Strengthening medical device cybersecurity across the healthcare ecosystem

Cooperative Research and Development Agreement Report by UL and the U.S. Department of Veterans Affairs

Empowering Trust™

Table of Contents

Acknowledgements

This report is based on joint research conducted by UL and the U.S. Department of Veterans Affairs. Research efforts were led and coordinated by:

Marc Wine
Director, Technical Integration Support & Industry Liaison
U.S. Department of Veterans Affairs

Anura Fernando
Chief Innovation Architect
UL, Life & Health Sciences

Kevin Harper
Global Strategy Manager
UL, Life & Health Sciences

Special appreciation to Paul Tibbits, MD, Executive Director Office of Technical Integration, VA Office of Information & Technology for his leadership in facilitating this research and development.

Key contributors to the research and development of the report include:

Joseph C. Taglione Jr.
Portfolio Director
Cybertech Solutions & Analytics
Enterprise Portfolio Management Division
Office of Information and Technology

William Conta
Senior Technical Program Manager
Cybertech Solutions & Analytics Team
Enterprise Program Management Division
Office of Information and Technology

Julie Lybanon
Chief Biomedical Engineer
VA Medical Center Tampa, FL

David Allen
Biomedical Engineer Technician
VA Medical Center Tampa, FL

Gregory Fogelman, CCE
VISN 8 Biomedical Engineer
U.S. Department of Veterans Affairs

Chaitanya Srinivasamurthy
Technical Director, Infusion Systems
ICU Medical

Chris Tenley
Senior Engineer, IV Informatics, Infusion Systems
ICU Medical

Julian M. Goldman, MD
Attending Anesthesiologist, Massachusetts General Hospital
Medical Director, Partners HealthCare Biomedical Engineering
Founder and Director, Program on Medical Device Interoperability & Cybersecurity (MD PnP)

David Guffrey, MS, MSM, HCISPP, ITIL
Biomedical Cybersecurity Specialist
Partners HealthCare
Medical Device Interoperability & Cybersecurity Program (MD PnP)

Adam Darkins, MD
President
Empiricon, LLC

Keith McCall
CEO
KRM Associates

Abel Torres
Principal Policy Advisor
UL Global Government Affairs

Thanks to the many key collaborators of VA's Health Technology Management and Information Security Office for their leadership and contributions to enhancing medical device cybersecurity in addition to Suzanne Schwartz, Director, Office of Strategic Partnerships and Technology Innovation, U.S. FDA for providing perspectives on medical devices safety and trust in the clinical environment.

This report was developed to support the health and safety of U.S. Veterans who we thank for their service to our country.

Abstract

Connected medical devices on the internet – i.e., the Internet of Medical Things (IoMT) – are revolutionizing patient care, increasing efficiency and improving healthcare quality. Achieving clinical IoMT deployments at scale depends upon secure interoperable data networks and appropriate end-device security controls. Expanding numbers of network connected medical devices with ever-evolving functionalities present health delivery organizations (HDOs) with an existential threat of data breaches, which recent high-profile data incidents have pushed higher on both public- and private-sector policy agendas. HDO professionals tasked with assessing, monitoring and mitigating these threats must competently manage end-device and overall network security throughout the product lifecycles of these new, complex devices. They must also maintain legacy device inventories that include devices operating beyond end-of-service (or end-of-support) and relying on potentially obsolete software systems.

The U.S. Department of Veterans Affairs (VA) has large-scale IoMT device deployments that support mission-critical care delivery to growing sub-populations of the roughly nine million patients it serves annually. Between 2016 and 2018, VA addressed critical cybersecurity hygiene issues in connected medical device deployment through a Cooperative Research and Development Agreement (CRADA) with UL. VA sought to use the UL 2900 Series of Standards to review its cybersecurity procedures for connected medical device procurement:

1. Formulate a strategy for lifecycle management of connected medical devices; and
2. Help define a practically realizable roadmap for lifecycle management of cybersecurity of connected medical devices.

Faced with a shortage of qualified cybersecurity professionals, VA also sought to determine whether leveraging Certification to UL 2900-2-1, the Standard for *Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems* as part of its device procurement process would positively affect the operational efficiency of the department's multi-professional teams managing cybersecurity across product lifecycles.

Under the CRADA, a crosswalk of the UL 2900 Series of Standards against existing VA requirements demonstrated that UL 2900-2-1 could accelerate procurement. Illustrative real-time security testing of a UL 2900-2-1 Certified infusion pump on VA IT networks showed that:

1. Using third-party testing and Certification to UL 2900-2-1 allowed for enhanced product development process assessment, product security control design evaluation, security control assessment, post-market patch management and security event monitoring support that significantly strengthened VA's current pre-procurement risk assessment capabilities and practices;

2. Adopting the UL 2900 Series of Standards for use in medical device acquisition and leveraging MedFusion would enable VA to optimize the balance between network security controls and product security controls necessary to further assure lifecycle cybersecurity threat management;

3. UL 2900-2-1 could enable an HDO to fully deploy mission-critical functionalities on leading edge medical device technology (i.e. without the need for deprecating functionality);

4. Incorporating these tools into device lifecycle management would enhance communication, improve efficiency, and simplify workloads for cybersecurity professionals, thus enabling HDOs to better focus limited resources on the most significant emerging threats to patients' security and safety.

Executive summary

Overview

This report addresses the Cooperative Research and Development Agreement (CRADA) research undertaken by the U.S. Department of Veterans Affairs (VA) and UL, a global safety science company, between June 2016 and September 2018. The CRADA focused on information security and privacy protection issues for connected medical devices on health information technology (HIT) networks. Its genesis was:

1. General concern about medical devices in the context of the U.S. national capacity to protect critical information technology infrastructure, and
2. Specific cybersecurity issues VA faced with connected medical devices.

Background

Connected healthcare technologies are transforming patient care and improving population health. On the other hand, inadequate cybersecurity protection of these technologies, and the IT structures that support them, compromise patient safety and can pose unacceptable risks to public health. Stakeholders, including national cybersecurity protection agencies, medical device manufacturers, regulators, standards development organizations and HDOs, recognize how preventing, mitigating and operationally responding to these dangers require an approach to medical device cybersecurity that:

1. Traverses product lifecycles (design - procurement - deployment – disposal);
2. Uses consensus-based security frameworks, standards, and product Certifications to support systematic product assessment and management of security risks and vulnerabilities;
3. Improves procurement, expedites device deployment, expands device use cases and use environments in order to reduce cyber risk in an industry with a projected value of USD 63.43 billion by 2023, and compound annual growth rate (CAGR) of 25.2% (2018-2023)[1].

Connectivity and precision medicine

Medical devices serve many functions, not all of which require the same level of connectivity. Device-associated risks are often specific to a particular type of device, and its mode of deployment. Medical device cybersecurity must therefore cover a spectrum of devices, from stand-alone, limited-functionality technologies to smart, multi-functional devices; and it must accommodate connectivity from direct interfaces with HIT networks via wired connections, wirelessly, and procedurally, e.g., via transfer of data and software updates via USB storage devices.

Medical devices have traditionally connected to networks in hospitals or their associated clinics, but they now increasingly operate across a continuum of care locations, ranging from hospitals to patients' homes. What is now called the Internet of Medical Things (IoMT) enables these devices to operate on other networks, not necessarily ones HDOs can secure (i.e.., consumer networks). Trust in the integrity and consistency of data exchange and helping to ensure its provenance underpins developments in artificial intelligence (AI) and machine learning (ML). These enhancements to devices are further revolutionizing how connected medical devices monitor disease, aid diagnostic decision-making and assist clinical care delivery.

Return on investment (ROI) from both connected medical device deployment and AI enhancements across the continuum of care are predicated on their support of precision medicine. Assurance of secure and consistent flows of relevant, valid, accurate, and timely data has become a critical dependency in realizing this ROI. Without these assurances, many current developments pertaining to precision medicine will likely stall, and major opportunities to add value to care as well as improve population health will likely be lost. Managing cybersecurity threats to these emerging care delivery systems must address device endpoints as well as network security.

Improving connected device interoperability

Greater interoperability of connected medical devices within HIT systems helps build ecosystems of multi-directional data flows and creates new value-based applications. However, associated risks can reciprocally increase the potential for software coding defects and "bad actors" to do harm by exfiltrating protected data, interfering with command and control systems, or holding healthcare infrastructure hostage through ransomware or denial-of-service (DoS) attacks that can disrupt care. Concern over serious cybersecurity breaches, which HDOs must report, and which can have significant financial and reputational repercussions, can deter HDOs from fully deploying the functional capabilities of connected devices they have procured, thereby devaluing their investment.

Recent high-profile cybersecurity incidents involving HDOs have heightened awareness of cybersecurity intrusions via connected medical devices. HDOs, as well as the wider provider community, face unprecedented cybersecurity threats against a wide inventory of devices that are of variable age and have varying lengths of time in service (some operating beyond their end-of-support dates). Legacy devices and systems typically consist of software that is no longer supported and maintained. This can result in a multitude of unsupported software that have known security flaws. Some operating systems are not intended for long lifecycles and may not support major breakthroughs in good security practices, opening up products for bad actors to exploit.

Regulatory landscape

The rapid transition of connected medical devices into operational clinical environments has outpaced the throughput capabilities of traditional regulatory approaches. Regulators have responded by prioritizing their activities related to dynamic, post-market surveillance measures that extend throughout product lifecycles. Regulators including the U.S. Food & Drug Administration are updating guidance and are continuing to develop commensurate enforcement processes to oversee both the relatively mature "traditional" medical device

industry and the new wave of connected device manufacturers and developers. In the interim, HDOs must find logical frameworks for standards and conformity assessment approaches to protect their patients as well as their organizations. Legacy device considerations are driving HDOs toward solutions that regularize medical device procurement; support sequential development of the capacity for full and comprehensive lifecycle management of cybersecurity across their inventories of connected medical devices; and orchestrate cost-effective replacement policies for devices identified as having unacceptable risk.

Few HDOs have the size and installed base of connected medical devices necessary to evaluate the practical implications of recent cybersecurity "wake-up calls," or to critically assess enterprise-level solutions. Any viable solution should meet such requirements as posed in the U.S. Cybersecurity National Action Plan (CNAP), and involve multi-stakeholder engagements – including: HDOs, medical device manufacturers, regulatory agencies, standards development organizations, medical device testing laboratories, Certification bodies, private-sector research organizations, and federally funded research and development centers (FFRDCs).

The 2016-2018 VA-UL Cybersecurity CRADA brought together:

1. VA, an organization delivering care to about nine million veterans annually, with an installed base of 55,000 connected medical devices and the capability to implement CNAP-appropriate requirements, given the requisite assessment and evaluation tools;
2. UL, an organization that routinely evaluates more than 96,000 products across 104 countries annually. UL collaborations with the American National Standards Institute (ANSI), the Standards Council of Canada (SCC) and the Association for the Advancement of Medical Instrumentation (AAMI) to produce deployable cybersecurity standards and conformity assessment programs, including the AAMI/UL 2800: Standard for Medical Device Interoperability and the UL 2900 Series of Standards for cybersecurity that, together with complementary resources such as UL's Cybersecurity Assurance Program (CAP), can establish a baseline of cybersecurity hygiene; and
3. A multi-stakeholder group (Task Group) capable of addressing related requirements across the federal government, public and private sector HDOs, federally funded research and development centers (FFRDCs), private sector researchers, academia, device manufacturers and other organizations involved in healthcare.

Scope and methods

The CRADA's scope was to evaluate:

1. The utility of the UL 2900 Series of Standards and Certification (UL CAP) as a means of independent third-party attestation that connected medical devices used to treat veteran patients have met a baseline of safety and security requirements;

2. Whether certification to UL 2900-2-1 provides a trusted mechanism to help ensure that robust and reliable safety and security features have been incorporated into product design and can be applied to the product lifecycle thereafter for products VA procures and deploys; and

3. Areas where VA can improve defense-in-depth architectural strategies for the mitigation of network security risks through increased reliance on endpoint (i.e., product) security controls.

CRADA Methods (by task) included:

1. Review the healthcare sector's current threat landscape;

2. Assess data security and privacy standards, best practices, guidelines/conformity assessment and compliance requirements for connected medical devices against VA care delivery system and cybersecurity risk assessment processes;

3. Consider applicability of the UL 2900 Series of Standards, testing and Certification processes in relation to Task 2.

4. Conduct a comparison of requirements (crosswalk) between VA's cybersecurity compliance practices and the requirements of the UL 2900 Series of Standards;

5. Determine how UL 2900-2-1 Certification of connected medical device products could help VA meet/complement its current cybersecurity practices;

6. Demonstrate the safety and security of a UL 2900-2-1 Certified product against attack through vulnerability scanning and penetration testing of a Class II medical device.

Outcomes

Standards Review

1. Task Group insights fed into *UL 2900-2-1 Software Cybersecurity for Network-Connectable Products*, Part 2-1, which was ANSI approved on 1st September 2017 and SCC Approved 27th April 2018,. and recognized by FDA on 7th June 2018.

2. VA became a voting member on the roster of the UL standards technical panel (STP) for the UL 2900-2-1 Standard to help ensure that veterans' needs continue to be reflected in the evolving UL 2900 Series of Standards.

Crosswalk of UL 2900 against VA Directives

1. UL 2900-1 and UL 2900-2-1 and VA Directives 6500 and 6550 were equivalent across 174 indices evaluated.
2. Independent third-party testing results based on UL 2900-2-1 complemented MDS2-based manufacturer attestation in determining product-level risks.

Infusion Pump (ICU Medical Plum 360) Security Control Testing Demonstration:

1. The device could not be connected to an unauthorized "guest" network per secure design requirements.
2. The network connected device and server successfully initiated data exchange.
3. Simulated spoofing of legitimate infrastructure was blocked by the device per tested security controls.
4. A Wi-Fi de-authorization attack demonstrated no measurable effects on essential performance or normal product operation.
5. Per tested product security design attributes, the device resisted a man-in-the–middle (MITM) attack with all application data encrypted. Device-level encryption (rather than AP security) protected all potentially VA-sensitive data (except Wi-Fi keys, which were no longer relied upon to protect other sensitive data).
6. The UL 2900 Series of Standards improved communication between cybersecurity professionals, illustrating the potential for improved efficiencies in the procurement process.

UL 2900-1 and UL 2900-2-1 offered a complementary way for VA to enhance protective measures for sensitive data through greater reliance on product-level security controls, also potentially minimizing the scope of data that need to be considered sensitive, while maintaining confidentiality of personally identifiable information (PII) and protected health information (PHI).

Conclusions

The UL 2900-2-1 crosswalk with VA's procurement standards demonstrated that UL 2900-2-1 can potentially accelerate and streamline HDO procurement of connected medical devices.

Simulated attack and security control testing of the UL 2900-2-1 Certified infusion pump showed:

1. Product development process assessment, product security control design evaluation, and post-market patch management and security monitoring support provided for by testing and Certification to UL 2900-2-1 significantly strengthened HDO pre-procurement risk assessment capabilities and practices of VA.

2. UL 2900-2-1 based conformity assessment and MedFusion$_2$ balanced network security controls with product security controls, enhancing lifecycle cybersecurity threat management of medical devices for HDOs. Communication, efficiency, and simplification of workload for cybersecurity professionals were also enhanced, allowing HDOs to focus limited resources on major emerging threats to patients' security and safety.

3. The enhanced end-device security capabilities required to attain UL 2900-2-1 Certification could better enable an HDO to fully deploy mission-critical product functionalities on leading edge medical device technology, without the need for deprecation of product functionality to accommodate network infrastructure constraints.

Purpose and background

Purpose of the White Paper
Between June 2016 and September 2018, the VA and UL engaged in a Cooperative Research and Development Agreement (CRADA) on Medical Device Cyber Security Standards and Certification Approaches. A specific UL deliverable under the CRADA statement of work was to produce a White Paper on *supply chain considerations, responsible sourcing, environmental compliance and life cycle management and other topics* to disseminate lessons learned within VA, and also across the wider health care industry. This document is intended to satisfy that CRADA requirement, and to be made publicly available.

Background

Digital delivery of Veterans' care

Of a total U.S. veteran population of 19,602,316 people, 9.17 million veterans were enrolled for care from the Veterans Health Administration (VHA) in FY2018.[3] This population is older, sicker, and poorer than the general U.S. population, due to an increasing burden of chronic disease.[4] Consequently, from the late 1990s onward, VHA has transitioned elements of the care it provides from hospitals to non-institutional settings, which are more appropriate for chronic care populations. This transformation was made possible by VHA's adoption, and widespread implementation of, innovative health information and telecommunication technologies that support changing the location of care. The return on investment has resulted in increased access to care, increased quality of care, and lower costs.

The Veterans Health Administration

- In 2018, more than nine million enrolled Veteran patients received VHA care from a system comprising 172 VA medical centers (VAMCs) and 1,241 community-based outpatient clinics.[5]
- In FY2018, VA delivered 2.29 million episodes of virtual care to 782,000 of enrolled Veterans across the same continuum of care via telehealth; with 33% living in rural communities and 87,000 able to live independently in their own homes because of care coordination support via home telehealth technologies.[6]

VA clinicians who delivered both in-person and virtual services used VHA's electronic health record (EHR) system. VA's clinician uptake of its EHR system is 100%.[7] Clinicians access it via one of VA's inventory of 314,000 desktop computers and 30,000 laptops.[8] While many changes have been taking place over the past two years, at the outset of the CRADA, VHA's EHR was a sub-component of a networked portfolio of medical information systems that comprised 104 discrete computer applications, such as:

- 56 health provider applications;
- 19 management and financial applications;
- 8 registration, enrollment and eligibility applications;
- 5 health data applications; and
- 3 information and education applications.

With routine healthcare delivery to nine million veterans now dependent on these information and telecommunication systems, VA budgeted[9] $370 million in 2016 toward information technology (IT) security, and a further $50 million to create a data management backbone.

These upgrades followed a 2015 report to Congress that highlighted areas for cybersecurity enhancement and remediation within VA. This included the recommendation that VA improve its network access controls for medical devices and segregate the networks on which they reside from general networks as well as from other mission-critical systems.[10]

VA defines medical devices as: [11]

1. Technology used in patient healthcare for diagnosis, treatment (therapeutic) or physiological monitoring of patients, and
2. Having gone through the Food and Drug Administration's (FDA) premarket review or received 510K clearance.

With 55,000 medical devices connected to the department's information technology (IT) networks; a cardiac device surveillance program monitoring 11,000 patients with implanted pacemakers or cardioverters; and the provision of care for 87,000 patients in their own homes using home telehealth devices, VA has come to rely on connected medical devices as a mission-critical component for providing healthcare across the hospital-to-home continuum.[12]

The wider healthcare delivery community has been, to some extent, aware of patient safety issues related to the cybersecurity risks of connected medical devices, and some providers had begun trying to address these issues with the International Organization for Standardization's (ISO)/IEC 27000-series[13] *"Information security management systems"* and ISO/IEC's 80001[14] *"Application of risk management for IT networks incorporating medical devices."* The 2016 U.S. White House Cyber Security National Action Plan (CNAP) highlighted cybersecurity risks to healthcare critical infrastructure, and the 2017 report from the US Department of Health and Human Services (HHS) Health Care Industry Cybersecurity (HCIC) Task Force identified and elaborated upon these issues more thoroughly.[15]

As a pioneer and long-established leader in the fields of health information systems and telehealth, and one respected for its focus on patient safety, VA was aware of the mounting complexity of managing cybersecurity threats in relation to connected medical devices in an industry where 81% of HIT cybersecurity staff in surveyed HDOs stated their organizations had been compromised by cyber-attack in the previous year.[16] [17] [18] [19] [20] VA needed to proactively

address these issues and, given its unique experience in delivering such healthcare services at scale and across an integrated healthcare system, VA regularly used root cause analysis and human factors engineering to arrive at solutions. Aside from its operational imperative to directly deliver care to Veterans and coordinate elements of their care across the wider healthcare system, VA also has a research mission. VA sought a trusted partner to research key cybersecurity concerns and share lessons learned with private sector HDOs, as well.

UL is a global independent safety science company that has championed safety solutions, including Certification, testing, inspection, training and education services for technologies including medical devices since 1894.[21]

Expanding value chains to include connected devices

Having identified the threat cybersecurity poses to connected devices, and with the emergence of IoMT products, UL has partnered with service providers, manufacturers, trade associations and international regulatory authorities to develop solutions to protect the value chains of critical infrastructure sectors. Managing patient care using connected medical devices across the continuum of care constitutes a complex value chain of services supported by information and telecommunication technologies.

Building a value chain of services involving connected devices requires interoperability of the technologies involved. But, as devices become interoperable and exchange data, risks to cybersecurity become increasingly important to assess and mitigate. Having worked with AAMI on medical device interoperability in a seven-year collaboration, UL additionally saw the closely related need for cybersecurity and developed the UL Cybersecurity Assurance Program (CAP) based on the UL 2900 Series of Standards.[22] In an environment where regulatory institutions and their mandates are adapting as "industrial" era products incorporate "informational[23] enhancements," UL had tools that VA could use for practical and testable cybersecurity. These tools offered improved standardization in procurement to assess compliance of network-connectable products and systems with respect to software vulnerabilities and weaknesses, exploitation risks, malware threats, security controls, software upgrades patching, security event logging requirements and improved security awareness.[24] [25] VA and UL began working together under this CRADA in May 2016.[26]

U.S. Public-Private Collaborative Research

Under the 1986 Federal Technology Transfer Act (P.L. 99-502), which amended the Stevenson-Wydler Technology Innovation Act of 1980[27], federal agencies can establish CRADAs with outside parties. Under the conditions of a signed CRADA, a federal agency and commercial sector party undertake joint research with any licenses negotiated for patented inventions that may result and protections for intellectual property. Using this CRADA, UL would work with VHA to critically assess the administrator's cybersecurity compliance processes and controls for medical devices; disseminate relevant findings to the wider healthcare community; and consider commercialization of any resulting intellectual property.

CRADA medical device cybersecurity standards and Certification: Aims, objectives, scope, materials and methods

UL-VA CRADA Objectives

Overview

The VA-UL Cybersecurity CRADA project's aim was to improve the safety and security of Veteran patients through the use of the UL 2900 series of standards and related Certifications. The UL 2900 Series of Standards formed a specific toolset for VA to use to improve processes for managing cybersecurity risk associated with the medical device products it procures connects to a wide range of HIT systems. Specific expectations involved:

- Refining existing and emerging standards-based practices related to network connectable medical devices, medical device data systems and related health IT;
- Accelerating sharing of medical device cybersecurity information, Standards and product lifecycle requirements;
- Indicating ways to leverage new safety/security Certifications for a veteran-centric framework of trust;
- Enabling VA to raise industry-wide situational awareness of both medical device vulnerabilities and threats; and
- Finding ways to positively impact how medical device manufacturers develop and improve upon their overall cybersecurity posture in alignment with Veterans' needs.

Objectives

The CRADA focused on the following objectives:

- Supporting VA's improvement of patient safety and security through the application and refinement of how the department applies existing and emerging standards related to network connectable medical devices, medical device data systems and related health IT.
- Developing product-design-oriented metrics and evaluation techniques for cybersecurity assurance of medical devices, medical device data systems and related Health IT by using UL 2900-2-1 for these evaluations.
- Proposing refinements/improvements to UL 2900-2-1 based on these evaluations that could enhance VA's medical device cybersecurity risk assessment processes; and
- Fostering collaboration across a broad group of cross-functional stakeholders to create a learning environment across the medical device and wider healthcare industry that VA and other government organizations interact with, in order to promote sharing of cybersecurity lessons learned and standardized practices for medical devices.

Scope

With VA's inventory of more than 55,000 connected medical devices, ranging from computed tomography (CT) and magnetic resonance imaging (MRI) scanners to glucose monitors, it was not feasible for the CRADA to attempt to cover all aspects of all medical devices and their complete post-market product lifecycles. While the concepts are broadly applicable across many different medical device and technology types, the specific activities of the CRADA were performed:

1. Using a Class II medical device type,[28] specifically an infusion pump use case;
2. Addressing product development, procurement, decommissioning and other associated processes; and
3. Demonstration (simulated cyberattack) testing with the infusion pump mentioned above, suitably integrated into a VA network, from which to evaluate proposed solutions, with findings that could be extrapolated to other connected medical devices in common use throughout VA.

Materials

To further the aims and objectives of the CRADA, UL and VA employed the following resources/assets/approaches:

I. VA-UL CRADA Workgroup ("Task Group")
This inter-governmental and inter-public-sector group was created to meet on a weekly basis and identify issues, with a specific focus on the UL 2900 Series of Standards, and compare them with regulations, other standards being used, and procedural safeguards for the cybersecurity of medical devices that VA, private sector HDOs and other federal agencies were adopting. The Task Force (see Appendix 1.) consisted of:

- VA and UL co-chairs
- Representatives from VA offices:
    1. Office of Information Security
    2. Office of Information Technology
    3. Medical Technology Office
    4. Biomedical Engineering
- UL Cybersecurity Experts
- Expert Members of Private Sector Industry (Manufacturers and HDOs)
- Federally funded research and development centers (FFRDCs)
- Expert Members from Academia/Medical Device Laboratories

II. UL Cybersecurity Assurance Program
a suite of solutions that tests for software vulnerabilities and weaknesses, reduces exploitation, addresses known malware, reviews security controls, tests these security controls, and enhances security awareness and preparedness by providing:

- **Advisory Services** – Providing audits, cybersecurity compliance guidance and support for planning and design of services to protect business operations and prevent reputational damage;

- **Training** – Offering training for security readiness for product design and sourcing third-party components;

- **Testing (including discrete benchmark testing)** – Such as fuzz testing, vulnerability scanning and review, static source code and binary analysis, penetration testing and malware testing; and

- **Certification** – Testing of products, processes and systems to establish compliance with the UL 2900 Series of Standards.

III. The ICU Medical Plum 360[29] infusion pump was selected for demonstration testing to illustrate the product security attributes of UL 2900-2-1 compliant products in a representative VAMC.

The Task Group recommended installing a connected infusion pump[30]system as the representative technology "use case" for UL 2900-2-1 demonstration testing. An infusion pump is a medical device that delivers fluids, such as nutrients and medications, into a patient's body in controlled amounts, and an infusion pump was selected because this type of device is:

- Used in clinical settings including hospitals, clinics and in the home, covering a wide spectrum of cybersecurity scenarios;

- Widely deployed, with more than 2,000,000 external infusion pumps[31] in U.S. hospitals and other healthcare settings;

- Increasingly interfacing[32] with EHRs and studied for use in systems of interoperable medical devices to address patient safety concerns[33] relating to medication errors; and strategies to reduce "alarm fatigue;"

- Have been known historically to have had cybersecurity vulnerabilities[34];

- Capable of significant morbidity and mortality, if a "would be" attacker tampers with prescribed intravenous fluid regimens and associated medication delivery;

- A known source of risk because of previous adverse events and device recalls related to deficiencies in device design and engineering[35]; and

- Long-lived, needing an extended period of lifecycle management (expected lifespan = 10 years[36]).

Methods

The following five methodologies were employed for the CRADA:

1. ***Regular Task Group Meetings:*** The Task Group met weekly to:
   a. Consider the general healthcare cybersecurity environment and critically assess associated regulatory approaches, standards, industry approaches and published guidance;
   b. Review specific VA policies, standards, and practices;
   c. Understand VA's environment for cybersecurity standards (See Appendix 2);
   d. Discuss the elements of the crosswalk; and
   e. Determine the utility of UL 2900-2-1 and UL CAP compliance to VAMCs.

2. ***Crosswalk of VA Directive 6550 and Handbook 6500 with UL 2900-2-1:*** The pre-procurement assessment (PPA) process for acquisition of medical devices in VAMCs throughout VHA was governed by the 2015 VA Directive 6550[37]Risk Management Framework for VA Information Systems (6550). This policy specifies the technical PPA requirements needing verification to authorize medical devices and medical systems to connect to VA information networks; and for operating medical devices that store protected patient information.

   Under 6550, Biomedical Engineering field staff (Biomed) work with VA contracting to coordinate the technical aspects of the PPA with the VA Office of Information Technology (OIT) via the Chief Information Officer (CIO), locally or regionally; appropriate OIT offices, as well as an Information Security Officer (ISO), are involved locally, regionally or nationally for input to ensure the medical equipment under PPA review can be operated as intended in the medical facility. Biomed is responsible for ensuring completion of the PPA in collaboration with OIT, and in conjunction with the manufacturer/vendor(s). This coordination requires completing a specific PPA assessment tool, which provides information on a medical device under procurement consideration relating to its:

   - System configuration;
   - Authentication and user account;
   - Data handling;
   - Networking;
   - Wireless networking; and
   - Integration with VA Healthcare Information Systems.

3. UL 2900-2-1 Device Certification

Pre-market
Management of cybersecurity in medical devices with respect to:

- Alignment with FDA guidance[38] on premarket submissions for management of cybersecurity in medical devices[39];
- Risk Management process adherence with respect to threats, vulnerabilities and implementation and testing of security risk controls;
- Incorporation of core functions of the National Institute of Standards and Technology (NIST) cybersecurity framework[40,41]: identify, protect, detect, respond, recover; and
- Availability of traceable cybersecurity documentation for product development and deployment.

Post-market
Management of cybersecurity in medical devices with respect to:

- Ongoing full product lifecycle Risk Management;
- Supply chain Quality Management System requirements (21 CFR 820[42] and/or ISO 13485[43]) and use of Common Vulnerability Scoring System[44](CVSS) or similar approach for ongoing medical device risk management;
- Detection and root cause analysis of product failures including security breaches;
- Software patch and update management.

The crosswalk required VA Biomed, OIT, and VA ISO to work with UL's engineers and ensure the information required by 6550 aligned with the UL 2900 Series of Standards, as shown in Figure 1.

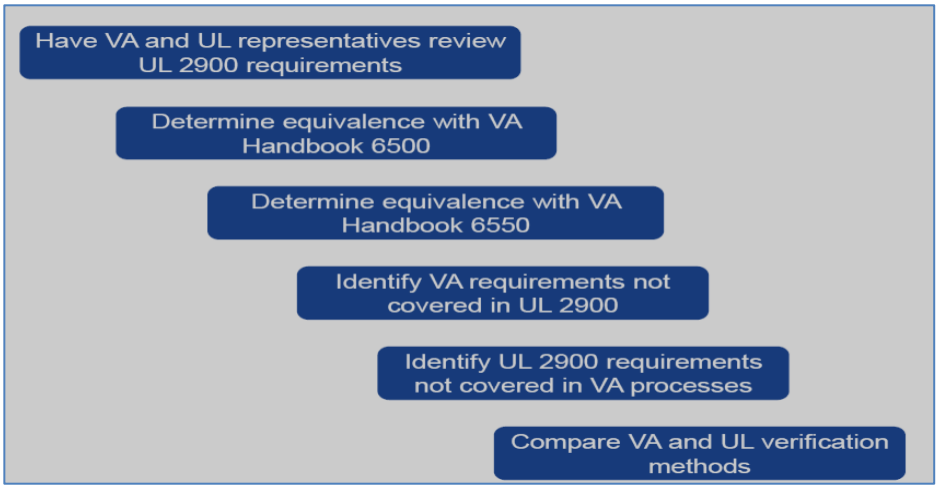

Figure 1 – Overview of CRADA crosswalk process

Some of the items discussed had “combination requirements,” which means that devices must undergo both design process verification and product testing to satisfy

conformance. The “design-level” and “process-level” requirements were those that either:

1) Needed to be tested independently to determine conformance; or

2) Could have conformance determined through an independent audit of the manufacturer’s Quality Management System and its traceable inclusion of the product-level Risk Management (RM) and Software Development Life Cycle (SDLC) processes. This could include the manufacturer’s verification testing conducted in accordance with UL 2900-2-1 during software development (and subject to periodic independent follow-up audit).

The intended outcomes of the crosswalk analysis included finding ways to: (1) facilitate easier adoption of new technologies by VA; (2) establish better channels of information flow from medical device manufacturers to VA; and (3) consider modifications to UL 2900-2-1 to not only align with pre-existing policies and requirements, but also address VA expectations and future needs in meeting its healthcare mission safely, effectively and securely.

Satisfactory conclusion of the crosswalk entailed comparing and contrasting the relationships between all elements of UL 2900-2-1 and all relevant parts of VA’s 6500[45] (Risk Management Framework for VA Information Systems) and 6550 in order to show either equivalence with UL 2900 or insufficient equivalence, in which case the adaptations needed to remediate insufficiencies should be captured for future action.

4. UL 2900-2-1 Demonstration Testing

Demonstration testing aligned with UL 2900-2-1 was intended to:

a) Understand how site-specific installation environment conditions factor into new product acquisition and deployment.
b) Determine how product updates (e.g., patches) are managed (solicited, received, deployed) and understand any site-specific considerations in this process.
c) Identify how tools such as free and public UL CAP certificates can potentially be used within current VA processes to complement existing workflows and practices.
d) Raise awareness of other tools that are used collaterally with UL CAP, such as the ICS-CERT database and coordinated vulnerability disclosure (CVD) scheme for newly discovered medical device vulnerabilities listed in the NIST National Vulnerability Database (NVD) that has been adopted by the International Telecommunications Union (ITU). ICU Medical Plum 360 infusion pump, the first UL 2900 Certified medical device, along with the manufacturer’s MedNet drug library server, were used to successfully demonstrate how VA-sensitive data is protected when using the security controls and defense-in-depth strategies of the UL 2900 Series of Standards.

The demonstration comprised two parts:

Part 1 - Pre-test Site Review Tasks:

1. *Discussing whether site-specific factors could influence new product acquisition and deployment using UL CAP versus usual* VA process;
2. Determining processes for managing routine software version upgrades and urgent patches into the demonstration testing process, and identifying whether these would be subject to influence from any site-to-site variations across VA; and
3. Assessing whether additional tools, e.g. free and public UL CAP certificates, could enhance existing cybersecurity workflows and practices in VA.

Part 2 - Demonstration Testing Steps:

1. Successfully place an ICU Medical Plum 360 infusion pump[46] in a "patient environment" and connect it to an ICU Medical MedNet drug library server;
2. Attempt installation of the ICU Medical Plum 360[47] infusion pump onto an unsecured "guest" network[48];
3. Connect the installation of the ICU Medical Plum 360 infusion pump and associated MedNet Server onto an authorized and secured VA network[49] and initiate communications between the system components (including transfer of dummy drug library data);
4. Connect a test computer (i.e. representing a malicious user) to the same wireless access point as a simulated spoof of legitimate infrastructure;
5. Demonstrate that all components of the ICU Medical Plum 360 infusion pump system under testing could be removed from the Wireless Access Point via denial-of-service attack with minimal disruption of service, and rapid operational recovery (i.e., infusion continues, without noticeable disruption, as intended for the given patient);
6. Conduct a man-in-the-middle-attack and demonstrate encryption of exfiltrated data to prevent patient privacy loss;
7. Use multiple tools to capture data exchanges and demonstrate that all application data is encrypted (including analysis of various data packet types to verify encryption of all potentially VA sensitive data [except Wi-Fi key]); and
8. Explain to VA staff how the additional penetration testing, malware testing, fuzz testing, etc., conducted to Certify the infusion pump to UL 2900-2-1, helped prevent compromise of VA sensitive data based on the pump's compliance with security controls and defense-in-depth strategies required for UL 2900-2-1 Certification.

5. **Assessment of Human Factors:** In the prior four methodologies used, information was gathered, observations made, and inferences drawn from workflows and associated organizational arrangements. Also, the roles and responsibilities of individual staff designated for medical device cybersecurity and the organizational structures they operated under were pertinent areas for potential "systematic" security defects that UL was able to address.

Findings, results and direct outcomes of CRADA research activities

Outcomes – Results and findings

Standards review

1. Insights from the Task Group review of standards and assessment of VA's policies, procedures and processes were primarily directed toward the subsequent crosswalk and demonstration testing but proved valuable to UL in the subsequent stages of development of *UL 2900-2-1, the Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*, which was ANSI approved on 1st September 2017 and SCC approved 27th April 2018. and recognized by FDA on June 7th, 2018.

2. VA was added to the roster as a voting member of the UL standards technical panel (STP) for UL 2900-2-1 to help ensure that Veterans' needs continue to be addressed as the UL 2900 Series of Standards evolve to keep pace with the changing cybersecurity threat landscape.

3. Crosswalk UL 2900 series of standards against VA Directives 6500 and 6550:
    a. Equivalence was agreed upon between the UL 2900 Series of Standards' requirements and VA Directives 6500 and 6500 across 174 requirements evaluated, and reviewers also established that UL 2900 addressed product design security issues (both product capabilities and limitations) not currently addressable through existing VA pre-procurement vetting.

    b. The crosswalk demonstrated VA Directive 6500 corresponded closely to the Manufacturer Disclosure Statement for Medical Device Security (MDS2) that provides information regarding security-related attributes of the product, and not necessarily the security risks associated with them. Certification to UL 2900-2-1 requires enumeration of product security attributes followed by test-based evidence gathering:

        1. Weakness and vulnerability scanning
        2. Evaluation of product source code
        3. Analysis of software bill of materials that requires testing such as static analysis
        4. Software composition analysis (SCA)
        5. Dynamic application security testing (DAST)
        6. Interactive application security testing (IAST) comprising structured penetration testing
        7. Fuzz testing

This process provides UL 2900-2-1 Certified end users with further insight, beyond the MDS2, into product security risk.

Outcomes from the infusion pump demonstration testing

1. The device was incapable (per secure design requirements) of connection to unsecured “guest” network due to design attributes protecting it from rogue (i.e. spoofed) access points (APs).
2. Network connected device and server successfully initiated data exchange between system components (including a dummy drug library).
3. Simulated spoofing of legitimate infrastructure was blocked by the device.
4. Device and system components could be removed from the AP via a de-authorization attack, but with no measurable disruption to Essential Performance or overall normal product operation coupled with very rapid (almost undetectable) operational recovery.
5. Device resisted a man-in-the-middle (MITM) attack to capture data (encryption of all personally identifiable information (PII) and protected health information (PHI) occurred at the device level rather than relying on AP security measures).
6. The device provided encryption of all application data, demonstrated through packet capture and analysis of various data streams, ultimately showing encryption of all potentially VA-sensitive data (except Wi-Fi keys, deemed non-sensitive due to confirmed encryption of underlying sensitive data via additional layers of protection).

In summary, the UL 2900 Series of Standards offered VA a complementary way to protect its sensitive data through greater reliance on product-level security controls, also potentially minimizing the scope of data requiring sensitive status designation, while maintaining confidentiality of PII and PHI.

Discussion

A viable cybersecurity strategy for an HDO cannot restrict itself to single-point protection and must consider “defense-in-depth” measures. Technical documentation review by an HDO cannot, in itself, ensure security: manufacturers may comply with relevant standards, but an HDO’s medical device cybersecurity policies and procedures may be deficient, or the HDO may not have access to some of the proprietary product design details necessary to adequately assess risk. The demonstration testing of the ICU Medical Plum 360 infusion pump showed that a product Certified to the UL-2900-2-1 requirements enabled integration of appropriate staff, policies and procedures with the device’s technical design details that could be shared with a trusted independent third party such as UL. During the course of the CRADA, UL helped VA emphasize the importance of issues such as:

1. Tracking software or hardware component vulnerabilities which are needed to identify the impact of cybersecurity threats

2. Linkage with outside cybersecurity tools and processes, such as Coordinated Vulnerability Disclosure through DHS ICS-CERT, is also critical to a coordinated cybersecurity response.

Upgrades and patches
Upgrades and patches present complex efforts for HDOs to systematically undertake and implement due to the long lifespan of connected medical devices. Devices, such as infusion pumps can outlast the life of a native third-party operating system and surpass end-of-support.

Application of patches can also prove difficult in instances where devices are not connected to networks or directly provide patient care, typically at times when rebooting a system is not possible. Establishing and maintaining robust inventory management systems can also help monitor and detect the need for patches or upgrades.

Inventory of devices
Following VA procurement of medical devices, those products are entered into the department’s Networked Medical Device Database, or NMDD. Then, devices go through a change control process and are entered into the VA’s Medical Device Isolation Architecture (MDIA). Virtual LANs (VLANs) are used to segregate these devices from other networked devices already in use.

At a device’s end-of-life phase, device owners are responsible for reporting the disposition of medical devices for tracking purposes, as well as meeting all compliance requirements for disposal, which again requires an adequate inventory control system. Cybersecurity concerns also necessitate a means to track the disposition of associated with such devices.

Lessons for a VA Comprehensive Connected Medical Cybersecurity Strategy

In working with the VA Task Group, UL and VA demonstrated that products that underwent testing and Certification to the UL 2900 requirements could provide the following benefits for VA:

- A process to establish whether manufacturers have characterized, and documented technologies used in their products that could constitute an "attack surface."
- Threat modeling based on intended use and relative exposure.
- Demonstration of an effective implementation of security controls protecting both sensitive data (e.g., PII, PHI) plus other assets such as command and control data.
- Objective evidence that software weaknesses and vulnerabilities have been appropriately dispositioned and further verified via penetration testing.
- Promotion of defensive design (e.g., defense-in-depth, partitioning, etc.)
- Confidence in system robustness (e.g., fuzz testing, malformed input testing).
- Improved monitoring for security events.
- Logging of security events.
- Managing of security logs.
- Systematizing software updates[50] to address safety, essential performance and security issues.
- Handling failures in the software update process (e.g., roll-back).
- Purchasing controls for components within a medical device.
- Management of sensitive data.
- Remote product management (e.g., remote product servicing).
- Decommissioning (e.g., purging of PII and/or PHI).

These inputs helped VA in its trajectory toward Level 1 and Level 2 objectives in its comprehensive cybersecurity strategy for medical devices. (See Figure 2.)

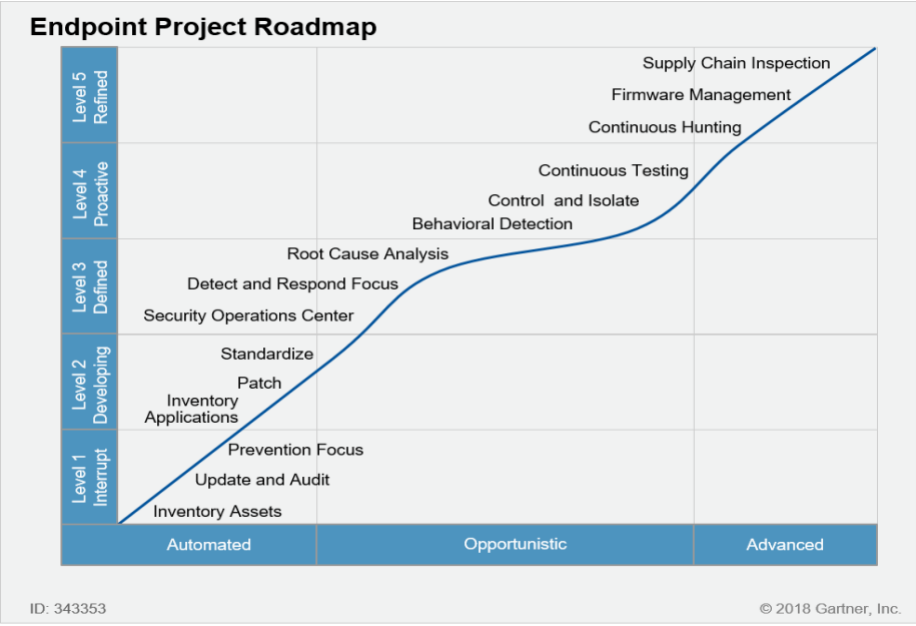

Figure 2. Diagrammatic roadmap used by VA

The findings of the CRADA showed that incorporating the UL 2900 Series of Standards could serve as an important layer in VA's defense-in-depth strategy.

Conclusions

1. **Use of UL 2900-1 and UL 2900-2-1 provided for more robust risk management of VA's connected medical devices:**

   Through the combined efforts of different organizational functions to satisfy the security requirements of UL 2900-2-1, VA risk assessment processes that meet UL 2900-2-1 requirements can facilitate more directed and effective communication between VA's contracting, biomedical engineering, IT and information security officers. This, in turn, helps ensure that minimum cybersecurity standards for medical devices are met. Utilization of the UL 2900 Series of Standards can reduce variation in compliance across VA's 172 medical centers, allowing providers to more consistently meet specific healthcare needs in the field. In cases where local VA providers require variation, this could be explicitly understood, authorized and auditable, thereby improving supply chain efficiency.

   UL 2900-2-1 can complement the efficiency and comprehensiveness of VA's existing procurement processes. However, due to federal government information security policies relating to FIPS 140-2, cryptographic approaches would need to be restricted in order to satisfy FIPS 140-2 compliance (per its reference, along with other cryptographic techniques, in UL 2900-1). If current policies were to be expanded to accommodate equivalent measures for safety and security that are compliant with the requirements of the UL standard, the use of the UL 2900 Series of Standards may furthermore drive development of new and innovative approaches to security.

   UL-2900-2-1 complements FIPS-140-2 access security for VA, but also has a broader scope than FIPS 140-2. UL 2900-2-1 focuses on a more holistic approach to end-point security that includes use-case-specific issues such as vulnerability assessment, management of security logs, and decommissioning, which span the product lifecycle. The UL 2900-2-1 approach could provide VA with tools to assess novel security features of leading-edge technologies that in turn could accelerate adoption of innovative new therapies and services to Veteran patients.

   Given the long-life of medical devices and often inadequate cybersecurity protections featured in legacy devices, UL 2900-2-1 offers a means of systematizing connected device procurement, and with a device inventory system, underpinning ongoing cybersecurity surveillance activities as part of a comprehensive cybersecurity program for lifecycle management of medical devices.

2. **Use of the UL 2900 series of standards could provide for more robust risk management of private-sector HDOs' connected medical devices:**

   Subject to a satisfactory crosswalk of an HDO's existing connected device procurement policies and processes, private-sector HDOs could also adopt, incorporate and harmonize to UL 2900-2-1 to improve cybersecurity assurance of purchased products.
   Through requisite combined efforts of different organizational functions to satisfy the security requirements of UL 2900-2-1, enhanced standardization of HDO security risk assessment processes via UL 2900-2-1 compliance can support more directed

communication between procurement stakeholders within a purchasing organization. Relying on a recognized consensus standard provides better end-point security and assists with adoption of leading-edge technologies within a comprehensive cybersecurity compliance program for connected medical devices.

3. **Benefits of widespread adoption of the UL 2900 Series of Standards for medical device manufacturers and the broader healthcare ecosystem:**

   Medical device manufacturers' return on investment (ROI) for improved cybersecurity assurance could be offset by:

   - Enhanced product differentiation by offering new functionalities with explicit cybersecurity risk protections that HDOs will adopt more readily.
   - Helping create a market for precision-medicine products and expand the overall connected medical device market by having a practical Trust Model to facilitate market transactions.
   - Driving global consistency of regulatory approaches and processes.
   - Providing tools to drive continuous improvement in product design and development.
   - Facilitating alignment of technical requirements across multiple critical infrastructure domains such that certain technologies developed for healthcare applications could be easily sold to other industry sectors and vice versa.
   - Enable the medical device sector to continuously improve the baseline of cybersecurity hygiene for a greater emphasis on emerging trends in product-level security within a challenging threat landscape.

4. **Widespread adoption of the UL 2900 Series of Standards provides potential benefits to the U.S. Department of Homeland Security in relation to CNAP:**

   Nationwide use of the UL 2900 Series of Standards in the connected medical device lifecycle could support a quantifiable risk assessment tool to determine cybersecurity risk associated with medical devices across the healthcare sector, as well as offer a way to assess threats and mitigate cyber-attacks at a medical device level for individual HDOs, HDO networks and critical-infrastructure-wide levels, in the event that a product or class of products used routinely in healthcare were targeted. Such an attack could have devastating consequences to care delivery, both from the threat itself but also from inappropriately instituting continuity of operations plans that could massively and unnecessarily disrupt care.

   In addition, UL 2900-2-1 could provide a means to rapidly develop threat reduction or mitigation strategies by facilitating threat responses using standardized, objective data rather than relying on inconsistent self-reporting.

Relevant standards

Authentication:

- XACML
- X.509, Oauth/OpenID Connect
- Kerberos
- SAML
- Lightweight Directory Access Protocol (LDAP)
- IEEE 802.11ac-2013

Encryption:

- WS-*, TLS per FIPS 140-2 requirements

Risk Management:

- **ISO 14971**—Medical devices – Application of risk management to medical devices
- **EC 60601-1**—Medical electrical equipment
- **IEC 62304**—Medical device software – Software life cycle processes
- **IEC 62443-2-1** Edition 1.0 2010-11 - Industrial communication networks -
- **IEC/TR 80001-2-9** – Application of risk management for IT-networks incorporating medical devices
- **IEC 80002-1**—Medical device software
- **AAMI/UL 2800**—Safety and Security Requirements of Interoperable Medical Systems
- **AAMI/TIR 57**—Principles for medical device information security management
- **CLSI/AUTO11-A** - IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard.

References

[1] https://www.marketsandmarkets.com/Market-Reports/iot-medical-device-market-15629287.html

[2] MedFusion is VA's proactive, innovative and advanced approach toward improving the security posture of Internet of Medical Things (IoMT). Led by VA's Healthcare Technology & Analytics PMO Team, the strategy is based on leveraging multiple leading-edge technologies that form a comprehensive solution necessary for the lifecycle management and security of medical devices and special purpose systems.

[3] National Center for Veterans Analysis and Statistics, Department of Veterans Affairs, NCVAS Pocket Cards. 3rd Qtr, FY 2019. https://www.va.gov/vetdata/docs/pocketcards/fy2019q3.pdf

[4] Eibner, Christine, Heather Krull, Kristine Brown, Matthew Cefalu, Andrew W. Mulcahy, Michael Pollard, Kanaka Shetty, David M. Adamson, Ernesto F. L. Amaral, Philip Armour, Trinidad Beleche, OlenaBogdan, Jaime L. Hastings, Kandice A. Kapinos, Amii M. Kress, Joshua Mendelsohn, Rachel Ross, Carolyn M. Rutter, Robin M. Weinick, Dulani Woods, Susan D. Hosek, and Carrie M. Farmer, Current and Projected Characteristics and Unique Health Care Needs of the Patient Population Served by the Department of Veterans Affairs. Santa Monica, CA: RAND Corporation, 2015. https://www.rand.org/pubs/research_reports/RR1165z1.html.

[5] National Center for Veterans Analysis and Statistics, Department of Veterans Affairs, NCVAS Pocket Cards. 3rd Qtr, FY 2019. https://www.va.gov/vetdata/docs/pocketcards/fy2019q3.pdf

[6] U.S. Congress, House Committee on Appropriations, Subcommittee on Military Construction, Veterans Affairs, and Related Agencies, The State of Veterans Affairs, Statement of the Honorable Robert L. Wilkie, Secretary of Veterans.

[7] Byrne CM, Mercincavage LM, Pan EC, Vincent AG, Johnston DS, Middleton B.The value from investments in health information technology at the U.S. Department of Veterans Affairs. Health Aff (Millwood) 2010;29(4):629–638.

[8] General Accounting Office. Veterans Affairs Information Technology Management Attention Needed to Improve Critical System Modernizations, Consolidate Data Centers, and Retire Legacy Systems. GAO-17-408T: Published: Feb 7, 2017. Publicly Released: February 7, 2017.

[9] One Hundred Fourteenth Congress, Second Session. United States House of Representatives, Committee on Oversight and Government Reform. VaCybersecurity and IT Oversight. March 16, 2016. https://www.hsdl.org/?view&did=795596 viewed 2-18-2019.

[10] Department of Veterans Affairs.Office of Inspector General Federal Information Security Modernization Act Audit for Fiscal Year 2015.https://www.va.gov/oig/pubs/vaoig-15-01957-100.pdf

[11] VA Directive 6550.Pre-Procurement Assessment for Medical Device/Systems 2015.US Department of Veterans Affairs, Washington DC.

[12] VA Office of Technology Strategies (TS) Office of Information and Technology (OI&T).VA Enterprise Design Patterns Privacy and Security.Medical Device Security.Version 1.0 Date Issued: January 2017.https://www.ea.oit.va.gov/EAOIT/docs/Oct_2016_Release_Docs/1-6-Enterprise-Auditing-Design-Pattern-020116_final.pdf.

[13] ISO/IEC 27017:2015. http://www.iso27001security.com/html/27017.html [accessed] 2-20-2019.

[14] ISO/TR 80001-2-7:2015.https://www.iso.org/standard/63509.html [accessed] 2-20-2019.

[15] US Government Cybersecurity National Action Plan. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [accessed] 2-25-2019

[16] Byrne, C.M., L.M. Mercincavage, E.C. Pan, A.G. Vincent, D.S. Johnston and B. Middleton. 2010. "The Value from Investments in Health Information Technology at the U.S. Department of Veterans Affairs." *Health Affairs* 29(4): 629–38.

[17] Darkins A. The growth of telehealth services in the Veterans Health Administration between 1994 and 2014: a study in the diffusion of innovation. Telemed J E Health. 2014;20(9):761–8.

[18] Bagian, J.P., et al. (2002). The Veterans Affairs Root Cause Analysis System in Action. Joint Commission Journal on Quality Improvement, 28(10), 531-545

[19] Williams PA, Woodward AJ. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices (Auckl). 2015;8:305-16.

[20] KPMG, "Health care and cyber security – increasing threats require increased capablities," KMPG, 2015.

[21] UL. http://www.UL.com. [accessed] 2-25-2019.

[22] AAMI and UL to Develop Interoperability Standards. http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/HT_Interoperability/091712_press_AAMI_UL_Interoperability.pdf [accessed] 2-25-2019

[23] Cohen, Julie E., The Regulatory State in the Information Age (January 11, 2016). Theoretical Inquiries in Law, vol. 17, no. 2. https://ssrn.com/abstract=2714072 [accssed] 3-8-2019]

[24] Sandisk. The Great IT Upgrade. IT pros are migrating from the land of Windows Server 2003... into modern territory. 2015. https://www.spiceworks.com/marketing/resources/reports/windows-server-2003-upgrade/ [accessed 3-8-2019].

[25] Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff. 2016
https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf [accessed 3-8-2019]

[26] VA-UL Cybersecurity CRADA. https://industries.ul.com/wp-content/uploads/sites/2/2016/06/UL-VA-Cybersecurity-CRADA-Press-Release.pdf [accessed] 2-25-2019.

[27] 96th Congress S. PL 96-480. https://www.congress.gov/bill/96th-congress/senate-bill/1250 [accessed] 2-25-2019

[28]US Food and Drug Administration. CFR - Code of Federal Regulations Title 2. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=807 [accessed] 2-28-2019

[29]ICU Medical. Plum 360 Infusion Pump. http://www.icumed.com/products/infusion-therapy/iv-systems/plum-360.aspx [accessed 2-28-2019]

[30]US Food and Drug Administration, Infusion Pumps Total Product Life Cycle: Guidance for Industry and FDA Staff, December 2, 2014. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm209337.pdf[accessed] 2-15-18.

[31]Medtech Insight, "U.S. Markets for Drug and Fluid Delivery Devices," October 2007.

[32]Husch, M., Sullivan, C., Rooney, D., Barnard, C., Fotis, M., Clarke, J., & Noskin, G. (2005). Insights from the sharp end of intravenous medication errors: Implications for infusion pump technology. Quality and Safety in Health Care, 14(2), 80-86. doi:10.1136/qshc.2004.

[33]Catlin AC, Malloy W, Arthur K. et al. Comparative analytics of infusion pump data across multiple hospital systems. Am J Health Syst Pharm. 2015; 72: 317– 324

[34]CISA Advisory (ICSA-15-174-01). https://ics-cert.us-cert.gov/advisories/ICSA-15-161-01 [accessed] 2-15-2019

[35]US Food and Drug Administration. White Paper: Infusion Pump Improvement Initiative.https://www.fda.gov/medicaldevices/productsandmedicalprocedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm205424.htm#ft2 [accessed 1-3-2019]

[36]"Life expectancy projection benchmarks", American Society for Healthcare Engineering of the American Hospital Association, Healthcare Facilities Management Series, published in 1995. Author, Joseph McClain, MS, SASHE, CBET, chief, clinical engineering division, Walter Reed Army Medical Center, Washington DC.

[37]US Department of Veterans Affairs. Directive 6550. Pre-Procurement Assessment for Medical Device/Systems. 3. 2015. Washington DC.

[38]US Food and Drug Administration Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf [accessed 2-3-2019]

[39] This guidance contained non-binding recommendations.

[40]National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.0. 2014. https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [accessed 2-3-2019]

[41] This was v1.0 in 2016

[42]Food and Drug Administration. Title 21--Food and Drugs. Chapter I--Food and Drug Administration

Department of Health and Human Services. Subchapter H--Medical Devices. Part 820. Quality System Regulation. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=820 [accessed 2-3-2019]

[43]International Organization for Standardization. ISO 13485:2016 Medical devices -- Quality management systems -- Requirements for regulatory purposeshttps://www.iso.org/standard/59752.html [accessed 2-3-2019]

[44]First. Common Vulnerability Scoring System. SIG. https://www.first.org/cvss/ [accessed 2-3-2019]

[45]Department of Veterans Affairs. Risk Management Framework for VAInformation Systems – Tier 3: VA Information Security Program. Washington DC March 10th 2015.

[46]The ICU Medical Plum 360 was a UL 2900 certified connected medical device

[47]ICU Medical. Plum 360 Infusion Pump. http://www.icumed.com/products/infusion-therapy/iv-systems/plum-360.aspx [accessed 2-28-2019]

[48]A "guest" VA wireless network

[49] Note the demonstration did not take place on a VA VLAN delivering clinical services and connected with HIT assets such as VA's EHR. It took place on a non-clinical network with corresponding configurations.

[50]Dameff C, Bland M, Levchenko K and Tully J. Pestilential Protocol: How Unsecure HL7 Messages Threaten Patient Lives. Abstract Black Hat Meeting Las Vegas 2018.http://acsweb.ucsd.edu/~mbland/pestilential_protocol.pdf [accessed 3-8-2019]

UL.com/cybersecurity

CT 24478783-0819