Department of Veterans Affairs

Memorandum

Date: FEB - 3 2020

From: Deputy Under Secretary for Health for Operations and Management (10N)

Subj: Medical Equipment Running Unsupported Operating Systems (VIEWS#1353650)

To: Veterans Integrated Service Network (VISN) Directors (10N1-23)

1. The purpose of this memorandum is to reaffirm and update policy relating to network-attached medical equipment that runs an unsupported operating system (OS). Veterans Health Administration has worked aggressively in recent years to mitigate security risks associated with medical systems that run unsupported OS. Medical equipment that runs unsupported OS may continue to be operated, provided all compensating controls are in place. However, it is expected that this equipment will be upgraded as soon as upgrade paths are available from the manufacturer, or replaced by the end of its lifecycle (per published HTM Life Expectancy).

2. According to Department of Veterans Affairs Directive 6550, published June 3, 2019, "Procurement of systems with unsupported operating systems is prohibited. Unsupported operating systems are OSes that are not supported by the manufacturer and have reached the end of the OS lifecycle as published by the OS manufacturer (i.e., no further security patches will be released for the OS by the manufacturer after the OS end of life nor will be available by other methods such as extended warranty purchases from the OS manufacturer)." Therefore, if a newly acquired medical device runs an unsupported OS, the medical device vendor must provide a support plan for the device (i.e., purchase of extended warranty from the OS manufacturer, an upgrade path to a supported OS, etc.) prior to deployment of the system.

3. VISNs are responsible for the following actions:
    a. VISNs shall no longer acquire new medical equipment that runs unsupported OSes.
    b. VISNs shall ensure that cyber security controls are applied (per the Attachment) for **all** network connected medical devices. This includes legacy medical equipment that runs an unsupported OS.
    c. VISNs shall develop plans (when systems will be upgraded or replaced) to transition all medical systems that run an unsupported OS to a supported OS.

Medical Equipment Running Unsupported Operating Systems

4. Microsoft Windows has several different builds or feature pack updates associated with the Windows 10 OS. Some of these builds are already end of life and no longer receive patches from Microsoft. Where possible, medical equipment running a Windows 10 OS should use the Windows 10 LTSC (Long Term Servicing Channel) version which are guaranteed to receive patches and updates for ten (10) years after their initial release date. Additionally, where possible, VISNs are encouraged to procure medical systems that can handle automatic patching if it is running a Windows OS. Manufacturer approval of automatic patching streamlines remediation of zero-day vulnerabilities for medical equipment.

5. Questions regarding this memorandum may be directed to Ms. Megan Friel, Associate Director, Office of Healthcare Technology Management, by email at Megan.Friel@va.gov.

for Renee Oshinski

Attachment

ATTACHMENT

The VA's Medical Device Protection Program (MDPP) is managed by the Office of Information Technology (OIT), Office of Information Security (OIS) Specialized Devices Security Division (SDSD), in collaboration with VHA's Healthcare Technology Management (HTM) Program Office. MDPP encompasses: (1) security guidance, training, and outreach to VA employees, manufacturers, and external business partners; (2) evaluation of risks and identifying compensating security measures; (3) continuous monitoring of evolving cyber security threats, including ongoing impact assessments for changes made to medical device hardware or software; (4) isolation architecture to ensure security of VA networks and to verify medical devices are operating as the manufacturer intended; and (5) vulnerability management and an incident response process to remediate security breaches.

The reference table at the following link: Security Controls Reference Guide lists the specific policies and guidance that have been fully implemented. Biomedical Engineers (BME), Information Security Officers, and Area Managers should be familiar with each of the documents and understand their roles and responsibilities. Plan of Action and Milestones (POA&M) must be opened for deficient security controls that can be remediated. Security controls that the VA cannot implement due to operational constraints and liability issues will be documented as a risk in VA's current tool for risk acceptance by the Authorizing Official.

For medical devices that have an unsupported OS, below are the most relevant cyber security controls that should be met to ensure protection of this network attached medical equipment.

- Medical equipment/systems shall be isolated in accordance with Medical Device Isolation Architecture (MDIA) guidelines.
- Network-connected medical equipment/systems shall be documented with complete and accurate medical equipment data elements in the VHA Healthcare Technology Management (HTM) Networked Medical Device Database (NMDD).
- Equipment/systems shall be patched to the latest OS release approved by the medical equipment manufacturer.
- When approved by the medical equipment manufacturer, the equipment/system shall run anti-virus scanning software with updates from the VHA Medical Device Update Server.
- Follow the Medical Device Protection Program (MDPP) Vulnerability Management Standard Operating Procedure for documenting remediation of this vulnerability.