SAFETY VERSUS SECURITY:
DEFINING HEALTHCARE INFORMATION TECHNOLOGY (IT)
SECURITY STRATEGIES

by

Christopher G. Schlak, Lieutenant Colonel, United States Air Force

A Research Report Submitted to the Faculty
In Partial Fulfillment of the Graduation Requirements
Advisor: Clinton A. Mixon, Colonel, United States Air Force

19 March 2015
DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.
Lieutenant Colonel Christopher G. Schlak entered the Air Force in 1997 as a graduate of the Embry-Riddle Aeronautical University Air Force ROTC program with a Bachelor of Science degree in aviation computer science. He continued his education by attending the Air Force Institute of Technology, through the civilian institution branch, gaining a Master of Science degree in interdisciplinary telecommunications in 2002 from the University of Colorado. He has held positions as executive officer, flight commander, USAFE and AF-level career field manager, branch and division chief, Stan/Eval chief, Commander’s Action Group chief, and was an instructor in the Communications and Information officer schoolhouse. Lt Col Schlak commanded the 607th Support Squadron under the 607th Air Operations Center at Osan Air Base, South Korea, and has held various staff positions at the NAF, MAJCOM, HAF, and OSD levels. He is currently a student at the Air War College at Maxwell Air Force Base, Alabama.
ABSTRACT

As with all facets of life, the United States healthcare system has experienced a massive influx of networked and IT enabled devices designed to increase the efficiency and effectiveness of patient care. Hospitals today average 10-15 networked devices per bed. As more networked devices are added, either wired or wireless, a patient’s care and personal data faces ever increasing threats and the possibility of physical harm or identity theft grows.

Healthcare providers must choose to prioritize patient safety or securing patient data or at least they think they have to choose. Devices can be manipulated remotely by hackers, causing patient devices to act in manners not intended. Alternatively, data can also be manipulated to cause injury. Based on these safety and security issues, what strategies should the Air Force adopt to prevent threats and vulnerabilities to healthcare devices and patient data to ensure patient safety? This paper will frame the problem, define the risks, describe the current strategy, and then provide recommendations for strategy changes to protect patients and their data in order to prevent loss of life.

Technology has led to hyper-connectivity which increases speed and efficiency of medical care, but also elevates the risk. Hyper-connectivity leads to numerous threats in the healthcare industry, and “there’s no muzzle flash with a laptop.”¹ By building a culture of cyber security awareness within hospitals, sharing data on known threats with medical communities, and the ability to extensively test and evaluate new technology for security flaws, modern medicine can move securely into the future.
INTRODUCTION

“By over-depending on these undependable things, we have created the conditions such that any single extreme individual could have profound and asymmetric impact on human life, national security, and gross domestic product.”
– Josh Corman, Atlantic Council, Feb 2017, RSA DevOps Conference

As with all facets of life, the United States healthcare system has experienced a massive influx of networked and IT enabled devices designed to increase the efficiency and effectiveness of patient care. The Department of Defense (DoD) health care system directly mirrors its civilian counterpart. Hospitals today average 10-15 networked devices per bed.\(^2\) As more networked devices are added, either wired or wireless, a patient’s care and personal data is placed in further jeopardy of being stolen.

In clear demonstration of the risk, a hacker exploited an insulin pump’s vulnerabilities in 2011, and then executed an attack on a pacemaker at the 2012 Breakpoint security conference in Melbourne, Australia.\(^3\) The insulin pump was attacked with malicious code, thereby seizing device control and directing the pump to either inject insulin when not required, or to withhold the insulin when required. For the pacemaker, the attacker demonstrated an ability to cause an electric ‘shock’ to any patient within a 50-foot radius.\(^4\) Similarly, attackers inject malicious code via websites, or emails, to gain footholds within the networks to extract personal health data. The threat is a real and ongoing dilemma for hospitals.

Healthcare providers must consider whether patient safety or the security of patient data is the primary concern. As the scenarios above illustrate, devices can be manipulated remotely by hackers, causing patient devices to act in manners not intended. Alternatively, data can also be manipulated to cause injury. Blood type can be changed which affects transfusions during procedures. Physical weight can be altered, which in turn, affects medication levels administered...
through infusion pumps. Through alterations of patient health history, a patient can be harmed. These possibilities cause doctors to question the validity of their patient’s information (if they are aware of a data breach) when making the proper diagnosis. Based on these safety and security issues, what strategies should the Air Force adopt to prevent threats and vulnerabilities to healthcare devices and patient data to ensure patient safety? This paper will frame the problem, define the risks, describe the current strategy, and then provide recommendations for strategy changes to protect patients and their data in order to prevent negligent loss of life.

PRIORITIES: SAFETY vs SECURITY

Healthcare professionals within the DoD rely on networked devices to deliver decision quality information to doctors, nurses, technicians, and administrators throughout the medical treatment facility. To have superior quality information accessible to doctors, medical device vendors are encouraged through policy to “plug everything in.” Networked medical technology has created a hyper-connectivity problem. While speed and efficiency of data flow are greatly increased, the risk to the data and devices on the network also rises. Every device connects to the network, therefore a flaw in one device is shared by all devices across the medical domain, no matter the security configuration of the device.

The Hippocratic Oath every doctor swears includes the statement ‘Do No Harm.’ It is this overarching philosophy that drives healthcare providers to prioritize patient safety. Patient safety in modern medicine is principally driven by its dependence on technology. The devices relied upon to produce information (MRI, CT scanner, or x-ray machine), or to relay information (portable tablets, desktop workstations, etc.), or to store information in electronic health records (EHR) creates a large attack surface for hackers and other nefarious actors looking to steal data or manipulate data and devices just for amusement.
The definition of safety in the medical field must also change. Traditional safety examines a chain of events which results in accidents or loss of life. According to Dr. Nancy Leveson’s research in the book *Engineering a Safer World* and *Safeware*, medical IT needs to adopt a safety posture based on a complex system of systems approach. The increased connectivity of medical devices highlights new dependencies between the network, attached devices, and the data. No longer can a safety incident be tracked to a preventable chain of events. Rather the complexity of the system drives second and third order effects that are not always evident. Safety is paramount and ensuring preventable fatal incidents is becoming more troublesome in the workplace.

**DEVICE SECURITY VS DATA TAMPERING**

Device tampering is just one avenue to induce patient harm. Hackers exhibited at consecutive Def Con briefings that devices are vulnerable based on the insulin pump and pacemaker examples listed earlier. The Food and Drug Administration (FDA) recommended hospitals cease operating a certain manufacturer infusion pump due to vulnerabilities that allowed hackers opportunities to change a patient dosage without consent. The list of vulnerabilities to devices is growing, as evidenced by the graph in Figure 1 from the Industrial Control Systems – Computer Emergency Response Team depicting vulnerability trend data from 2015 to 2017.

Data manipulation or theft can also cause patient harm. Hackers insert malicious code, or use a known backdoor into a provider network, targeting patient data for personal gain. Personal health records are worth more than $100 per record on the dark web (although with recent breaches this value is dramatically down due to large amounts of files already available for sale). Similarly, ransomware encrypts entire hard drives or data servers in hospitals, waiting
for administrators and security professionals to submit payment of funds to unlock their data. Finally, the data within a personal record can be changed to directly affect the patient. Examples include changing blood type, removing procedural notes, or altering medical images from scans. These varieties of data manipulation result in delayed or erroneous diagnosis due to lack of, or improper data. This could lead to death or severe medical problems that are life altering.11

Whether it is device or data tampering, injection of malicious code to gain unauthorized access, or ransomware which shuts down a hospital network, hospital staff members need to be able to counter a breach of security. While it is much harder to treat a patient without key hardware, EHRs should be backed-up to allow for the provision of medical care when electronic data is not available. This will slow down the provider, but better to provide the proper treatment two minutes slower, than provide a potentially life ending treatment in ten seconds.

TECHNOLOGY CATCH-22

Ensuring device security or preventing data tampering of medical records directly links security to patient safety. This changes the paradigm from safety VERSUS security to safety
AND security. This is a culture change for medical professionals, driving dedicated cyber security professionals to be on hospital and clinic staffs.

Technology has driven healthcare to be efficient, but also to be fully dependent on electronic devices, and electronic health records. It is this dependence on network availability and data sharing that results in a lack of manual backup training. When the power goes out, or ransomware hits a hospital, are paper records or forms available? Electronics have enabled doctors to examine more patients, order more tests, and keep track of data in a complex system of records. Without these tools, doctors cannot assess the same number of patients, are unsure of test history, and are uncertain regarding prescription orders. They cannot keep up with the pace of modern medicine without access to electronic systems and devices.

From a security standpoint, technology is moving faster than security professionals can secure it. Software patching of embedded code becomes a problem that affects patient safety. While some vendors offer patches to their devices, other legacy devices use operating systems embedded within the core of the device. If an MRI machine requires a patch, does the doctor or the IT administrator fully understand the patch? The patch could update the graphics output of the imaging device to counter a vulnerability; however, that patch may also change how the image is created or displayed for the doctor. The FDA certifies devices to work under specific parameters. By patching the device an administrator may invalidate the FDA certification. In other words they continue the culture of safety versus security, but in this case siding with security. By declining to patch the device, the hospital network is open to known vulnerabilities. It’s a catch-22 for security concerns.
UNDERSTANDING RISK

Hospital staff members need to define and understand the risks to the network, devices, and data. The first action is to step back and look at what is to be defended. According to Ms. Essye Miller, interim DoD Chief Information Officer, defining what is worth defending and its relevance to ensuring patient health is paramount. “Risk depends on the information that a doctor needs. We need to define what data is critical and always needs to be right,” she remarked during a personal interview. Figure 2 highlights vendor and hospital attack preparedness, where two in five vendors surveyed have not taken appropriate security steps to protect against attacks. Security starts with knowing the security landscape and changing day to day operations to remain secure.

Network security is just as important as physical security. When sitting in an examination room, drawers and cabinets with sensitive medical items are locked until needed by the doctor, or nurse. Yet a yellow stickie note is tacked above the computer with an IP address, shared login names, and passwords for quick reference when doctors transition between exam rooms. This key data can be used by hackers to impersonate the doctor, or nurse, and gain access to data or devices that should be private and protected.

Medical equipment is available to purchase for home use. This assists in-home care but also raises a security issue. Hackers can purchase devices to take them apart, physically and logically, to discover security bugs or ways to manipulate the device. Some devices are built with default accounts and passwords which medical staff rarely change. Other devices have hard coded maintenance accounts and passwords which cannot be changed. The solution is to remove hard coded passwords, thus allowing administrators to change both the administrator default account name along with management passwords. Customizing security is best but may
reduce remote accessibility from the vendor if outside maintenance or support is needed.

The Internet of Medical Things (IoMT) has caused an explosion of devices supporting medical providers and patients. IoMT categories include wearables fitness trackers (Fitbit), wearable external/internal devices (insulin pumps), implanted devices (pacemaker), and a myriad of portable wireless devices (iPads, tablets, voice transcribers, etc.). Many of these devices utilize Bluetooth and/or WiFi connectivity, but do not use encryption to pass data from the device to the network. Securing the data via encryption is effective, but also slows down record transactions. When security protocols interfere with efficiency and effectiveness of patient care, security is often removed at the direction of the doctors who need speed, but sacrifice security.

**DATA SECURITY: A SECURITY PROFESSIONAL’S DILEMMA**

In cybersecurity, the CIA (Confidentiality, Integrity, and Availability) triad is key. In medicine, integrity and availability of the data compete for primacy. Doctors require as much data about a patient as possible when making the correct diagnosis, and they want it available
anytime. This places availability as their primary consideration. However, if the data is incorrect, or has been manipulated, then availability is irrelevant because the data is untrustworthy. The data provided by medical devices, or from within a patient’s EHR, should be pure. Trust in the data presented to the doctor is paramount. But is all data equally important? Parts of the patient record should be immutable — blood type, date of birth, previous procedures, or surgeries. Some elements of the record may require less security scrutiny such as where someone was born, marital status, or social history. Like air superiority which can be targeted for specific airspace at specific times, data protection can and should be focused on the immutable components of patient data. The ability to secure parts of the health record, not the entire record, allows security experts to focus efforts where most required, ensuring data that doctors need most is trustworthy and available. Today, all data in the EHR is treated the same, with no special protections. The result is the repeated questioning of patients to validate blood type, date of birth, and other data prior to procedures ensuring what is known is in fact what is recorded in the EHR.

Blockchain technologies are being developed with ledger features that protect and ensure the veracity of data. John Halamka, Chief Information Officer at Beth Israel Deaconess hospital in Boston stated, “Imagine when a doctor sees a patient or writes a new prescription, the patient agrees to have a reference or “pointer” added to a blockchain—a decentralized digital ledger like the one underlying Bitcoin. Instead of payments, this blockchain would record critical medical information in a virtually incorruptible cryptographic database, maintained by a network of computers, that is accessible to anyone running the software. Every pointer a doctor logs on the blockchain would become part of a patient’s record, no matter which electronic system the doctor was using—so any caregiver could use it without worrying about incompatibility issues.
A medical blockchain is being advocated for but must be created from scratch. Once created, a medical blockchain ensures electronic health records are more secure, more easily accessed, and shifts the security focus from change prevention to change detection.

The country of Estonia is an early front runner in the deployment of medical blockchain. Since early 2017, Estonia has offered its one million citizens access and protection of their medical data via Keyless Signature Infrastructure, using their government issued e-ID. The configuration protects against interference, glitches, and viruses. To secure the EHR, the system only allows entries into the record, keeping the rest of the data secure from any alterations. Likewise, the Dubai government is leading a blockchain effort to digitize and share all government data which includes personal health records. Both countries are leading the way, demonstrating how blockchain can facilitate secure and reliable health care record sharing.

DEVICE SECURITY: IT’S OUT OF DATE BEFORE YOU BUY IT

Unlike regular IT, medical devices undergo extensive development and testing before the FDA will certify the device. Once certification is complete, the company is permitted to sell the devices to hospitals for operational use. Some devices are intended to have a useful life of 10-20 years, depending on the equipment and operational requirements (either in a hospital or with a patient). From development to certification, sales, and lifespan, it is not uncommon for devices to have an actual 15-30 year lifespan. However, embedded operating systems used as controllers for high-end equipment turn over every 18-24 months. Before a device is certified, it is possible for systems to be two or more versions outdated. By the end of life, with no patching or updates, the number of vulnerabilities could number in the thousands for a single device. All operating systems will require updates and patches, but many vendors cannot, or do not, provide updates as these ‘fixes’ place their device’s FDA certification at risk. “The medical
community needs to catch up with cyber procurement based on the 18-24 month operating system changeover,” according to Peter Kim, Chief Information Security Officer (CISO) for the Air Force. Patching, upgrades, and overall lifecycle management need to be more centrally managed within the medical community to ensure security is “baked in, not bolted on.”

ACQUISITION AT A SNAIL’S PACE

Consider the Deepwater Horizon oil spill from April 2010. Millions of barrels of oil spilled into the Gulf of Mexico in the world’s largest marine oil spill. It took five arduous months to shut off/cap the broken wellhead. Now translate the event to the healthcare industry: a sustained denial of patient care from malware or ransomware, Mirai, WannaCry, or Petya as examples. Vendor development time until clinical testing can take 2 – 3 years on average, the equivalent of 12.5 Deepwater Horizon events worth of spilled oil. Next, FDA certification of the device is required, then fielding to hospitals to swap out vulnerable or impacted devices. In the end, the medical community could wait almost 10 years to replace every affected piece of networked equipment and reduce the exposure to threats. In that same period, other threats will emerge causing the cycle to repeat. During this period of transition, patients’ lives will remain at risk until the device is replaced or upgraded. If security is not integrated from inception, long lead times will be required to counter an ever-growing and much more responsive cyber threat.

GUIDANCE AND LEGISLATION DRIVING CHANGE

Medical IT is not without security guidelines. The guidance established by the National Institute of Standards and Technology (NIST), the FDA, and even Department of Defense Instructions (DoDI) are just that – guidance. There is pressure and expectation to follow guidance, but there are no ‘teeth’ behind these security guidelines. NIST special publication 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and*
Organizations, DoDI 8510.01 Risk Management Framework, and the Defense Information System Agency (DISA) Security Technical Implementation Guides (STIGs) all require additional layers of security to mitigate vendor, or legacy device security shortfalls. However, issues manifest in medical networks when trying to meet these established security standards. Common security struggles include implementation of multifactor authentication for privileged users on medical devices, deployment of endpoint security tools (like McAfee host-based security system), and a requirement to scan devices every 30 days for known vulnerabilities. Medical devices, in general, are ill-suited to host-based defense, but policy (STIG and DoDI) drive a review at the device level. These policies work for standard IT systems but cannot be applied to IoMT devices in the same manner. A balance between the two must be discovered, or new policies specific to IoMT must be crafted to ensure security is designed in from the beginning.

The FDA issued Post Market Guidance for Medical Devices, with the intent to assist device vendors in handling cyber security risks throughout the lifecycle of a device. The shortfall of this guidance is the usage of the word ‘encouraged.’ According to Beau Woods of the Atlantic Council, the FDA post-market guidance is less focused on vendors, but rather on how the FDA wants its evaluators to critically review new medical devices before certifying. It behooves vendors to understand and follow the guidance, then build-in safety mechanisms and security features. Vendors knowing how the evaluators will score prototype devices presented for FDA approval, ensures a product is not deficient in any category, especially cyber security. FDA denial translates to prohibited sales in the US healthcare market.

Vendor profits is a critical factor that cannot be overlooked. Per unit costs become quickly prohibitive when security is added. A sensor may be simple and cheap (less than $1 per
unit), but when security requirements are designed in, the unit cost could triple or quadruple. Security can quickly erase any profit margin available to vendors or make the price too high and no longer feasible to be developed. A device that is fully developed but not secured is not available for sale and decreases profits. To make money, vendors prioritize their development budget without fully understanding the potential loss of human life to a device that is not secure.

Finally, Congress is also getting involved with medical IT security. Separate bills introduced in the House and Senate are currently being discussed in committee. Senator Richard Blumenthal (D-CT) introduced S.1656, *Medical Device Cybersecurity Act of 2017*, in August 2017 to create a cyber report card for devices, and require testing to be performed before being sold to the medical community. Congressman David Trott (R-MI) introduced H.R.3985, *Internet of Medical Things Partnership Act of 2017*, in October 2017, proposing to create a working group of public and private entities to collaboratively identify security gaps and find actionable solutions for IoMT developers to reference. Both pieces of legislation have the potential to create transparency of security for devices used throughout the medical community. The committees must also ask what is being measured for the report card. Individual metrics are not easy to define, and everyone disagrees on the focus. “Report cards are also inherently subjective and evaluate a point in time. Today’s report card or scorecard is out of date tomorrow, as the network and parameters being scored change daily,” stated Beau Woods.

**RELEVANCE: WANNACRY AND FUTURE THREATS**

On Friday, May 12, 2017, a global ransomware attack known as WannaCry began impacting more than 100 countries. In the United Kingdom (UK), the National Health System (NHS) declared the attack a major cyber incident and began implementing emergency procedures to ensure continued health care for patients. Across England, 81 of 236 trusts (acute
hospitals) were shut down by the ransomware, or administrators terminated operations to preventively protect their vulnerable devices. In either case, these acute facilities were now unable to provide lifesaving medical care. An additional 603 UK NHS primary care organizations were also impacted by WannaCry over the following week. From May 12 to 19, at least 34% of all medical trusts in England were impacted. More troubling is the fact that the full extent of the disruption is not known.

A report on the WannaCry event was directed by the UK National Audit Office to determine causes, health care disruptions, and lessons learned. The cause was simple, a patch had been available from Microsoft for months and was not installed. Windows 7, 8, XP, and Server 2003 operating systems were the most vulnerable. The vast majority of devices infected in the UK were Windows 7 devices and were missing the required security patch. Sadly simply enabling automatic Windows Updates would have prevented the infection and kept the medical trusts open. In the UK, two hospitals that were directly impacted by WannaCry had also been infected with ransomware in 2016, though the cause was likely different.

The single biggest issue for NHS England was the cancellation or postponement of 19,494 medical appointments. An estimated 6,912 appointments were cancelled in a single day on May 12. NHS England could not establish an actual number of individuals directly impacted because that data was not collected. In hospitals affected, support and diagnostic equipment was indirectly impacted due to inability to share images from MRI or CT scanners with doctors who needed diagnostic information. Additionally, ransomware impacted five hospitals who had to divert emergency patients to other hospitals not affected by WannaCry due to lack of available services.
WannaCry was not developed to steal patient data or cause direct harm, but directly impacted patient care. From the UK report, “neither the Department nor NHS England know how many general practice appointments were cancelled, or how many ambulances and patients were diverted from the five accident and emergency departments that were unable to treat patients.” From this statement there is acknowledgement that WannaCry impacted timely patient care and resulted in an increased mortality rate due to lack of medical IT services.

This recent WannaCry example illustrates how a lack of cyber security and cyber culture within hospitals contributed to the speed with which a single missing software patch can impact a national healthcare system. This significant event could have been avoided by simply updating systems throughout the network. A lack of security staff, decisions about patient care driving availability, or any number of issues could explain why the patches were not applied in time. This demonstration of cyber security decision making affecting the physical domain clearly highlights the future implications of security considerations with any medical IT environment. Hospital staffs, administrators, and security professionals need to work together to ensure safety and security of the medical network.

RECOMMENDATIONS

After establishing the primary focus of the medical community, evaluating risk versus patient safety, and identifying areas of weakness inherent in the medical IT security field, the following six recommendations are provided for the medical community and security professionals to better posture the healthcare community for the future. This list is a starting line, as security measures are dynamic and need to be constantly updated. At the same time, security professionals must work within hospital requirements to meet patient care effectiveness and efficiency. According to Jeff Eyink in the Cyber Security Division, Defense Health Agency
1- Establish education, create policy, and change the culture. As noted above, security is not the focus of medical professionals, and many are unaware of the threats presented through careless and uneducated behaviors while using networked devices. Education through the Cyber Secure program and cyber-related courses added to medical professional military education will help with information about the threat, sharing information, and connecting the dots of security and safety within a hospital. Policies to direct specific medical-related IT training about threats, coupled with new cyber security staff members allow for immediate awareness and a heightened security posture. This information needs to be shared with new doctors and healthcare professionals along with seasoned members of the healthcare industry. The culture will change, but that change needs to start immediately.

2 - Create a developmental testing and evaluation environment. DHA should work with medical vendors and the FDA to accomplish additional device testing before purchasing new capabilities for military medical facilities. Devices can be tested in FDA certified configurations for all known security flaws, penetration testing, and numerous other security checks to produce a security scorecard for each device. Based on scorecard data, the DHA can approve the device for Service-wide use or require additional security from the vendor or network mitigations to protect the device and its data. If the vendor chooses to fix the identified issue, or a mitigation strategy works to protect the device, vendors may be able to use a ‘DoD Approved’ stamp of approval to further market their device to a much broader commercial healthcare network.

3 - Require vendors to produce a software bill of materials. Electronic devices have thousands, if not millions, of lines of embedded code to enable device features, wireless connectivity,
safety protocols. But this code is not completely custom, much of the code is recycled from
previous product lines or other vendors with similar products. Within the medical IT field, there
is rampant reuse of code versus custom code. This is done simply to cut down on development
time, certification, and ease of integration. Code that has been tested and certified with
appropriate cyber security measures can be tracked. Rather than retesting a new device and all
its components and subroutines, code listed on an approved bill of materials can be certified
quickly. Additionally, code with security risks can easily be detected and identified for specific
vulnerabilities. The software bill of materials can quickly inform security experts what kinds of
attacks a new device will be susceptible to and immediately direct a change, a patch, or deny
certification. The goal for the bill of materials is to make it easier to track what is vulnerable
versus testing every device from every vendor.\textsuperscript{42}

4 - Build a defensible infrastructure\textsuperscript{43} from which medical IT can be protected and secured.

Many commercial medical networks are created as a flat network. Administrator access from
one device allows attackers to control everything. Defense in depth is not the solution… it’s just
an overused catch phrase from 20 years ago.\textsuperscript{44} Blacklisting was easy, there were very few
threats on the network in the early years. Vendors and administrators were not sure what ports,
protocols, or services (PPS) needed to be open for future applications, therefore they left
everything open and denied PPS as needed. Whitelisting is more secure, denying all PPS and
allowing only by exception. Hospital cyber security professionals need to map data flows,
external and internal connections, and only allow the system to work as it is designed, not to
allow shortcuts. Architectures and monitoring help solve the security professional’s dilemma.
DHA should establish a core infrastructure based on segmentation, virtual local area networks,
encryption, and a regime of continuous updating and patching.
As an extreme implementation step for this strategy, the DHA could disconnect the medical network from the unclassified DoD network, using the unclassified network only for official email traffic. However, this will require additional core infrastructure and connectivity between medical treatment facilities not already provided by organizational budgets. This solution solves a major security risk shared between the medical network and the unclassified network, allowing security professionals to ensure medical device security compliance, and protection of personal data. This change in architecture clearly drives a change to DHA and military service risk evaluations of the medical networks.

5 – Join the National Health - Information Sharing and Analysis Center (NH-ISAC) to share threat information. As much of the security information is at a classified level, military hospitals are not made aware of potential threats to networks or devices in their hospital. DHA should engage as a partner with NH-ISAC to openly share and learn about threats, vulnerabilities, and lessons learned countering similar threats from other hospitals. With increased awareness of threats, hospital staff, doctors, and security professionals can be informed of major threats to commercial networks and take appropriate actions to counter each threat.

6 - Establish a Program Management Office to manage medical devices. With the explosion of the IoMT including home and wearable trackers for health data, creating, storing, and managing the devices and data stored will be paramount. However, medical treatment facility (MTF) commanders control their own budgets and device purchasing. A CISO has limited influence on a MTF Commander and their choice of purchases. A program office would oversee testing, develop an approval list of approved medical devices, and could make purchases as required for treatment facilities. This level of oversight would conform to mandatory acquisition processes (potentially solving the software catch-22) over the lifespan of a device; could be influenced by a
security team to ensure only tested and secured devices are on the approved list; and finally, allow standards to be established across the DoD medical networks regarding data at rest, encryption, and patching requirements.47

CONCLUSION

The safety of a patient and the security of the data should no longer be a competition, but a synergistic pairing. Security of the data and the device are directly tied to patient safety. In June 2017, the healthcare industry cybersecurity task force reported to Congress, stating specifically the need to increase security and resilience of medical devices and health IT.48 Modern medical facilities are filled with networked devices, patient data is electronic, and security has been a secondary consideration. Technology has led to hyper-connectivity which increases speed and efficiency of medical care, but also elevates the risk. Hyper-connectivity leads to numerous threats in the healthcare industry, and “there’s no muzzle flash with a laptop.”49 By building a culture of cyber security awareness within hospitals, sharing data on known threats with medical communities, and the ability to extensively test and evaluate new technology for security flaws, modern medicine will move securely into the future.
BIBLIOGRAPHY


I Am The Cavalry. “Hippocratic Oath for Connected Medical Devices.”


Kuchler, Hannah. “Medical device makers wake up to cyber security threat,” Financial Times, 1 Aug 17. https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691 (accessed 3 Nov 17)


https://www.wired.com/2017/03/medical-devices-next-security-nightmare/ (accessed 3 Nov 17)


Orcutt, Mike. “Who will build the Healthcare blockchain?” MIT Technology Review, 15 Sep
(accessed 14 Dec 17)

Ossola, Alexandra. “Hacked Medical Devices May Be The Biggest Cyber Security Threat in 
life-ransom-by-hijacking-your-medical-devices (accessed 27 Nov 17)

Siwicki, Bill. “How emerging cyber threats are transforming the HIPAA landscape,” Healthcare 
IT News, 29 Aug 17. https://www.healthcareinfosecURITY.com/1-billion-lawsuit-focuses-on-
ehr-data-integrity-concerns-a-10463 (accessed 5 Nov 17)

Siwicki, Bill. “Medical IoT legislation could boost device security… if it can get through 
iot-legislation-could-boost-device-security-if-it-can-get-through-congress (accessed 5 Dec 17)

Snell, Elizabeth. “How IoT Impacts Medical Care Device Cybersecurity Considerations.” 
device-cybersecurity-considerations (accessed 8 Dec 17)

Snell, Elizabeth. “Partnership Stressed in IoMT Medical Device Cybersecurity Bill.” Health IT 
device-cybersecurity-bill (accessed 5 Dec 17)

Tynan, Dan. “Yes, your life-saving medical devices can be hacked.” The Parallax, 3 Aug 17. 

U.S. Coast Guard] [Web.] Retrieved from the Library of Congress.


END NOTES


5 Beau Woods (Atlantic Council), interview by the author, 4 Dec 2017.

6 Jeff Fay and Steve Fisher, interview by the author during visit to DoD CIO, Pentagon Washington DC, 6 Dec 2017.


11 Ashley Andrews and Kristopher Thomas, interview by the author during visit to DoD CIO, Pentagon, Washington, DC, 5 Dec 2017.

12 Jeff Fay and Steve Fisher, interview by the author during visit to DoD CIO, Pentagon Washington DC, 6 Dec 2017.

13 ibid.

14 Essye Miller (Interim DoD Chief Information Officer), interview by the author, 5 Dec 2017.
15 Hannah Kuchler, “Medical device makers wake up to cyber security threat,” Financial Times, 1 Aug 17. https://www.ft.com/content/00989b9c-7634-11e7-90c0-90a9d1bc9691 (accessed 3 Nov 17)

16 Jeff Fay and Steve Fisher, interview by the author during visit to DoD CIO, Pentagon Washington DC, 6 Dec 2017.

17 Essye Miller (Interim DoD Chief Information Officer), interview by the author, 5 Dec 2017.


21 Jeff Fay and Steve Fisher, interview by the author during visit to DoD CIO, Pentagon Washington DC, 6 Dec 2017.

22 Peter Kim (AF Chief Information Security Officer), interview by the author, 5 Dec 2017.

23 ibid.


25 Scott Ham, Mapping the Medical Device Development Process, California Polytechnic State University, 4 Jun 10.


33 Jeffrey Tully (Atlantic Council), interview by the author, 25 Jan 2018.


36 ibid., pg 14.

37 ibid., pg 9.

38 ibid., pg 8.

39 Jeffrey Eyink, Chief, Assessment and Authorizations Branch, Cyber Security Division, Defense Health Agency, Falls Church, VA, to the author, e-mail, 6 Feb 2018.

40 Peter Kim (AF Chief Information Security Officer), interview by the author, 5 Dec 2017.

41 Ashley Andrews and Kristopher Thomas, interview by the author during visit to DoD CIO, Pentagon, Washington, DC, 5 Dec 2017.

42 Beau Woods (Atlantic Council), interview by the author, 4 Dec 2017.


45 Ashley Andrews and Kristopher Thomas, interview by the author during visit to DoD CIO, Pentagon, Washington, DC, 5 Dec 2017.

46 Jeffrey Eyink, Chief, Assessment and Authorizations Branch, Cyber Security Division, Defense Health Agency, Falls Church, VA, to the author, e-mail, 6 Feb 2018.

47 Ashley Andrews and Kristopher Thomas, interview by the author during visit to DoD CIO, Pentagon, Washington, DC, 5 Dec 2017.


If defining security is that elusive, there is little wonder why operating within its coverage is so fluid. In the name of security, people and governments have taken actions where intended and unintended outcomes have become difficult to handle. Because of its seeming lack of conceptual boundary, security, as a concept, is used to entice and whip up patronage for many political projects both at the state and international levels of politicking. Because security technology has the capability to enhance a protection of assets strategy, it is necessary to determine the role of the technology in providing security. This chapter is concerned with the detection, recognition, and identification of persons who are either authorized or unauthorized to be present at a particular location in a facility. Engage the healthcare organization’s information technology (IT) staff early and often to ensure that the cabling, networking and software support resources are available and reliable, as the plan is implemented and used in real-life situations. Health-care organizations are vulnerable to modern trends and threats because it has not kept up with threats. OBJECTIVE: The objective of this systematic review is to identify cybersecurity trends, including ransomware, and identify possible solutions by querying academic literature. METHODS: The reviewers conducted three separate searches through the CINAHL and PubMed (MEDLINE) and the Nursing and Allied Health Source via ProQuest databases. Using key words with Boolean operators, database filters, and hand screening, we identified 31 articles that met the objective of the review. RESULTS: The