Department of Veterans Affairs

Memorandum

Date: February 13, 2015

From: Deputy Assistant Secretary for Information Security (005R)

Subj: Updated Security Requirements for Network Connected Medical Devices and Systems (VAIQ #7566605)

To: See Addressees Below

1. Consistent with my role as the VA Chief Information Security Officer (CISO), I am issuing updated security requirements and implementation guidance specifically for network-connected medical systems and devices. Information technology (IT)-enabled and network-connected medical devices and medical systems (collectively referred to as 'medical devices') directly support VA's mission to deliver the best healthcare services to Veterans. Medical device availability and security can directly impact patient care and Veterans' healthcare diagnoses, treatments, and outcomes. However, medical devices and the networks to which they connect present a unique set of IT challenges and expose VA facilities to a broader range of security and privacy risks than typical IT network servers and endpoints. To this end, the requirements and recommended best practices outlined in this memorandum, with attachments, will increase VA's security posture by further protecting VA and patient data confidentiality, integrity, and availability.

2. The Medical Device Protection Program (MDPP) Leadership Working Group identified the need for updated security guidance for medical devices connected to VA networks. In response to the MDPP recommendations, Attachment 1 provides updated information security requirements for the management of network-connected medical devices owned and operated by VA (Attachment 1).

3. These security requirements and processes apply to all VA offices and personnel responsible for acquisition, implementation, operation, and maintenance or disposal of network-connected medical devices and sets VA-wide policy for the security controls and practices to be applied throughout the medical device(s) lifecycle. These VA security requirements also acknowledge the fact that many medical devices are also subject to Food and Drug Administration (FDA) regulations.

4. VA issued a memorandum in May 2014, "Certification of Medical Devices in MDIA" (Attachment 2), that provided security guidance for medical devices connected to Medical Device Isolation Architecture (MDIA) Virtual Local Area Networks (VLAN). The May 2014 memo included a number of action items to prepare for the FY 2014 audits.

For planning purposes, VA expects to issue a memo with a similar set of action items prior to the start of the FY 2015 audits.

5. Please direct any questions regarding this memorandum to Lynette Sherrill, Deputy Director, Health Information Security Division, at (210) 692-4231 or lynette.sherrill@va.gov.

Stanley F. Lowe

Attachments:

1) Security Requirements and Procedures for Network- Connected Medical Devices and Systems
2) *Certification of Medical Devices in MDIA* Memorandum, dated May 5, 2014

Addressees:
Executive in Charge and Chief Information Officer (005)
Deputy Assistant Secretary, Information Technology Resource Management (005F)
Deputy Chief Information Officer, Architecture, Strategy and Design (005E)
Deputy Chief Information Officer, Product Development (005Q)
Deputy Chief Information Officer, Service Delivery and Engineering (005OP)
Executive Director, Quality, Performance and Oversight (005X)
Deputy Director, Interagency Program Office (005J)
Deputy Chief Information Officer, Advocate for Corporate (005C)

Updated Security Requirements for Network Connected Medical Devices and Systems

1. **Background**. These security requirements outline security practices that will help VA personnel protect devices from cyber-attack and compromise, protect VA and patient data confidentiality, integrity, and availability, and prevent clinical service malfunction or the loss of device functionality that may negatively impact patient healthcare or safety. To identify, develop, promote, assess, and continually improve medical device security measures, VA has established a Medical Device Protection Program (MDPP) in the Health Information Security Division (HISD), Field Security Services (FSS), in the Office of Information Security (OIS). The MDPP is a joint effort between Veterans Health Administration (VHA) Healthcare Technology Management (HTM) and HISD. All references to MDPP responsibilities and requirements in the document refer to this joint program.

2. **Definitions**.
   Within VA, a medical device is defined as any device that:
   - Is used in patient healthcare for diagnosis, treatment, or monitoring of physiological measurements, or for health analytical purposes;
   - Has been subject to and completed the FDA Premarket Notification – 510(k) certification – or Premarket Approval (PMA) Process;
   - Is a component of a medical device system – hardware or software – and, if modified, can have a negative impact on the functionality/safety of the medical device system

   A network-connected medical device is any medical device that is connected to the VA IT network through wired or wireless technologies.

   A network-connected medical system is any group of devices that make up a complete medical system with one or more connections to the VA network. In a medical system, multiple device components are required for the medical system to function as intended by the manufacturer/vendor.

   VHA Healthcare Technology Management (HTM) is the authoritative source for defining what constitutes a medical device and maintaining the official categorization and labeling of medical devices owned and operated by VA. VHA HTM maintains a comprehensive list of medical device systems using VA Medical Device Nomenclature System (VA-MDNS).

3. **Compliance with VA Information Security Requirements:** To support complete and accurate reporting as required by VA IT security policy requirements and the Federal Information Security Management Act (FISMA), network-connected medical devices and systems are to be considered part of the security authorization of the General Support System (GSS) at the facility which the devices are being connected. These medical devices and systems will not require a separate Assessment and Authorization (A&A) package to be completed but will primarily be documented through the OIS risk-based decision (RBD) process. The addition of

these devices to the existing GSS will also not change the existing operation and maintenance responsibilities of network connected medical devices and systems. Paragraph 6 of this document describes the criteria that must be met to allow direct connection of a device to the network. In most cases, the devices will be segregated from the VA enterprise network GSS as part of a securely configured Medical Device Isolation Architecture (MDIA) Virtual Local Area Network (VLAN). The default configuration of the MDIA ACL for these devices and systems will prohibit external access to the medical device or system, and will prohibit access from the device to other resources external to the MDIA VLAN. The security controls of the MDIA VLAN and an inventory of all the devices contained in the VLAN will be described and referenced in the security documentation and other security authorization artifacts that are maintained for the applicable GSS. In support of continuous monitoring through configuration management and change control, any modifications (e.g., addition, removal/transfer, or other changes) to the medical devices or the VLAN will need to be assessed for potential security risk impacts to the overall security of the GSS, as required by VA IT security policy, FISMA, and the risk management framework concepts contained in National Institute for Standards and Technology (NIST) guidance. Acceptance of security risks introduced by medical devices or systems can only be made by the VA Chief Information Officer (CIO), or the VA Chief Information Security Officer (CISO), and are done primarily through the Office of Information Security (OIS) RBD processes maintained by the OIS Office of Cyber Security (OCS).

The Facility Information Security Officer (ISO) is responsible for conducting the risk assessment for all IT-enabled medical devices or medical systems prior to the device being connected to the VA network. OIS will provide recommendations for any additional or tailored security controls that may need to be implemented to address major security risks introduced by a particular medical device. Each of the MDIA VLANs at VA facilities must be reviewed at least annually and assessed for compliance with VA guidelines and information security requirements. The OIS Field Security Services (FSS) Health Information Security Division (HISD) may also develop a national level risk assessment to address issues that are common across multiple MDIA implementations.

4. **Procurement of Medical Devices**. VHA Facility Directors must ensure that:
    - Procurements of medical devices, support contracts, and service contracts are developed and are executed in compliance with national security regulations, the policies and procedures defined in VA Directive 6550, Pre-Procurement of Medical Devices and the policies and procedures defined in VA Handbook 6500.6, Contract Security.
    - There exist adequate resources to manage and maintain the security aspects of all medical devices not maintained by OI&T;

- The personnel responsible for operation and maintenance of medical devices and/or overseeing contracts have sufficient and current training to adequately execute their responsibilities;
- These processes are routinely followed and updated - - - Facility Biomedical Engineers (BME) must review medical device contracts and acquisitions as directed by VA Directive 6550 to assure compliance with security standards and must work with Contracting Officers to adequately address security standards with all acquisitions and contracts related to medical devices. In the setting of VISN or regional level contracts, these responsibilities also apply to the Network or Regional Director. This directive requires the Biomedical Engineer, or an appropriate delegate, to review relevant technical operational and security requirements at the time of pre-procurement, and to review those details with their Facility ISO and Facility CIO. The document requires signature sign-off by both the ISO and CIO. For VISN or Regional level activities, these act ivies are to be done by the VISN or Regional ISO and CIO.

5. **Medical Device Inventory**. MDPP will define the required inventory data that is to be collected, updated, and maintained for network-connected medical devices. VHA Facility Directors must ensure that an accurate inventory is maintained and reported for all medical devices. VHA Facility Directors must ensure that all network-connected medical device inventory data is reported to MDPP at specified intervals. MDPP will capture and record all submitted inventory data at least once every ninety (90) days for submission to an enterprise network-connected medical device inventory database. MDPP will maintain the enterprise inventory database.

6. **MDIA Implementation.** The MDIA Work Group is responsible for developing and maintaining a standard process for isolating and securing network-connected medical devices using a protected VLAN approach to segregate medical devices from the VA enterprise network and provide limited, controlled access to resources external to the MDIA. The default setting will prohibit external access to the device, and will also prohibit access from the device to other resources external to the VLAN. Exceptions to this requirement can only be permitted through the OIS risk-based decision (RBD) process. Non-medical devices requiring isolation shall not be placed within MDIA VLAN. Special purpose equipment such as industrial control system computers and other non-medical, legacy or non-supported computers must be placed within their own separate Device Isolation Architecture (DIA) VLANs. OIS will issue a policy memo describing the approach to be followed and requirements for DIA VLANs. Biomedical Engineering is responsible for the maintenance and operation of medical devices and must ensure that any IT-enabled medical device that cannot meet the following criteria is placed within the MDIA in accordance with the most current version of the *Medical Device Isolation Architecture Guideline*:

- The device platform operating system (OS) is a version of Microsoft Windows supported by VA OIT.
- The device can join the enterprise Active Directory services domain and receive Group Policy settings.
- VA OIT personnel have all necessary access to install and maintain the full suite of OI&T endpoint security controls on the device. These controls include, but are not limited to, OS patching and automatic updates, Universal Serial Bus (USB) device access controls, anti-malware protections, hardware/software inventory and asset management agents, and host intrusion prevention software (HIPS).

VA OIT Service Delivery and Engineering will configure and maintain MDIA VLANs in accordance with the most current versions of the *Medical Device Isolation Architecture ACL Implementation Rule Set* and the *Medical Device Isolation Architecture Guideline*.

NOTE: Default access control policy for all packets that are routed into or out of a MDIA VLAN is to deny all and allow by exception. Any exceptions must have a corresponding business justification approved via the OIS RBD process.

MDPP will perform audits and technical reviews of MDIA implementations to ensure that medical devices are protected by properly configured and maintained MDIA VLANs and access control lists (ACLs). Remediation of any identified deficiency in the configuration of an MDIA VLAN or ACL must be completed in accordance with remediation timelines due to the potential security risks to the VA enterprise network and patient safety. A memo documenting required timelines for remediation of MDIA ACLs will be released by OIS no later than 30 days from the date of this memo.

7. **MDIA Configuration Management and Change Control**. The MDIA Work Group is responsible for developing and maintaining a standardized change management process for the addition/removal of medical devices to/from a MDIA VLAN as well as modifications to the VLAN ACLs. In order to ensure consistency, OIS will establish a National MDIA Approval Board that will review all ACL change requests, and resolve any issues or problems identified at the local level. Existing SDE Change Control Boards will be utilized for implementation of approved ACLs. All approved MDIA changes shall be executed in accordance with the *Medical Device Isolation Architecture Access Control List Change Management SOP.*

8. **Role-Based Training**. MDPP is responsible for working with IT Workforce Development (ITWD) on developing, delivering, tracking, and reporting on targeted medical device security training to BME, ISO, and IT personnel to ensure all parties involved in medical device protection understand their specific roles and responsibilities in executing medical device security measures. MDPP is also responsible for developing and delivering implementation presentations to medical device stakeholders on all new policy and guidance developed for medical device

security. The OI&T supervisors must ensure that OI&T field personnel, with responsibilities for supporting network connected medical devices, attend MDPP training and presentations. The facility BME or Engineering Supervisor must ensure that field personnel attend MDPP training and presentations.

9. **Medical Device Incident Response**. MDPP is responsible for developing and maintaining a process to expedite the reporting and response of compromised medical devices in order to prevent alteration of the device's function or availability. All VA personnel must report suspected security incidents in accordance with VA Handbook 6500. These incidents include adverse events, suspicious activity, compromise, or loss of functionality involving IT-enabled medical devices. Any medical device identified as being infected with any type of virus or malware is considered a compromised device/system and must be taken out of patient care services as soon as possible in order to perform full remediation of the device/system. Medical device incident response must be performed in accordance with the *FSS Medical Device Incident Response Standard Operating Procedure*. HISD will coordinate, track, and report on all incident response involving a medical device to include the participation and activities of VA-Network Security Operations Center, Facility ISOs, BME personnel, network administrators, and Enterprise Risk Management personnel.

Department of Veterans Affairs

Memorandum

Date: MAY - 5 2014

From: Acting Deputy Under Secretary for Health for Operations and Management (10N)
Deputy Information Officer, Service Delivery and Engineering (005OP)
Deputy Assistant Secretary for Information Security (005R)

Subj: Certification of Medical Devices in MDIA

To: VHA VISN Directors (10N1-23)

1. The Department of Veterans Affairs (VA) Medical Device Protection Program (MDPP) implemented the Medical Device Isolation Architecture (MDIA) in April 2010 to safeguard network connected medical devices and their associated systems. Medical systems are critical to patient care, and the safety and security of these medical systems is the shared responsibility of the Veterans Health Administration (VHA) Office of Healthcare Technology Management (HTM), VA Office of Information Technology (OIT) Service Delivery and Engineering (SDE) and Office of Information Security (OIS).

2. The MDIA provides for the secure management of medical systems on medical Virtual Local Area Networks (VLANs) and Access Control Lists (ACLs). VISN and facility Biomedical Engineering staff, as agents of the Network and Medical Center Directors, in coordination with facility Chief Information Officers (CIOs), have responsibility to ensure the active management of network connected medical systems. All medical systems connected to VA information networks must adhere to published MDIA guidance that has been jointly created by VHA HTM, OIT SDE and OIS FSS HISD. MDIA implementation for all medical systems connected to VA information networks is mandatory.

3. All 2014 OIG audit sites must certify within **14 days** of this memo that all medical systems and their associated ACLs are in full compliance with MDIA guidelines.

4. All non-audit sites must certify within **90 days** of this memo that all medical systems and their associated ACLS are in full compliance with MDIA guidelines.

5. **Actions:**
    a. The facility Chief Biomedical Engineer and the facility CIO will work jointly to ensure that all medical systems within the medical center are protected per published MDIA guidance.
    b. The Chief Biomedical Engineer at each facility will provide the facility CIO with an inventory of all medical systems and medical devices connected to the VA information network.
    c. The facility CIO will certify that the medical devices on the list are in full compliance with MDIA guidelines. If there are medical devices that are not in compliance with the published guidance, the CIO and Chief Biomedical Engineer will continue to work together to bring these devices into compliance with the MDIA guidance.
    d. The facility Chief Biomedical Engineer will certify the status of compliance by the due dates established in this memo by uploading their inventory to the following SharePoint: http://vaww.vha.vaco.portal.va.gov/sites/DUSHOM/HTM/laptopencryption/Lists/MDIA%20Certification/AllItems.aspx. The fields required to be reported in this inventory are included in the following template: (http://vaww.vha.vaco.portal.va.gov/sites/DUSHOM/HTM/laptopencryption/MDIA%20Inventory%20Template/MDIAG%20Inventory%20Worksheet.xlsx). Status of any non compliance devices will be updated on this site until all network connected medical devices are brought into full compliance.
    e. OIS FSS HISD will validate all facility certifications and provide action item reporting to OIT and VHA Leadership.
    f. If patient care will be adversely affected by the timelines outlined above, a detailed plan including rationale and the timeline for completion shall be submitted by the Medical Center Director on an OIS Risk Based Decision form: (https://vaww.portal2.va.gov/sites/infosecurity/ca/VA%206500%20Waiver%20Process%20Templates%20Approved%20Waivers/OIS%20Risk%20Based%20Decision%20Memo.docx) to Kurt Finke, Director, Office of Healthcare Technology Management (10NA9) at vafssmdi@va.gov.

6. The definition of a medical device/system includes any component(s) [hardware, software] that is/are:
    a. Used in patient healthcare for diagnoses, treatment (therapeutic), monitoring physiological measurements, or for health analytical purposes.
    b. Has gone through the FDA's Premarket Review Process (510K Certification) or,

c. Is incorporated as part of a medical device/system and, if modified, can have a negative impact on the functionality/safety of the main medical device/system.

7. OIS FSS HISD and VHA HTM will provide training/support sessions to aid field (OIT and VHA Biomedical Engineering staff) understanding and address questions. Several sessions will be scheduled and communicated to the field following issuance of this memo.

8. Guidance for implementing MDIA is available by clicking on the Medical Device Isolation Architecture link at the following location: https://vaww.portal2.va.gov/sites/infosecurity/fieldsecurity/HISD.aspx

9. For questions or additional information, please contact the VA Office of Information Security FSS HISD vafsshisd@va.gov or VHA Office of Healthcare Technology Management (HTM) at vhacohtmit@va.gov.

A. Gonzalez 5/5/14

Art Gonzalez Date
Deputy Information Officer
Service Delivery and Engineering
Office of Information and Technology

stan.lowe@va.gov Digitally signed by stan.lowe@va.gov DN: cn=stan.lowe@va.gov Date: 2014.05.06 11:42:12 -04'00' 5/6/2014

Stanley F. Lowe Date
Deputy Assistant Secretary for
Information Security
Office of Information and Technology

Joseph Dalpiaz 5/5/14

Joseph Dalpiaz Date
Acting Deputy Under Secretary for
Health for Operations and Management

cc:

VHA Facility Chief Biomedical Engineer
OIT Facility Chief Information Officer