CYBERSECURITY INCOMING INSPECTION: BIOMEDICAL ENGINEERING

1. Purpose

To define the procedure to be followed when a medical device arrives in a Health Authority and requires cybersecurity considerations prior to clinical installation:

1.1.1 When the device first arrives (initial inspection) in the Health Authority, or

1.1.2 When the device returns to the Health Authority (e.g. after repair).

Note: This procedure is to be used in conjunction with BCBME SOP012 – Incoming Inspections

2. Definitions

Acronym or Word	Definition
BCBME	British Columbia Biomedical Engineering
CMMS	Computerized Maintenance Management System, which is the database that houses all medical device records, including repairs, inspections, purchase information, warranties, parts, etc.
Demonstration (of medical device)	Demonstration of a medical device involves <u>no</u> patient contact (i.e. sales presentation)
Evaluation (of medical device)	Evaluation of a medical device may involve patient contact (i.e. evaluating a new infusion pump in a clinical setting)
Sensitive Information	Any data not meant for public disclosure and should be protected for legal/ethical reasons. This includes patient information, business information, and/or passwords.
Patient Protected Information	Is defined, in part, as an individual's name, address, phone number, age, race, sex, marital status, healthcare history, or an identifying number (MRN, Visit Number, PID, etc…). *** For more detailed information please contact your Health Authority's Privacy office ***
II	Incoming inspection ('acceptance testing') refers to the inspection procedure to be followed on all medical devices prior to being used in a clinical setting
IT	Information Technology
PC	Personal Computer
HA	Health Authority – 1 of seven organizational units within BC providing healthcare services to its residents. Made up of: VIHA, IHA, NHA, VCH, FHA, PHC, PHSA
OAG	Office of the Auditor General – performed a cybersecurity audit of medical devices in the Lower Mainland of BC. Report released Feb 9, 2021

Firmware	Unlike normal software, firmware cannot be changed or deleted by an end-user without using special programs. Can incorporate an operating system and clinical application but they are tied together and cannot be separated or updated individually. Usually upgraded as an entire package (OS and application).

3. Scope

3.1 Included:

The procedure applies to both new and used medical devices that meet at least one of the following criteria:

- Is a network-capable asset (wired and/or wireless)
- Records, processes, and/or stores sensitive information
- Supports having its password changed from the factory default

All medical devices that meet at least one of the above criteria AND BCBME supports them for their lifecycle, or by special request (e.g. Lab, FMO, etc.):

- Purchased devices
- Donated devices
- Devices on loan from vendors
- Devices on lease or rental (if applicable)
- Devices on a contract of any sort (if applicable)
- Devices in for evaluation
- Devices transferred from another HA
- Physician owned devices that are the responsibility of BCBME (if applicable)
- Devices returning to the Health Authority after being sent out for service, loan, etc.
- Research medical equipment if used on patients (HA dependent – reference specific Health Authority SOP)

3.2 Excluded:

- Medical devices in for demonstration or testing only
  - Not for clinical, diagnostic, or treatment of patients
  - Note: These devices are required to meet Health Canada and the BC Electrical Safety Regulation.
- Assets not the responsibility of BCBME
- Patient owned devices

4. Principles

- Medical devices and associated accessories, upon entering any Health Authority site, will be inspected and may require implementing cybersecurity measures/mitigations before being used clinically.
- The Cybersecurity Incoming Inspection procedure is intended to ensure that:
    - All important IT-related information is captured in the CMMS.
    - Device passwords that support being changed are changed according to your HA's policy on medical device passwords.
    - If supported the device has appropriate Anti-virus/Anti-malware software according to your HA's policy.
    - Appropriate patch management considerations are applied to the device following your HA's policy on medical device patching

5. Procedure

If you are unsure of any part of this procedure, contact your Supervisor or HA BME cybersecurity lead

Before starting this procedure ensure you have:

- Networking information if this is a network connected asset
- Device password according to your Health Authority's policy on medical device passwords

Notes prior to starting:

- TMS will automatically attach the cybersecurity incoming inspection procedure to all incoming inspection WO's for assets that meet any one of the following 3 criteria:
    1. Is a network-capable asset (wired and/or wireless)
    2. Records, processes, and/or stores sensitive information
    3. Supports having its password changed from the factory default
    - Note it can also be manually attached like any other procedure using Procedure #1135
- TMS will auto-populate some data in the procedure based on what is already recorded in the asset record (for existing assets only and not for an incoming inspection WO started as part of a new asset entry)
- Changes to auto-populated data in the procedure will be copied to the asset when the procedure/WO is saved
- Some data is being captured to fulfill OAG audit response recommendations

5.1 Cybersecurity Incoming Inspection Procedure

5.1.1 Introduction – read and select the "Confirmation" radio button when ready to proceed.

a) Contact your Supervisor or HA cybersecurity lead if you have questions or concerns

5.1.2 Passwords

a) Password Changed Date – Date selection field

i) Enter the date the device password was changed

b) If the device does NOT support password changes select the check box – "NO – Not changeable"

5.1.3 Network Information

a) Fill out the text boxes for **all** attributes in the procedure

b) For network capable devices NOT connected to a network enter "N/A"

c) When the Incoming Inspection WO is saved these will be automatically recorded/updated in the asset record

5.1.4 Wireless (WiFi) Enabled

a) Choose the appropriate radio button

i) RATIONALE: The intention is to disable/turn off all device WiFi radios if they are not in use/needed for the device's clinical function

5.1.5 Wireless (802.11) encryption protocol

a) Choose the appropriate radio button for wireless encryption protocol in use or N/A if not applicable.

5.1.6 Wireless SSID

a) Enter the SSID (wireless network name) of the wireless network the device connects to or N/A if not applicable

5.1.7 Operating System Patch Management – Select the appropriate method used for applying device patches (Currently only applicable to Microsoft Windows Operating Systems)

a) **BME-Auto** – BME responsible for patching and device automatically updates from Microsoft

b) **BME-Manual** – BME responsible for patching and they are applied manually by BME staff

c) **BME-WSUS** – BME responsible and utilizes Windows Server Update Services

i) HA specific and you may need to work with your cybersecurity lead to see if this is an option

d) **Health Authority IM/IT(s)** – Your HA's IM/IT(s) department manages OS patching

e) **Vendor Supported** – Device vendor has responsibility for applying OS patches

f) **N/A-Device not patchable** – Device does not support applying Microsoft OS patches

5.1.8 Clinical Software Application and Version – The name of the software clinical staff use for the diagnosis or treatment of patients and its version number. Usually installed on PC-based medical devices.

5.1.9 Firmware version – the currently installed version of firmware on the device.

5.1.10 Anti-virus/Anti-malware installed – name and version of software installed. If device does not support this type of software enter "N/A"

5.1.11 Notes/Comments – any free-text information that is relevant to the device's cybersecurity or clarifies data entered in one of the above fields.

5.1.12 Model/Asset needs cybersecurity specialist review – for assets/models that require more in-depth investigation to ensure cybersecurity needs are being met your HA's cybersecurity specialist can provide further assistance.

a) This field will be audited in TMS to ensure incoming inspection WO's are not orphaned and technologists receive support from HA cybersecurity specialist(s).

5.1.13 Cybersecurity Acknowledgement

a) **Passed-Completed** – The cybersecurity portion of the incoming inspection WO was completed without incident or need for further investigation/support.

b) **Passed with Exception** – cybersecurity procedure passed with noted exceptions in the Notes/Comments field (#11 above).

c) **Incomplete-Needs BME cybersecurity specialist review** – This selection is audited to ensure incoming inspection WO's are not orphaned and the BCBME cybersecurity team can work to resolve issues and support BME technologists in the area of medical device cybersecurity. Please also notify your Supervisor / BME cybersecurity lead about issues leading to this procedure being marked "Incomplete".

5.1.14 Complete the rest of the device's normal incoming inspection procedure and acknowledgement steps in the WO.

6. Reference Documents

- BCBME CMMS SOP005 – Preventive Maintenance Program
- BCBME CMMS SOP012 – Incoming Inspections

Effective Date:	05-JUL-2021			
First Released:	05-JUL-2021			
Last Revised:				
Last Reviewed:				
Approved By:	BCBME Federated Directors			
Owners:	CMMS Team			
Revision History:	**Version**	**Date**	**Description/ Key Changes**	**Revised By**
	0.1	21-MAY-2021	First Version	DBM Team
	1.0	05-JUL-2021	Approved	Federated Directors