refers to any unwanted or malicious code; this includes adware, computer viruses, Trojan horses, spyware and others. Protecting a system against malware is an important part of maintaining the security of systems. Crowdstrike is the Standard enterprise EDR for FHA, PHC, PHSA, and VCHA. For devices that are not validated for use with Crowdstrike, Trend Micro is available. Contact the LMBME Cybersecurity Team for installation instructions. LMBME shall:

- Verify which anti-malware software is approved for use by the manufacturer of the system.
- Where possible, enlist IMITS to install the HA standard anti-malware software and to update virus definitions as needed.
- Where LMBME installs a non-standard anti-virus, keep anti-malware and virus definitions current by applying updates at least quarterly.

2.3 Disposal of medical devices

Biomedical Engineering is responsible for safeguarding personal information when a clinical device is decommissioned, disposed, returned to vendor or being transferred to another site. Adhere to ABCD-14-16-40003 Decommissioning of Medical Devices SOP.

IMPORTANT: Ensure a viable backup of the data exists before the device is removed from service. In the instances where the device is to be disposed, the hard drive containing personal information must be one of the following:

(1) Low level formatted
(2) Wiped using a utility that deletes the data and makes it unrecoverable
(3) Physically destroyed

If the device needs to be used at another site or returned to the vendor then the data shall be erased using a utility that makes the data unrecoverable.

2.4 What to do when a Privacy Breach or Cyber Event occurs

Should you become aware of a privacy breach (theft or loss of a device storing personal information or confidential information), immediately inform the supervisor or manager of the clinical area involved and your Biomedical Engineering supervisor. The area supervisor or manager shall immediately report this to the Information Privacy Office (IPO) and initiate and complete a Patient Safety Event Report.

The IPO will want to know the following:

- Location of theft or Loss.
- Time of theft or Loss.
- Time of discovery of theft or loss.
- Description of device stolen or lost.
- Description of the information stolen or lost.
- Contact information of staff most familiar with the information or responsible for its safeguarding.

All staff are required to report any instances of cyber-attacks or ransomware resulting in extortion immediately to management and the Information Security team at cyberincident@phsa.ca, for all Health Authorities.

3. Responsibility

The LMBME Program will:

- Ensure it aligns with the Clinical Engineering Standards of Practice (CESOP) Clinical Data and System Management service provisions objectives. Namely, sections 7.10: Clinical Data and System Management and 7.11: Disposal and Relocation.
- Ensure all LMBME staff complete the Privacy and Confidentiality course through Learning Hub every two years.
- Ensure this policy is applied to all clinical devices managed or serviced by LMBME.
- Ensure personal information on devices managed by LMBME is protected from unauthorized access and/or disclosure.

- Ensure personal and private information stored on clinical devices is protected.
- Ensure cost effective and reasonable measures are employed.
- Ensure that all new medical systems implemented have a Security Threat and Risk Assessment (STRA) completed.
- Ensure that STRA's are reviewed and updated for any substantial changes applied to the medical devices during its lifetime. Upgrades or changes may include: substantial software upgrades/patches, changes that allow remote access by vendors, changes to how or where personal information is stored, major configuration changes.
- Ensure that all new networked devices have a Privacy Impact Assessment (PIA) completed prior to implementation.
- Ensure a PIA review of any substantial upgrades or changes made to existing devices or systems. Upgrades or changes may include: software upgrades/patches, changes that allow remote access by vendors, changes to how or where personal information is stored, and changes to privacy controls, major configuration changes.
- Assess when data is transmitted across organizations, and be aware of and adhere to the Privacy, Confidentiality and Security processes and policies of the organizations involved.
- Design, evaluate and implement unique/custom solutions when typical methods of securing personal information are not viable.
- Comply with their respective Health Organization's privacy and security related policies.
- Ensure Personal Information in the Organization's custody will not be accessed outside of Canada unless specifically permitted by law.
- Follow proper medical devices disposal procedures described in LMBME's Decommissioning of Medical Devices Standard Operating Procedure SOP012. All patient data that may be stored on a medical device is to be erased and made unrecoverable.

4. Compliance

All staff members are responsible for adhering to this policy and monitoring their activities in accordance with the policy. Staff members may warn others if they observe a violation of this policy. Failure by staff to comply with this policy may result in disciplinary action up to and including termination of employment, services or privileges.

5. Supporting Documents

5.1 Related Policies

- Patch Management Process for LMBME Networked Device
- Clinical Engineering Standard of Practice for Canada (3rd Edition) – August 2014
- Decommissioning of Medical Devices

5.2 PHC-PHSA-VCH Policies

- Information Security
- Information Privacy & Confidentiality
- Reporting and Management of Information Privacy Breaches
- Management of Standard Software Patches
- Network Security Standard
- Role based Access Control
- Password Management Standard
- User ID and Password Standard

5.3 FHA Policies:

- Access Control Policy
- Privacy and Confidentiality (previously: Confidentiality and Security of Personal Information)
- Data Leakage and Loss Prevention Standard
- Information Security Policy
- Managing Privacy Breaches
- Portable Storage Devices Standard

6. Definitions

Clinical Device	Any electronic device including PC's, laptops, tablets, or any computing device, mobile or stationary, used in the diagnosis or treatment of patients. In this document the term device refers to all computing devices or data storage devices such as portable hard drives, USB drives, CD's, DVD's, etc. The terms medical device and clinical device may be used interchangeably.
Cyber Attack	Any offensive maneuver that targets computer information systems, computer networks or infrastructures for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Encryption	The conversion of data into a form that cannot be easily understood by unauthorized parties.
Full Disk Encryption	The encoding of an entire disk drive using a complex algorithm so that the drive cannot be readily read without the decoding cipher.

Health Organization or Organization	As referenced herein, is defined as Providence Health Care (PHC), Fraser Health Authority (FHA), Provincial Health Services Authority (PHSA) and Vancouver Coastal Health (VCH).
Medical System	Any computer based device, stand-alone or networked, used in the diagnosis or treatment of patients. The system may include acquisition devices, PC's, review stations and servers.
Personal Information	Any information about an identifiable individual (including, but not limited to patients, clients, residents, volunteers, students, staff, physicians or members of the public), but it does not include business contact information such as an individual's title, business telephone number, business address, email or facsimile number.
Privacy Breach	Means the loss, theft, intentional or inadvertent unauthorized collection, use, disclosure, storage or disposal of personal information in the custody or control of the organization
Ransomware	Is a form of malware designed to encrypt files on a device or system, rendering any files and the systems that rely on them to be unusable. Malicious actors then demand ransom in exchange for decryption.
Unmanaged Workstation	The term used by IMITS and NTT to refer to workstations on which users or Biomedical Technologists have local administrative privileges to manage a clinical application and/or data. This device is managed. OS updates and Endpoint Detection are managed by Biomedical Engineering, NTT or a combination.

Effective Date:	15-NOV-2023			
First Released:	22-May-2013			
Last Revised:	15-NOV-2023			
Last Reviewed:	15-NOV-2023			
Approved By:	PHC Executive Director			
Owners:	Medical Device Security Manager			
Revision History:	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
	1.3	29-Apr-2013	Issued to LMBME	Lead Technologist
	1.4	22-May-2013	Reviewed by Executive Director	LMBME Engineer
	1.5	21-Oct-2013	Add comments about upgrades	Medical Device Security Manager
	1.6	16- Dec-2013	Minor wording edits made	Medical Device Security Manager
	1.7	17-Jun-2018	Minor wording edits, added sections for security patches and anti-malware, added definitions	Medical Device Security Manager
	2.0	10 Nov-2018	Adjustments made to policy following TACC"s audit on Networked Medical Device Assessment.	Medical Device Security Manager
	2.1	10-Oct-2023	Adjustments made to policy to reflect current practices, added info for reporting cyber events, added more definitions, updated links to related documents	Medical Device Security Manager