A NEMA/MITA White Paper

CSP 1-2016

Cybersecurity for Medical Imaging

Published by:

National Electrical Manufacturers Association
1300 North 17th Street, Suite 900
Rosslyn, Virginia 22209

www.nema.org

NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of persons engaged in the development and approval of the document at the time it was developed. Consensus does not necessarily mean that there is unanimous agreement among every person participating in the development of this document.

NEMA standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest in the topic covered by this publication. While NEMA administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications. NEMA disclaims liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document.

NEMA disclaims and makes no guaranty or warranty, express or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any of your particular purposes or needs. NEMA does not undertake to guarantee the performance of any individual manufacturer or seller's products or services by virtue of this standard or guide.

In publishing and making this document available, NEMA is not undertaking to render professional or other services for or on behalf of any person or entity, nor is NEMA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

NEMA has no power, nor does it undertake to police or enforce compliance with the contents of this document. NEMA does not certify, test, or inspect products, designs, or installations for safety or health purposes. Any certification or other statement of compliance with any health- or safety-related information in this document shall not be attributable to NEMA and is solely the responsibility of the certifier or maker of the statement.

Introduction

Medical imaging devices, like all computer systems, are subject to risks that might harm the software, hardware, or data security of the device. As devices become increasingly connected to networks, security risks move beyond the system to intrusions across digital networks. Advancing cybersecurity measures within healthcare and public health relies upon a ‘whole of community’ approach, requiring manufacturers, installers, service staff and healthcare providers alike to accept shared ownership and responsibility. MITA seeks to foster collaboration such that current and emerging threats can be appropriately addressed across the life cycle of imaging devices—from design to installation through end of life.

NEMA recently published a similar white paper that identifies a set of best practices and guidelines that electrical equipment and medical imaging manufacturers can implement during product development to minimize the possibility that bugs, malware, viruses, or other exploits can be used to negatively impact product operation.

We believe the adoption of best practices and standards by manufacturers and healthcare providers presents the clearest line of defense.

Device Security

The concept of software assurance and device security is based on the premise that medical imaging manufacturers should test their devices to ensure they are functioning properly and as intended. A manufacturer initiates this process by designing threat models that describe the various use cases of the device. This is often done pictorially to show various ports, protocols, and services that are used by the medical device. Data flow diagrams take into consideration information relating to how data is received, processed, stored, or transmitted from the device.

A device can be considered secure if it defends unintended or unauthorized operation with respect to its intended environment and its intended use—as specified by its manufacturer. Building security into the device is a key concept in ensuring that the product meets high quality expectations of the manufacturer, as well as demanding standards from such regulators as the US Food and Drug Administration (FDA) and, most important, provides quality healthcare to patients. A recent Ponemon study reported that the cost of rework for software code was seven times greater than initial development work. Manufacturers embedding software assurance activities earlier in the software development life cycle (SDLC) can ensure that security concepts are built into the overall product. Some concepts involve appropriate training for software developers, standardized coding practices, and software code testing as examples.

Manufacturers should also define the means for continuous vulnerability monitoring to enable detection of patches and updates that address functionality or repair vulnerabilities that might affect a particular device, determining whether they affect the functionality and security of the device and, where appropriate, provide a validated patch. Manufacturers must validate all software changes that address cybersecurity before installation to ensure that functionality of the device has not been compromised.

A critical component of manufacturers’ cybersecurity best practices is a high priority on incident risk mitigation. User interfaces should be simple. Consider options for robust, yet rapid, multi-factor authentication, including password fields allowing long strings (more easily remembered, user generated passwords), access options for smart cards, biometric identification, multi-factor authentication, and secured near field communication.

Manufacturers should also allow healthcare providers to know the type and status of security software installed within devices, including computers, routers, and other at-risk components, as well as current status of security upgrades and software at particular risk. If devices communicate remotely using connections not covered by the healthcare provider’s firewall, they should have secure controls in place to access the network and use technology that does not compromise security.

External Security

Once installed, equipment operators should make provisions to safeguard their networked medical devices by deploying firewalls or other means to “mask out” imaging devices. Suppliers can document product-specific measures an operator can take to minimize the exposure of the imaging device embedded in the operational network.

Suppliers should close unused communication channels on their devices, such as ports or interfaces, and possibly disable auto-run features for external media. Suppliers should also pre-test the penetrability of a device in its intended operational environment to determine and document constraints operators must consider in the field.

Whitelisting mechanisms can effectively preclude execution of malware code and can be integrated into a device prior to commissioning. This approach also protects from installing and running software not foreseen as part of the manufactured medical device, thus avoiding incompatibilities with authorized clinical applications.

Virus protection mechanisms are good practice to combat (known) threats, and suppliers should ensure that virus definition and updated virus protection patterns do not affect clinical/operational functionality by conducting basic assurance testing of the imaging device. Even though virus protection might be interpreted as non-clinical functionality, updated patterns should be analyzed and validated before release in order to ensure proper function and performance of the device in terms of clinical usability.

Securing Communication

Secure communication is essential when transmitting Protected Health Information (PHI) and associated information between devices and recipients, whether internal to the organization or with external parties.

External communication should use standards in place today, such as HTTPS–TLS. Additional certificate-based authentication models can be implemented to ensure the identity of the user/system.

Digital Imaging and Communications in Medicine (DICOM) is the standard for communication and management of medical imaging information and related data and is maintained by the DICOM Standards Committee. PS3.15 of the DICOM Standard specifies security and system management profiles to which implementations may claim conformance. Security and system management profiles are defined by referencing externally developed standard protocols, such as LDAP (Lightweight Directory Access Protocol), TLS (Transport Layer Security), and ISCL (Integrated Secure Communication Layer). Security protocols may use security techniques such as public keys and smart cards. Data encryption can use various standardized data encryption schemes.

Increasingly, medical device manufacturers are being considered Business Associates (BAs) by their customers and prospective customers if their devices interact with patient data. This is an important development because HITECH placed BAs under the control of HIPAA Security Rule Part 45 of the CFR, which requires BAs to protect sensitive information, in addition to sharing responsibility for protection with the Covered Entity. This development is critical to medical device manufacturers as it defines a minimum level of security and privacy that must be met in order to comply with regulations.

The Responsible User

Most imaging modalities and all imaging informatics applications are interconnected through the hospital intranet and/or a departmental sectioned intranet. Most of these intranets are, in turn, connected to the internet, albeit with such security provisions as a firewall. Within healthcare, medical imaging was one of the earlier implementations of the ecosystem now called the Internet of Things (IoT). Most, if not all, imaging technologies rely on digital technology, software, and hardware connected to the IoT, which can also make these systems vulnerable to cyberattacks. The danger of these attacks resides not only in the disclosure of electronic PHI but in potentially compromised patient safety. Cyber-attacks can indeed interfere with the correct functioning and performance of imaging modalities and imaging informatics applications.

In cybersecurity, the axiom “an ounce of prevention is worth a pound of cure” rings true. It is much more critical to work to take a proactive, rather than a reactive, position. Prevention of cybersecurity incidents will require cyber awareness and training of personnel.

Medical imaging manufacturers and hospital IT departments share responsibility for the technical infrastructure and mechanisms to provide compliance with best-in-class cybersecurity provisions and risk-assessment tools. These include such technologies as VPN, encryption, thin client technologies, high availability IT infrastructure, data back-up mechanisms, firewalls, and meeting the requirements of such standards as ISO 80001, ISO 14971, and EN ISO 14971. However, a truly robust cybersecurity plan can be achieved only when processes for cyber prevention are clearly defined and effectively followed by staff thoroughly trained in information and cybersecurity.

Make sure to employ current best-in-class Imaging IT processes when using the cybersecurity features of imaging modalities, image and report distribution, sharing and communications (e.g., using encryption when creating CDs). Consider discussing the following with your IT department:

- Audit logs for imaging equipment and imaging informatics systems
- Change management for updating processes
- Formal participation in organization-wide cybersecurity planning
- Operational Communication processes with IT and the cybersecurity resources of the Cybersecurity Systems Officer (CSO) and Cybersecurity Information Officer (CIO) to avoid penetration-testing incidents, for example
- Incident Patient Information Process

Responsible users also include manufacturers’ field service representatives and training staff. They should be aware of their customers’ specific security requirements and abide by them. This includes obtaining prior permission from the appropriate customer IT security staff to insert thumb drives or computers into any component, if that customer’s protocols require it.

Security Program Resources

Rather than seeking to define the specific steps required for establishing an effective security program aligned with HIPAA requirements, we recommend that groups refer to the already-established security best practices, resources, and tools that can enable users to maintain effective regulatory compliance and device security.

The National Institute of Standards and Technology (NIST) Special Publications 800 Series contains a set of documents relevant to computer security. NIST 800-66 is a guide for implementing the HIPAA Security Rule.

Free Resources

- HITRUST Alliance HITRUST Common Security Framework (CSF)—The HITRUST The foundation of all HITRUST programs and services, this is a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management.
- NIST HIPAA Security Toolkit Application—intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment
- HIMSS Risk Assessment Toolkit—designed to guide healthcare organizations through the security risk analysis and risk management process. A risk assessment should be conducted to insure that budgets and other resources address and mitigate actual risks faced by the organization.
- HIMSS Privacy & Security Toolkit—additional Privacy and Security Toolkits
- HIMSS list of Security Standards and Baselines
- SANS 20 Critical Security Controls—focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with strong emphasis on what works: security controls where products, processes, architectures, and services are in use that have demonstrated real world effectiveness.
- Security Document Templates—A security management program is built on administrative controls tailored to address risks faced by an organization. Policies, standards, baselines, guidelines, and procedures document the specifics on how an organization manages security. Additional administrative, physical, and technical controls are implemented based on those policies. HIPAA requires specific documentation, and templates such as the SANS Information Security Policy Templates are available from organizations.
- HIMSS/NEMA HN 1-2013 Manufacturer Disclosure Statement for Medical Device Security was developed by MITA and members of the HIMSS Medical Device Security Task Force in collaboration with multiple industry associations, government agencies, and other stakeholders. This standard specifies a device manufacturer's model-specific description of a device's ability to maintain/ transmit electronic protected health information (ePHI) and the security features associated with the device. It also aids the healthcare provider's review and analysis of the large volume of security-related information supplied by manufacturers for medical devices installed on the provider's premises.
- NEMA CPSP 1-2015, *Supply Chain Best Practices* —a white paper that addresses U.S. supply chain integrity throughout the product life cycle. It outlines best practices that should be considered in design, manufacture, and delivery of products across the supply chain.

Resources Available to Purchase

- RSAM—A suite of applications that can assist an organization in meeting various security goals.
- Security Documentation
  - http://www.instantsecuritypolicy.com/index.html
  - http://www.complianceforge.com/

- HITRUST CSF Assessors—can assist with HITRUST CSF implementations and conduct CSF Accreditation\Certification
- Security Awareness Training
  - SANS http://www.securingthehuman.org/
  - http://www.knowbe4.com/products/kevin-mitnick-security-awareness-training/
  - NIST 800-66, “An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule”

Conclusion

Cybersecurity in medical imaging is a shared responsibility between healthcare providers and manufacturers. Imaging staff must be aware of cybersecurity threats and best-in-class practices. Processes must be defined and implemented, and the proper technology must support ultimate zero-breach cybersecurity goals. MITA, representing medical imaging device manufacturers, will continue to be a valuable resource in the field of cybersecurity standards and regulations, in collaboration with professional organizations representing medical imaging and IT professionals.

§