Securing Connected Hospitals

A Research on Exposed Medical Systems and Supply Chain Risks

Mayra Rosario Fuentes and Numaan Huq
Trend Micro Forward-Looking Threat Research (FTR) Team

A **TrendLabs**[SM] Research Paper

TREND MICRO AND HITRUST LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro and HITRUST reserve the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro and HITRUST use reasonable efforts to include accurate and up-to-date information herein, Trend Micro and HITRUST make no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro and HITRUST disclaim all warranties of any kind, express or implied. Neither Trend Micro, HITRUST, nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

For Raimund Genes (1963-2017)

Contents

The damage caused by the WannaCry ransomware during and after it held systems hostage in May 2017 exposed just how vulnerable healthcare networks are to cyberattacks. Spreading indiscriminately to 300,000 computers in 150 countries,[1] WannaCry's hold over infected systems blocked National Health Service (NHS) trust hospitals from accessing patient records, compelled hospitals to divert ambulances to other area hospitals not affected by WannaCry, and forced doctors to cancel scheduled appointments, scans, and even surgeries.[2, 3, 4]

The ramifications of this IT security nightmare, considering that WannaCry was not even specifically intended to target healthcare networks, prompted us to examine oft-overlooked infection vectors in today's healthcare networks. As hospitals and other healthcare facilities adopt new technology, add new devices, and embrace new partnerships, patients get better and more efficient services — but the digital attack surface expands as well. The more connected they get, the more attractive they become as lucrative targets to threat actors.

For this research, we first analyzed internet-connected medical-related devices and systems found using the IoT search engine Shodan, such as databases, hospital admin consoles, medical devices, and the like. We successfully discovered exposed medical systems, healthcare software interfaces, and even misconfigured hospital networks, that should not be viewable publicly. While a device or system being exposed does not necessarily mean that it is vulnerable, exposed devices can potentially be leveraged by cybercriminals and other threat actors to penetrate into organizations, steal data, run botnets, install ransomware, etc. Furthermore, it shows that a massive amount of sensitive information is publicly available when it shouldn't be.

We also sought to shed light on a yet-unexamined attack vector as it translates to healthcare networks: supply chain attacks. Several high-profile breaches in recent years involved lapses in the supply chain.[5, 6, 7] Furthermore, according to a health and human services public breach reporting tool, 30 percent of healthcare breaches in 2016 were due to business associates and third-party vendor breaches.[8] To learn from these cases, we studied the different ways threat actors can take advantage of weaknesses in the supply chain to infiltrate healthcare networks.

Finally, we performed a qualitative risk analysis across various attack vectors to give healthcare IT teams an overview of the most pressing threats in their respective environments and help them prioritize. We then provide actionable guidance for healthcare IT teams to implement as a basic minimum. We strongly recommend a blend of security technology and employee/partner awareness and education, including a threat response protocol. Healthcare IT teams must also create, enforce, and frequently review a risk management system and governance framework related to the transfer of resources to and from any entity outside a network's trusted circle to minimize the risk of supply chain attacks. The smooth operation of daily hospital services makes a life-or-death difference for patients — IT security should be an enabler, never an obstacle, to delivering these life-preserving services.

Cyberattacks Against the Healthcare Industry: A Quick Primer

Global life expectancy has been steadily increasing,[9] and much of it can be attributed to advances in medicine and healthcare technology. Technology is at the heart of the modern hospital. Technology allows physicians to identify diseases and treat patients quickly and effectively. A patient in a modern hospital is typically treated by a small team of doctors and nurses who attend to different aspects of the patient's care. This system is designed to ensure that the patient receives the best possible treatment in the most efficient manner. This cooperative patient care is made possible through advances in medical technology and fast data transfers.

The Hospital Information System (HIS) is the backbone of this data transfer and manages all the information processing aspects of a hospital's operation such as medical (diagnostic, treatment, admission/discharge, life support, etc.), legal, administrative, financial, records, and such. Thus, it is important to acknowledge that each application and every device running on the network represents a possible entry point for a cyberattack against the hospital. Clearly, this connectedness also makes technology-heavy modern hospitals lucrative targets for cybercriminals. For one, given the critical nature of hospitals, cybercriminals have quickly realized that if they can successfully compromise the hospital IT environment using ransomware, then there is a high probability of payout by the affected hospitals. Beyond ransomware, hospitals are also treasure troves of personally identifiable information (PII), including financial data, that can be monetized in deep web marketplaces. In this section we take a close look at what cybercriminals typically target and their motivations and methods when it comes to attacking healthcare networks.

What is at risk?

Ransomware has been in the limelight in terms of media coverage and public attention, but in reality, it is not the only threat. The hospital environment has many pathways for different threat actors and several vulnerable areas. In our observation and based on our research into cyberthreats against hospitals, the three broad areas that are at high risk of being targeted by cybercriminals are the following:

Hospital operations

Everyday hospital operations like staff scheduling databases, hospital-paging systems, building controls, pneumatic tube transport systems, inventory systems, payroll, administration, and the like

Data privacy

Patient and employee PII, which includes patient diagnosis and treatment data, insurance and financial information; research and drug trial data, payroll, intellectual property among others

Patient health

Diagnosis, treatment, and monitoring of patients

These will be our three critical areas of interest.

Who is attacking the healthcare industry?

Where there are opportunities, there are perpetrators who attack, steal, and abuse the system for a wide variety of reasons. These threat actors can be criminal gangs that are highly skilled hacking teams, funded and controlled by organized criminal gangs, or sometimes even governments, and they target victims using different methods such as ransomware, phishing, and so on, to generate illicit revenue for the gangs or malicious actions for political reasons.

Likewise, nation-states have been found to gather intelligence using software espionage tools and customized malware in order to use these in social engineering attacks, steal intellectual property, or gain competitive advantage. For instance, the second largest healthcare insurance provider in the United States was affected by a foreign government attack in this way in 2014.[10] Cyberterrorists, meanwhile, launch disruptive or destructive cyberattacks to cause physical destruction of property, loss of life, and spread terror. Hacktivists are internet activists who attack cyber assets to draw attention to their political causes and tend to choose highly visible or high-profile targets. Lastly, script kiddies are persons with low-level programing skills that use automated tools for hacking and are usually motivated by attention on social media sites from peers.[11]

Another category of possible attackers is the insider threat. This type of attacker can be motivated by money, ideology, coercion, ego, revenge, and politics, and could very well be disgruntled employees who steal data or equipment, or keep old employee and admin accounts active for snooping purposes. Other times, insider threats may be borne out of negligence, like opening a phishing email by mistake.

Why is the healthcare industry being attacked?

The key motivator for the vast majority of cyberattacks that we see daily is money. But in the healthcare world, not all perpetrators attacking healthcare providers will be motivated by money. Healthcare providers such as hospitals are highly visible targets and attacks against them will be high-impact, which in itself is a key motivator for many of these perpetrators. For instance, threat actors using ransomware can severely impact the daily operations of healthcare providers. Taken further, disruptive attacks can disable, sabotage, or knock offline critical systems inside a hospital. The health and safety of vulnerable patients suffers as a result.

Other than that, threat actors can steal intellectual property, research data, drug trial data, PII, financial/insurance data, medical records, and the like, and monetize the stolen data in various ways. The stolen data can be used for identity theft, privacy violation, financial fraud, industrial espionage, blackmail, and for sale in the cybercriminal underground. Stolen research data, specifically, represents significant financial investment, years of research, and expensive patient trials, and could save interested parties billions of dollars in research money.

Attacks perpetrated by insiders, or those with physical access to the systems or expert knowledge of their use, are typically acts of revenge.[12] Hacktivists, meanwhile, regularly deface high-profile targets to draw attention to their political and/or social causes.

How are they attacking the healthcare industry?

The healthcare industry is a massive, complex, interconnected ecosystem with thousands of endpoints, systems, and users. The size, complexity, and functions of this ecosystem create large and oftentimes unpredictable attack surfaces. In a technical sense, threat actors can use a number of the following attack vectors to infiltrate or sabotage a system.

- **Spear phishing** — Fraudulent emails target specific organizations[13]; a subset of this is business email compromise (BEC), which targets companies that conduct wire transfers abroad.[14]
- **Distributed denial-of-service (DDoS) attacks** — A coordinated denial-of-service attack launched from multiple locations.[15]
- **Exploitation of software vulnerabilities** — Deliberate use of known weaknesses in a software; in a striking example in August 2017, the U.S. Food and Drug Administration (FDA) recalled half a million pacemakers due to the firmware having vulnerabilities that could allow a hacker access to the device and let them manipulate pacing and battery strength.[16]
- **Malware** — Malicious code intended to disable, damage, compromise, or steal data from computers; various examples exist where ransomware,[17] keyloggers,[18] worms,[19] Trojans,[20] and others affected healthcare networks.

- **Misuse of privileges** — Such as gaining administrative rights in an unauthorized manner, as in a previous case where a hacker was able to get into a healthcare supplier's network via installed third-party software that had weak passwords and allowed administrator access.[21]
- **Data manipulation** — Digital image or data alteration; in 2015, the FDA warned that certain infusion systems contained a vulnerability that could allow a hacker to manipulate the data in infusion pumps used for dosage calculations, thus putting patients' lives at risk.[22]

Threat actors can use any of the above methods to launch major cyberattacks against hospitals in recent years. The following statistics from the HITRUST Cyber Threat XChange (CTX) program — a threat indicator sharing platform — show a few chosen markers about the health industry cyberthreat landscape that provide a snapshot about the most common infection vectors.

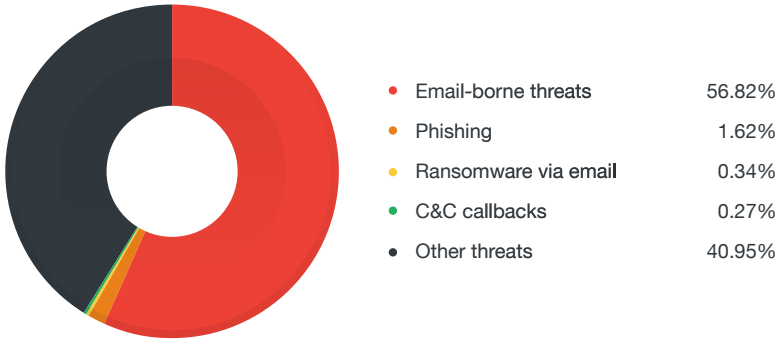


Figure 1. Distribution of Indicators of Compromise (IoC) types, 2017 Q4

(Source: CTX Enhanced Pilot)

Figure 2. Trend of Indicators of Compromise (IoCs) by month, 2017 Q4

(Source: CTX Enhanced Pilot)

To date, the majority of publicly reported cyberattacks against hospitals have been one of the following: data breaches, ransomware, or medical device compromise.

The Privacy Rights Clearinghouse (PRC) is a non-profit corporation based in California that corroborates our observation on data breach attacks against hospitals. Based on their data, the number of reported data breach incidents in hospitals resulting from hacking or malware attacks is on the rise.[23]

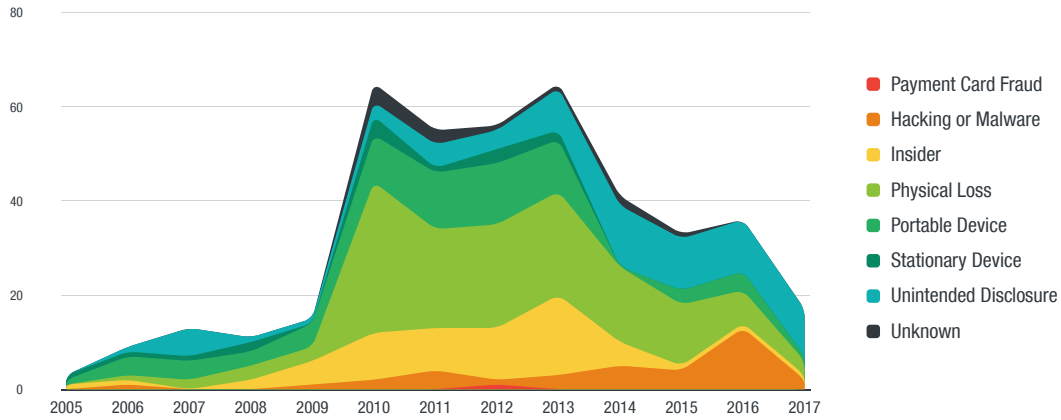


Figure 3. Number of incidents for hospital data breach methods from January 2005 to July 2017

The WannaCry incident was the highest profile case among a slew of healthcare-related ransomware attacks, but ransomware has been affecting the entire cyberthreat landscape for a long time. Ransomware encrypts data such as documents, folders, databases, among others, on the victim's computer, making them inaccessible, and demands a ransom payment in the form of digital currency like Bitcoin to decrypt the data. Ransomware will typically use email phishing and drive-by downloads as the main infection vector, but recent ransomware families like WannaCry have built-in worm-like functionality. The end goal, as with many attacks, is profit.

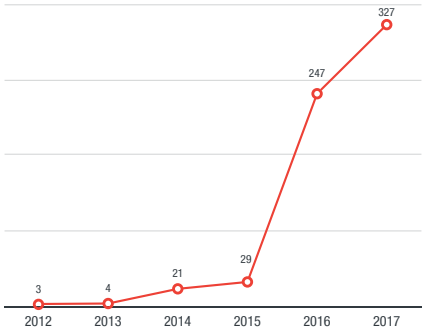


Figure 4. Annual number of ransomware families since 2012

Finally, and perhaps fortunately, we found only a handful of reports about compromised medical device incidents, none of which ended with the attackers sending any commands to the devices.[24] In the next section we will examine how exposed medical devices and systems are in healthcare networks.

Exposed Devices and Systems in Healthcare Networks

The internet of things (IoT) is fast becoming the new norm, connecting everything from computers, mobile devices, cars, industrial robots, home appliances, and even smart clothing to the internet. This interconnected world is very exciting and has created new and unique opportunities to improve our lives. But truth be told, today's society is adopting connected technologies at a faster rate than we are able to secure them. There is a strong likelihood that some of our internet-connected devices and systems may be inadvertently exposing information about us and our surroundings online, and that could potentially jeopardize everyone's safety and security.

The diagram in Figure 5 shows what a typical modern healthcare facility looks like in terms of how connected every part of the hospital is to the HIS. Note, this diagram is not meant to be comprehensive, but merely illustrative of the connected nature of an IoT-enabled environment.

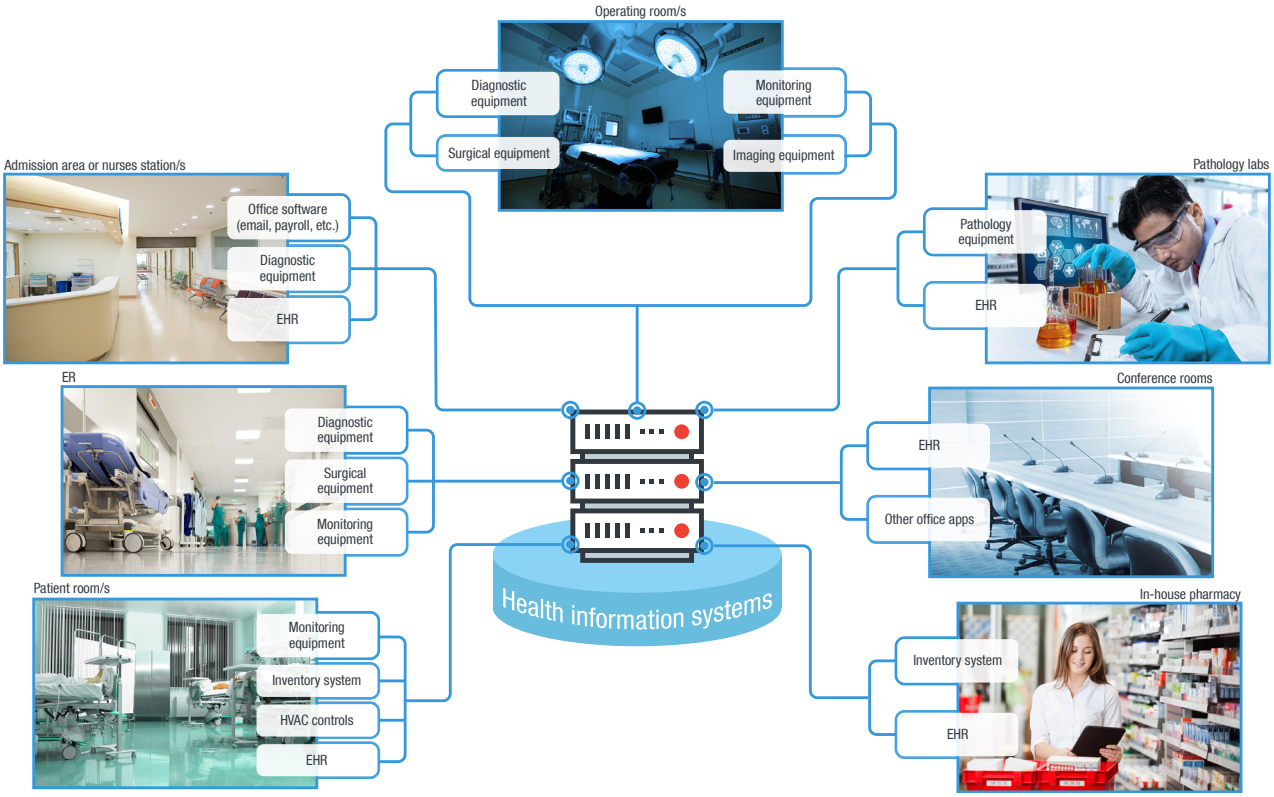


Figure 5. The connectedness of devices and systems to the health information system

In order to further understand the risks facing medical devices and information systems, we determined whether and how many healthcare-related cyber assets were exposed on the internet. It is important to note that when a device or system is exposed on the internet, it does not automatically imply that the cyber asset is vulnerable or compromised. It simply means that the device or system can be remotely accessed over the internet.

What is Shodan?*

Shodan is a search engine for internet-connected devices. It provides an easy one-stop solution to conduct Open-Source INTelligence (OSINT) gathering for different geographic locations, organizations, devices, services, etc. Software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in the exposed cyber assets. However, an adversary can also use Shodan to perform detailed surveillance and gather intelligence about a target, which is why Shodan has been called the World's Most Dangerous Search Engine.[25]

* *DISCLAIMER: AT NO POINT DURING THIS RESEARCH DID WE PERFORM ANY SCANNING OR ATTEMPT TO ACCESS ANY OF THE INTERNET-CONNECTED DEVICES AND SYSTEMS. ALL PUBLISHED DATA, INCLUDING SCREENSHOTS, WERE COLLECTED VIA SHODAN. NOTE THAT ANY MENTION OF BRANDS IN THIS RESEARCH DOES NOT SUGGEST ANY ISSUE WITH THE RELATED PRODUCTS, ONLY THAT THEY ARE SEARCHABLE IN SHODAN. FURTHERMORE, THE ANALYSIS WAS DONE USING SEPTEMBER 2017 DATA, SO GIVEN THE FLUID NATURE OF THE INTERNET, THE STATE OF EXPOSURE MAY CHANGE.*

For our research, we searched for exposed devices and systems in hospitals and clinics using the Shodan web interface (https://www.shodan.io/) and downloaded the raw results for further analysis. The basic unit of data that Shodan gathers is called the banner, textual information that describes a service on a device. The content of the banner varies depending on the type of service. In addition to the banner, Shodan also grabs metadata about the device, such as its geographic location, hostname, operating system, and more.[26]

One of the quirks of searching for devices on Shodan is that exposed devices can't always be traced back to the organization to which they belong. The most common reason for this is the organization name that Shodan reports the device is registered to oftentimes also happens to be the name of the Internet Service Provider (ISP). Without knowing the ISP's confidential customer data, there is no way to map the device to the owner. To avoid false positives, we narrowed our Shodan searches using the following search filters: *"isp:hospital"*, *"org:hospital"*, *"isp:clinic"*, and *"org:clinic"*. Luckily for us, many hospitals and clinics around the world register their devices or systems using their own organization names, or mark themselves as the ISP. This strategy of narrowing the Shodan searches has the benefit of having few, if any, false positives, but the downside risk is that we are only collecting a subset of the actual number of exposed devices in hospitals and clinics. For the purposes of this research, it was more desirable to have high-confidence verifiable results vs. larger data sets that may contain false positives. Shodan also has built-in modules (*_shodan.module*) that can identify protocols. We extensively used the *_shodan.module* classifications in our analysis. On October 17, 2017, we notified US-CERT of the vulnerabilities identified in this report.[27]

Why are devices exposed and what problems does exposure create?

We define exposed cyber assets as internet-connected devices and systems that are discoverable on Shodan or similar search engines and can be accessed via the public internet. When we say a certain device or protocol is exposed, we do not mean to imply that the cyber asset is automatically vulnerable or compromised — we simply mean that the device or protocol is remotely accessible via the internet.

Some of the common reasons that hospitals and clinics leave their systems and devices exposed online include the following:

- Incorrectly configured network infrastructure that allows direct device and system access
- Internet connection as a requirement for the system or device to function correctly
- Remote access enabled for remote troubleshooting or remote operations

Since an exposed device is reachable and visible to the public, attackers can take advantage of the available information about the machine either via Shodan or by directly profiling the machine using a variety of network tools such as nmap in order to collect information on the device (including the potential vulnerabilities of the said device) and use that information to mount an attack on it. Threat actors could get access to sensitive data, including webcam feeds; use access to move laterally through the network to commit espionage, sabotage or fraud; or compromise exposed cyber assets to launch DDoS attacks, become part of botnets, host illegal data,or hold hostage for ransom. Furthermore, cyber assets that operate critical infrastructure can jeopardize public safety if compromised.

The exposed information we were able to locate in Shodan belong to any one of the following categories:

- Exposed medical images
- Protocols
- Databases
- Exposed industrial controllers
- Healthcare systems software network misconfigurations

We discuss each of these categories in more detail in the following sections.

Exposed Medical Images

Digital Imaging and Communications in Medicine (DICOM®) is the "international standard to transmit, store, retrieve, print, process, and display medical imaging information," enabling the integration and interoperability of medical imaging devices such as scanners, servers, workstations, printers, network hardware, and Picture Archiving and Communication Systems (PACS) from multiple manufacturers.[28] The DICOM Information Object Definition encodes data produced by a wide variety of medical imaging devices used in procedures such as CT (computed tomography) scan, MRI scan, ultrasound, X-ray, fluoroscopy, angiography, mammography, PET (positron emission tomography) scan, endoscopy, etc. The devices and systems that process these medical images also support DICOM and include PACS, image viewers and printers, CAD (computer-aided detection/diagnosis systems), RIS (radiology information systems), EMR (electronic medical records) or EHR (electronic health records) systems, etc.

Port 104 has been assigned to DICOM for communications over TCP or UDP. Ports 2761, 2762, and 11112 are also registered DICOM ports but are rarely used. Searching Shodan with *tag:medical* returns a list of devices/systems with port 104 open and the banner containing text "DICOM Server Response." The graph in Figure 6 shows exposed DICOM devices/systems plotted against Top 20 countries.

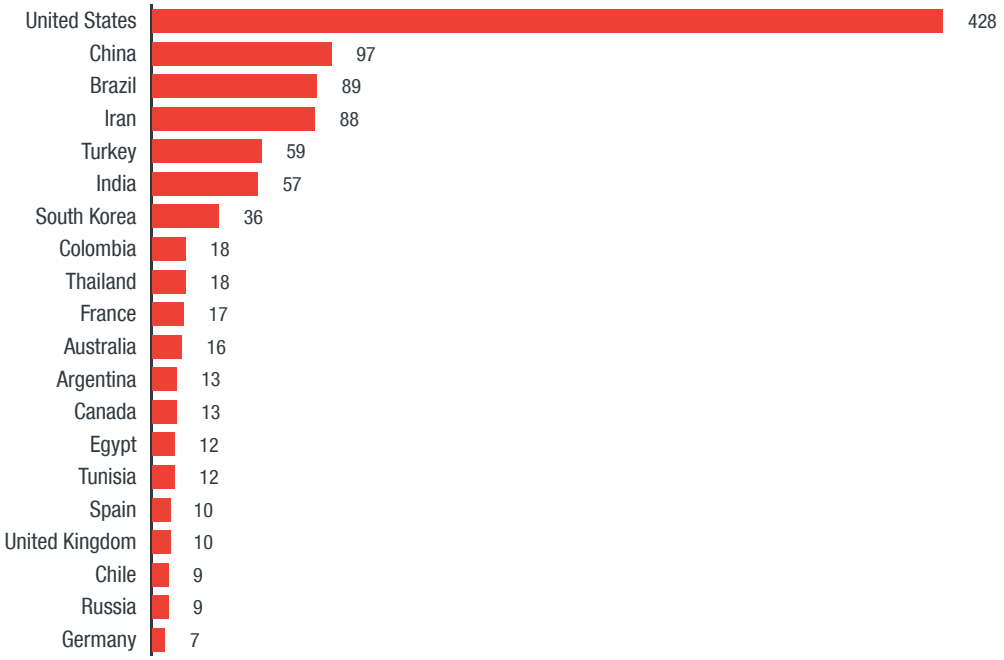


Figure 6. Top 20 countries with DICOM servers exposed

- As expected, the vast majority of DICOM devices are registered to their ISPs, thus making it very difficult to identify the actual owners of the devices.
- There were 21 universities listed as device owners. Some of these university names also include the medical department name, e.g., Neurology, Radiology, etc., thus positively confirming these are medical systems.
- Going through the raw banner data, we managed to identify the DICOM application names. Without giving out the specifics, we found DICOM applications from Asteris, Offis, Datamed, MultiTech, Medweb, Raypax, etc. The software name and version information are embedded in the banner data and a perpetrator can use this information to search for known vulnerabilities and exploit them to compromise the device/system.
- Shodan managed to fingerprint the device operating system (OS) for only 22 devices: 15 Microsoft® Windows® 7 or 8, and seven Windows XP. Our educated guess is, all the DICOM devices/systems that Shodan discovered are application servers that store and process medical images.

These DICOM servers should not be exposed online. Exposed medical systems potentially jeopardize critical data such as patients' PII and medical records. Perpetrators can also disrupt hospital and clinic operations by corrupting the data, issuing incorrect device commands, or infecting the systems with ransomware, among others.

Exposed Ports

Protocols refer to standards used to define how computers communicate over a network. Exposed ports in the context of this research means that we were able to view the port numbers or the services that are in use and open on the internet. Vulnerabilities in the related protocols can be exploited to successfully compromise the devices or systems that run them.

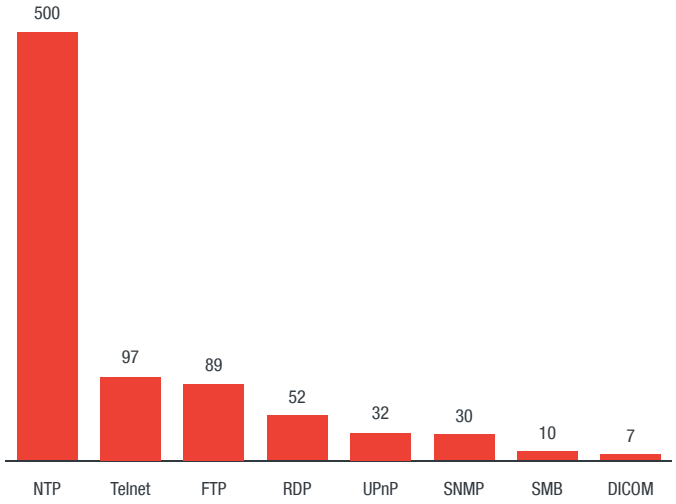


Figure 7. Exposed protocols in clinics and hospitals

We found many exposed ports/services inside hospitals and clinics, and from there we selected the following eight ports/services that we think, if abused, will introduce the greatest amount of cyber risk for the hospitals and clinics:

- **NTP** (Network Time Protocol) is one of the internet's oldest protocols and is designed to synchronize time between computer systems communicating over unreliable variable-latency network paths. Connections between computers and NTP servers are rarely encrypted, making it possible for hackers to perform man-in-the-middle (MitM) attacks that reset clocks to times that are months or even years in the past. Hackers can wreak havoc on the internet with these NTP MitM attacks.[29, 30] An attack that prevents sensitive computers and servers from receiving regular time-synchronization updates can cause malfunctions on a massive scale. These attacks can be used to snoop on encrypted traffic or bypass important security measures such as DNS Security Extensions (DNSSEC) specifications, which are designed to prevent DNS record tampering. The most troubling scenario involves bypassing HTTPS encryption by forcing a computer to accept an expired transport layer security certificate.
- **Telnet** (Teletype Network) is an internet protocol used to provide a bidirectional eight-bit byte oriented communications facility. Telnet allows a standard method of interfacing terminal devices and terminal-oriented processes to each other. The three key features of Telnet are: i) network virtual terminal, ii) negotiated options, and iii) symmetric view of terminals and processes.[31] In a Telnet session, all data

is sent and received in clear text, that is, there is no end-to-end content encryption. This makes Telnet highly vulnerable to packet sniffing attacks.

- **FTP** (File Transfer Protocol) is a standard network protocol used to transfer files between a client and server on a computer network.[32] FTP is enabled by default on most web servers, which makes it a lucrative target for exploitation by hackers. Once FTP is exploited and the server compromised, the hackers will have access to all hosted files and can upload new malicious files.
- **RDP** (Remote Desktop Protocol) is a proprietary protocol developed by Microsoft that provides users with a graphical interface to connect to another computer over a network connection. The users employ RDP client software for this purpose, while the target computer must run RDP server software.[33] RDP has traditionally been abused to exfiltrate data as part of a targeted attack, to steal information that can be sold in Deep Web marketplaces, and to integrate the hijacked systems into botnets. For instance, the Crysis ransomware was discovered using brute-forced RDP as one of its infection vectors.[34]
- **UPnP** (Universal Plug & Play) is a set of networking protocols that permits networked devices, such as personal computers, printers, internet gateways, WAP, and mobile devices, to seamlessly discover each other's presence on the network and establish functional network services for data sharing, communications, and media.[35] SSDP (Simple Service Discovery Protocol) is used for the discovery of UPnP devices. It was first introduced in 1999 and is used by many routers and network devices. The Metasploit framework includes many UPnP and SSDP modules that can be used to exploit and compromise devices with UPnP/SSDP enabled.
- **SNMP** (Simple Network Management Protocol) is a popular protocol for network management. It is used for collecting information and configuring network devices such as servers, printers, hubs, switches, and routers.[36] SNMP provides a convenient way for hackers to figure out the network topology map, which they can later use for lateral movement within the target network. SNMP can also be used to manage devices, e.g., to shut down a network interface — this makes it a dangerous tool in the hands of malicious hackers.[37] Another big threat is hackers abusing devices configured to publicly respond to SNMP requests to amplify DoS attacks. The hackers use the IP address of the individual/organization they are targeting as the spoofed source of the SNMP request. Then they send bulk requests to devices configured to publicly respond to SNMP requests, which results in a flood of SNMP GetResponse data being sent from the devices to the victim(s).[38]
- **SMB** (Server Message Block) was brought into the limelight by the recent WannaCry ransomware outbreak. WannaCry exploits an SMB vulnerability (MS17-010) to spread and infect unpatched systems. WannaCry demands $300 ransom in Bitcoins, with the ransom doubling after three days. If no payment is received in a week's time, then all the encrypted files on the system will be deleted. One of the hardest-hit victims of WannaCry was the National Health Service (NHS) trust in the U.K. NHS trust hospitals affected by WannaCry were reported to have been unable to access patient

records and to have diverted ambulances to other area hospitals not affected by WannaCry and cancelled scheduled patient appointments, scans, and surgeries.

- **DICOM** (Digital Imaging and Communications in Medicine) is a standard for storing and transmitting medical images enabling the integration of medical imaging devices from multiple manufacturers. We already discussed DICOM in the previous section, but the results presented here are for DICOM-compatible devices/systems confirmed to be inside hospitals and clinics.

Interestingly, in our recent roundup *A Look Into the Most Noteworthy Home Network Security Threats of 2017*, we tracked around 2.5 million inbound attacks using brute-force logins via RDP, SQL, POP3, and SMTP. While the report focused on home networks, attacks like these do not discriminate. And if home routers can be compromised in this manner, then these attacks can just as easily find their way to services or protocols used by healthcare networks that we found exposed.

Exposed Databases

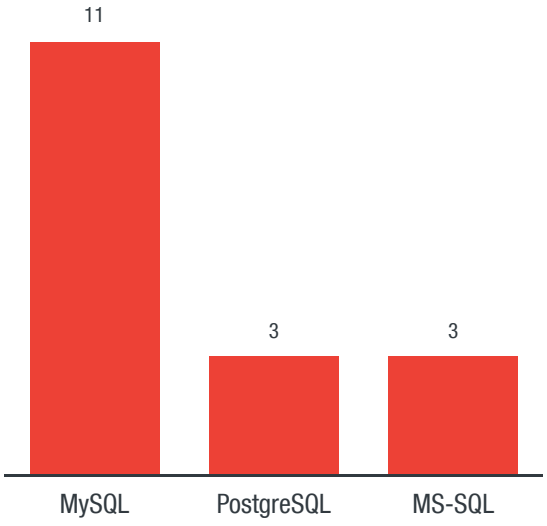


Figure 8. Exposed databases in clinics and hospitals

Databases play a critical role in modern hospital operations; EHR/EMR and PACS are primarily database applications that doctors, nurses, and medical technicians use to plan out and track patient treatment. Databases are also treasure troves of critical/sensitive/important data, which makes them lucrative targets for hackers. For this reason, database theft incidents (full database dumps stolen) are regularly reported in news stories about hackers attacking organizations. Another major threat is when databases are encrypted by ransomware and the hackers demand payment to release the decryption keys.

From the Shodan results, we find MySQL as the most popular database exposed inside hospitals and clinics, while MS-SQL and PostgreSQL have smaller exposure footprints. It is fairly safe to assume EHR/EMR and PACS use MySQL, PostgreSQL, MS-SQL, etc., as their primary data store, and thus, exposed databases inside hospitals and clinics can jeopardize both hospital operations and the critical patient data they store.

MongoDB, a NoSQL database, is seeing an uptick in usage and we might see some exposed databases of this type in the healthcare space very soon.

Exposed Industrial Controllers

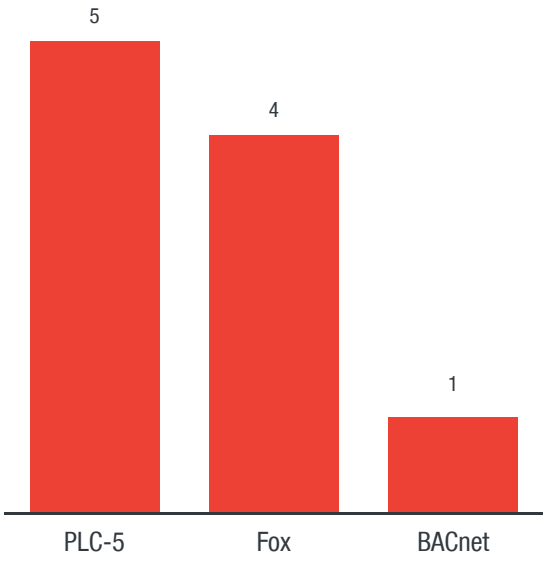


Figure 9. Exposed controllers in clinics and hospitals

One of the interesting things that we discovered in the Shodan results was that there were exposed industrial controllers inside hospitals and clinics. The Shodan modules identified three: PLC-5, Tridium Fox, and BACnet.

- **BACnet** is a communications protocol for Building Automation Control networks. BACnet was designed for communications by applications such as heating, ventilating, and air conditioning (HVAC) control, lighting control, building access control, and fire detection.[39]
- **Fox** is a proprietary protocol that is part of the Niagara Framework developed by Tridium Inc. The Niagara Framework is a universal software infrastructure that allows building control integrators and mechanical contractors to build custom web-enabled applications for accessing, automating, and controlling smart devices real-time via the LAN or the internet.[40] Fox and BACnet are the two major building automation control systems.

- **PLC-5** is a programmable controller that supports CIP (Common Industrial Protocol), which is a set of services and messages for control, security, synchronization, configuration, information, and so forth, and which can be integrated into Ethernet networks and the internet. CIP has a number of adaptations providing intercommunication and integration for different types of networks. PLC-5 supports *EtherNet/IP* — an adaptation of CIP to TCP/IP.

Compromising exposed building automation controls can allow a hacker to "turn off the lights" inside the hospital. Compromising exposed building controls might also give hackers access to the backup generators, which they can then disable or sabotage. Doomsday scenarios like these are unfortunately not unrealistic, and extreme care should be taken to ensure building automation controllers are never exposed to the public internet.

Exposed Healthcare Systems Software

Shodan has an image search database (https://images.shodan.io/) for browsing screenshots that it has collected. Screenshots are collected from five different sources: Virtual Network Computing (VNC), RDP, Real Time Streaming Protocol (RTSP), XWindows, and webcams. We searched through the Shodan images database looking for examples of exposed medical systems, and our findings were quite alarming. All included screenshots were found in Shodan using search term *rfb authentication disabled*, i.e., they came from VNC servers that have authentication disabled, and thus, are open to all to access. Sensitive PII data has been redacted for privacy reasons.

An EMR is a database that holds medical and clinical data obtained at the health providers' office, such as medical history, diagnoses, medications, immunization dates, and allergies. An EHR database holds a comprehensive patient history that allows the patient medical history, such as progress notes, diagnoses, medications, immunization dates, allergies, lab data, and imaging reports, to move with them.[41] Electronic medical records and images are shared across different healthcare settings (such as laboratories, clinics, hospitals, doctor's offices, etc.) through network-connected enterprise-wide information systems, or other information networks and exchanges. We found several EHR/EMR system interfaces exposed on Shodan Images, two of which we share here. While some of these and subsequent screenshots were observed outside of North America, these show how likely such exposures can also happen in North American healthcare organizations.

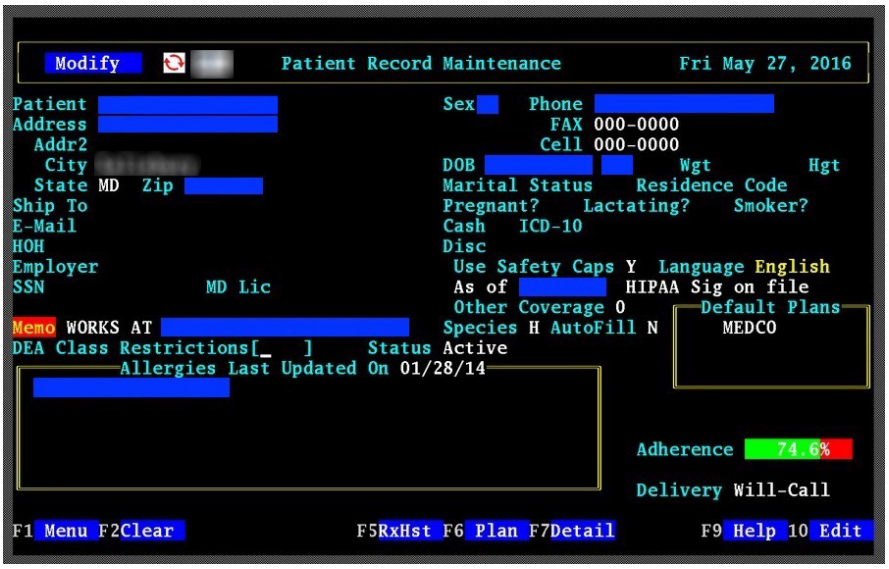


Figure 10. Exposed graphical user interface (GUI) for patient record maintenance containing various PII

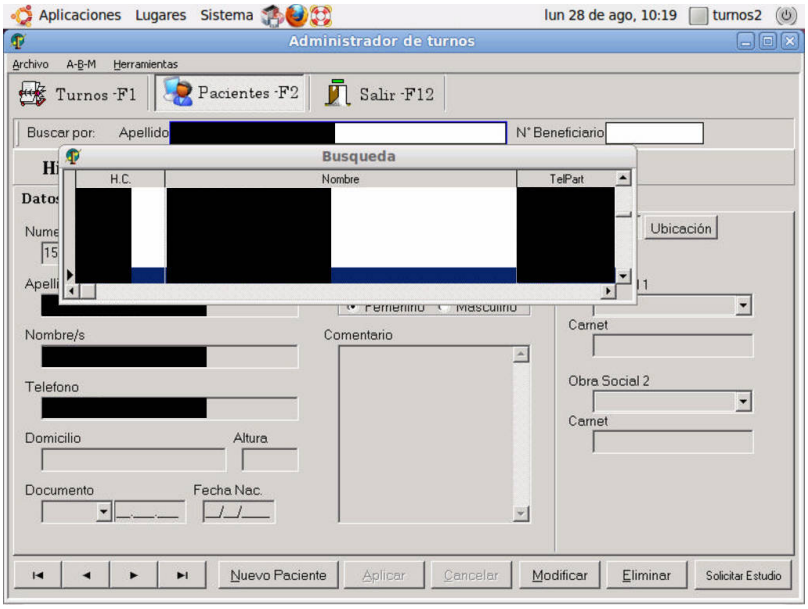


Figure 11. Exposed GUI for patient record maintenance containing various PII

We also found a patient scheduling/appointment system that contained the patients' diagnosis information exposed in Shodan Images.

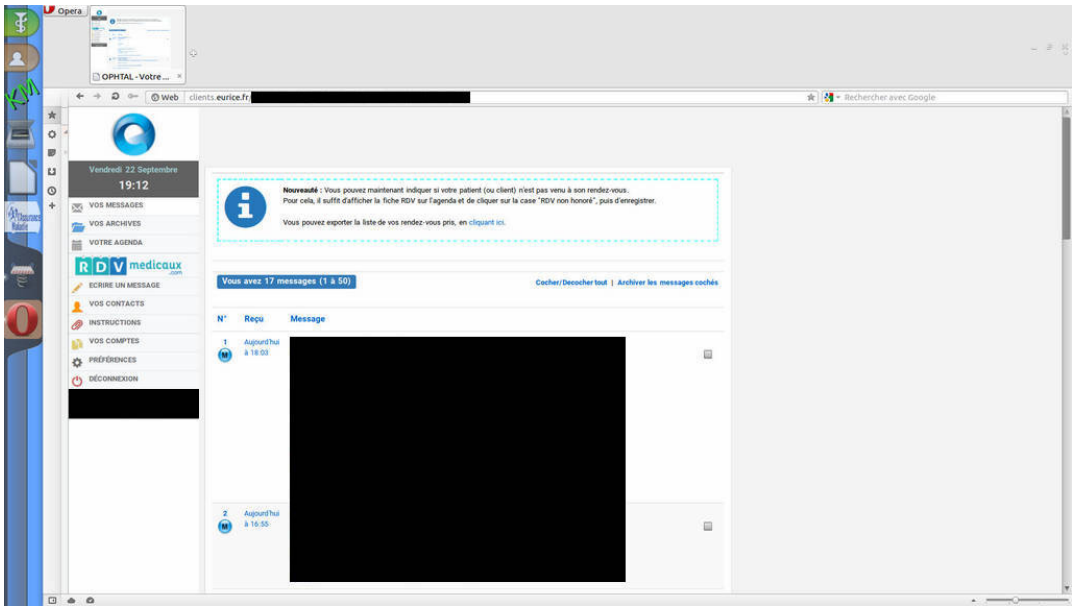
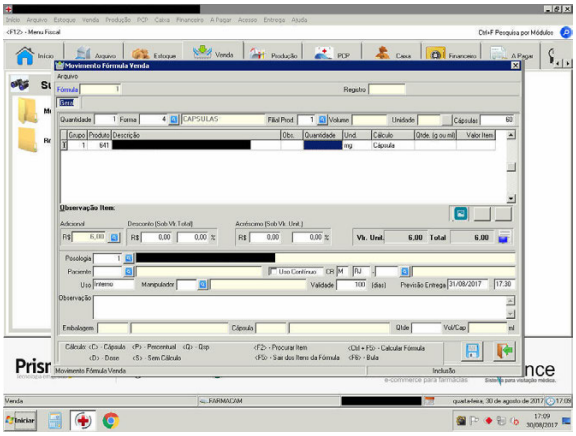


Figure 12. Exposed patient scheduling or appointment program GUI

One of the more common medical systems that we found exposed online via Shodan Images was pharmacy management software. This specialized software is used by pharmacies for various integrated management functions such as drug inventory, drug ordering, OTC management, narcotics tracking, patient data, patient prescription history, point-of-sale (PoS) transactions, drug insurance claims, prescriptions and refills, label printing, etc. Hospital pharmacies use similar management software that are integrated with the hospital's EHR/EMR systems and with the automated drug dispensing machines found in clinical departments and patient care floors.



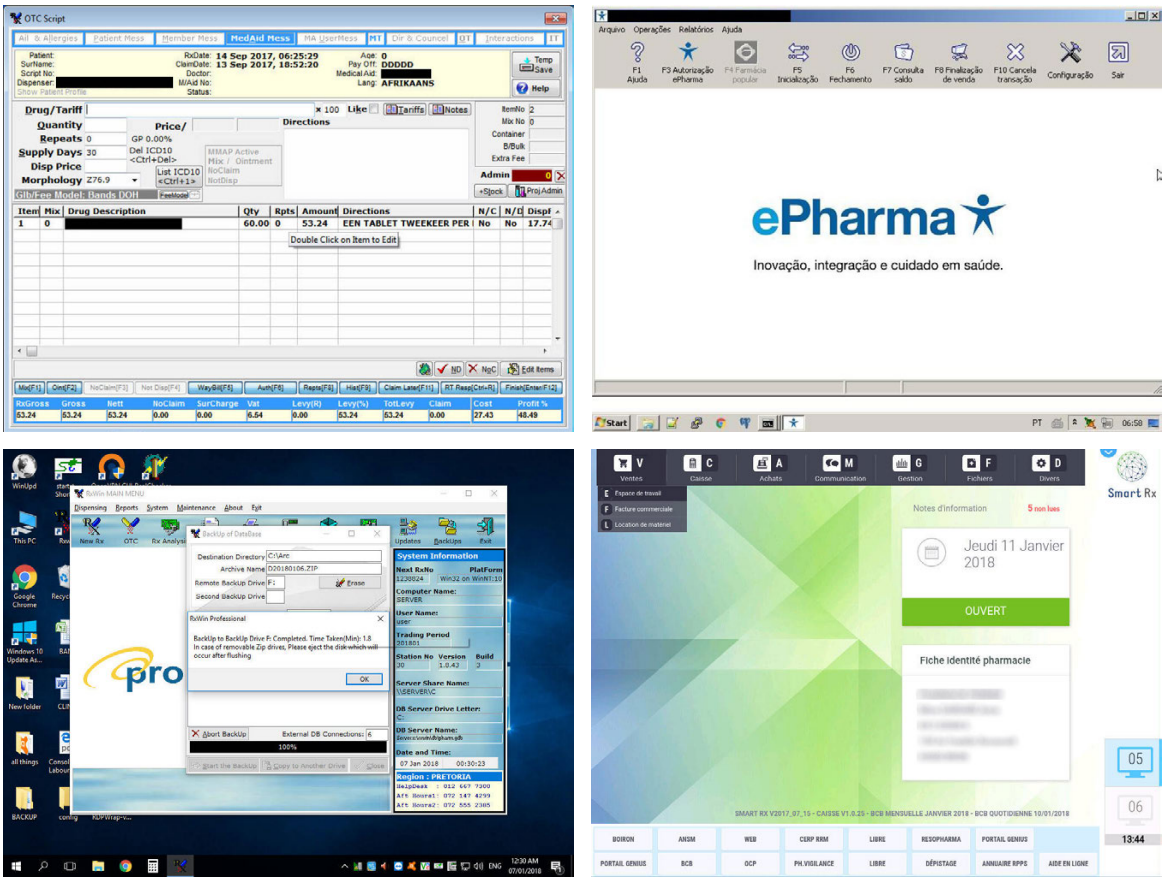


Figure 13. Exposed pharmacy management software GUI

These VNC servers are potentially accessible to all internet users, if they can identify them, which isn't difficult using an IoT search engine like Shodan. Exposed medical systems can potentially jeopardize critical data such as patients' PII, medical records, and financial/insurance information. Perpetrators can also disrupt hospital, clinic, and pharmacy operations by corrupting the data, issuing incorrect device commands, infecting the systems with ransomware, etc. The silver lining is, over several days of device-hunting in Shodan, we only found a handful of these systems online. The vast majority of medical systems/devices are properly protected and inaccessible to the public internet. But even finding a few of these systems exposed is proof enough that these systems can become exposed online if the network is not configured properly.

Network Misconfigurations

While searching for exposed devices and systems in Shodan, we came across some very unusual results: More than 79 percent of all the exposed devices/systems in hospitals around the globe can be traced back to one hospital in Canada. The following screenshot shows these unusual results (names and IP addresses redacted):

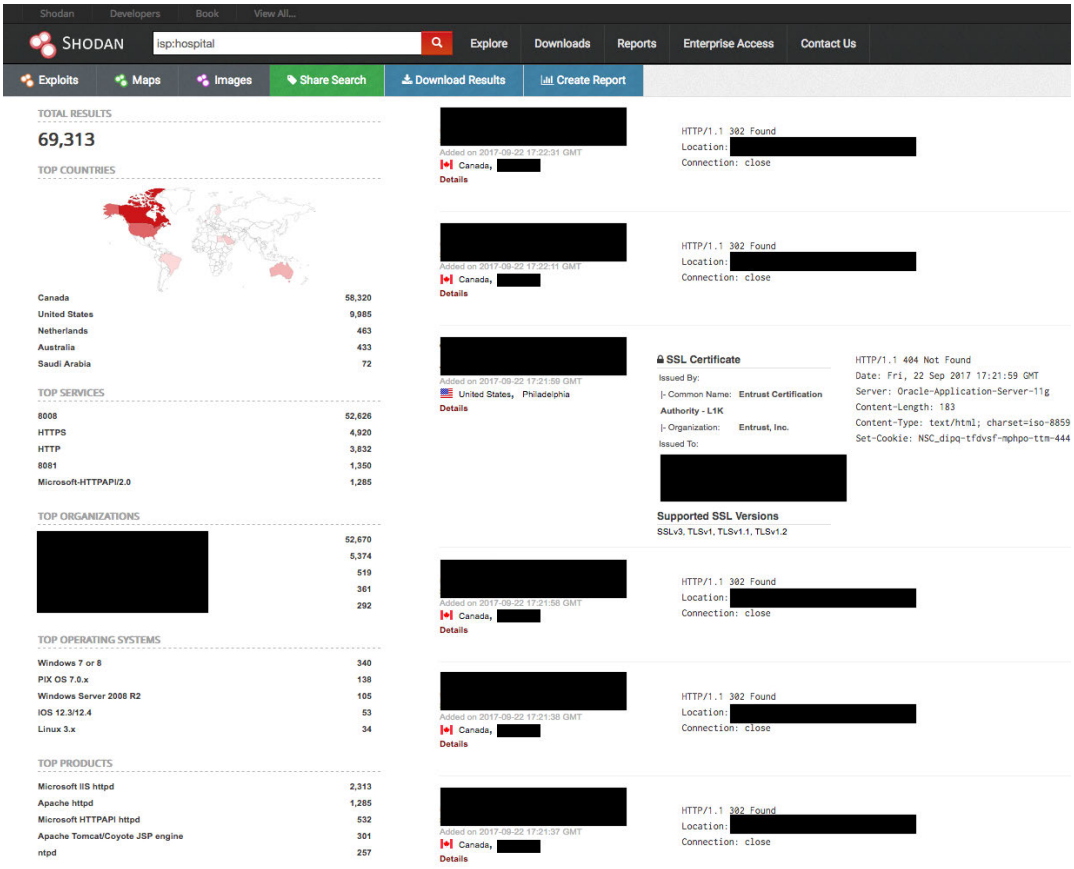


Figure 14. Shodan results page

Digging deeper into the results, we found the hospital in question had all its unused IP addresses redirecting to the domain: *unused.********.**.ca* (domain redacted for privacy reasons). While it is easy to find the entire IP address space allocated to an organization using WHOIS, unused IP addresses should not be exposed to the internet in this manner. This is most likely the case of a misconfigured proxy or bad proxy administration that Shodan has found. The underlying risk is that there might be other device/system misconfiguration issues inside this hospital that hackers might discover and exploit to compromise the network. We have reported our findings to the Canadian Cyber Incident Response Centre (CCIRC) so they can reach out to the hospital in question and advise them about their publicly visible proxy misconfiguration issues.

Healthcare Supply Chain Attacks

In addition to exposed medical devices and systems, we now take a look at an often-overlooked facet of hospital operations — the supply chain. Supply chain threats are potential risks associated with suppliers of goods and services to healthcare organizations where a perpetrator can exfiltrate confidential/sensitive information, introduce an unwanted function or design, disrupt daily operations, manipulate data, install malicious software, introduce counterfeit devices, and affect business continuity. The healthcare industry is more dependent than ever on cloud-based systems, third-party service providers, and vendors in the supply chain. Thirty percent of all breaches reported to the U.S. Department of Health and Human Services (HHS) public breach tool in 2016 were claimed to be due to breaches of business associates and third-party vendors,[42] which is all the more reason for us to look closely at where the systems' weaknesses lie.

NIST Recommends Cyber Supply Chain Risk Management

The National Institute of Standards and Technology (NIST), mandated by the U.S. government to develop frameworks for voluntary use by critical infrastructure owners and operators, revised its *Framework for Improving Critical Infrastructure Cybersecurity* to, among others, clarify the use of the framework to manage cybersecurity within supply chains.[43] In the revised section 3.3 of the document, NIST set forth terminologies an organization may use to communicate requirements among different interdependent entities in the supply chain.

NIST emphasizes the importance of supply chain relationships by including awareness of supply chain risks in its tiering of framework implementation from partial to adaptive. It also considers supply chain risk management (SCRM) a critical organizational function, where cyber SCRM is a set of activities needed to manage the cybersecurity-specific risk associated with external parties. Cyber SCRM aims to identify, assess, and mitigate "products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices within the cyber supply chain."

While this adequately captures the overall intent of the recommendation and should indeed be implemented where possible, understanding supply chain threats and risks in more detail can lead healthcare IT teams to develop specific policies that protect from them. We discuss the said threats in a subsequent section.

FDA Requires UDI for Devices

In a more industry-specific view, the FDA recognizes that the increasing connectedness of devices puts hospitals at risk of supply chain threats, prompting them to mandate Unique Device Identification (UDI) codes for all medical devices — either on the packages or on the device itself — in the U.S. in 2014 and to provide recommendations that help protect the medical supply chain via the *Postmarket Management of Cybersecurity in Medical Devices* guidelines in 2016.

The UDI alphanumeric code provides the version, model of a device, manufacturing batch number, expiration date of device, serial number, and date of manufacture. The information is entered into the FDA-administered Global Unique Device Identification Database (GUDID), which is available to the public at AccessGUDID (https://accessgudid.nlm.nih.gov/).[44] A patient can also use the database to verify if the UDI is the make and model of the device prescribed by their medical professional. If the patient does not find their UDI device code, it may be a counterfeit product.

Figure 15. Samples of medical device UDI bar codes[45]

The FDA's *Postmarket Management of Cybersecurity in Medical Devices* guideline encourages manufacturers to consider potential supply chain threats throughout the life cycle of the medical device. The FDA has also made it easier for device manufacturers and software developers to update medical devices without the need to go through a new regulatory review to add software updates.[46] The FDA has also recommended monitoring third-party software for new vulnerabilities throughout the device's total product life cycle, engaging stakeholders across the cybersecurity community to obtain information about vulnerabilities, and developing plans to address vulnerabilities.

However, the recommendations listed in the FDA document are just guidelines and no practical steps have been taken to enforce them. While this is a good start to make manufacturers consider security solutions early in the medical device development process, hospital IT network defenders must do more to protect patients.

Where are the risks in hospital supply chains?

In practice, there are numerous potential entry points that threat actors can use to compromise the hospital supply chain. While we do not intend for this list to be complete, this list of risk situations by category can help illustrate how detailed IT teams need to be in their review of their own security posture when it comes to their supply chains.

- **Medical product/medicine/supplies manufacturer** — The hospital/clinic acquiring the product may not have control over the manufacturing process, specifically whether it is secure enough to prevent threat actors from tampering with the product during manufacture.
- **Distribution center** — The hospital/clinic eventually buying the product may not have intimate knowledge of the security enforced by the distribution centers, or whether their employees or their third-party contractors have access to the products prior to shipping to actual hospital suppliers.
- **Shipping and transportation companies** — The hospital/clinic buying the product may not have intimate knowledge of the security enforced by their or the distribution center's logistics vendor, or whether their employees or their third-party contractors have access to the products prior to delivery to end users.
- **Suppliers** — The hospital/clinic buying the products or services may not have control over the storage or repacking practices of suppliers, if any, or whether cybersecurity practices are in place in the supplier's network the hospital is expected to be connecting to regularly.
- **Vendor/contractor (equipment, HVAC, ISP, telephony or the like) or hospital staff** — The hospital/clinic may not have control over vendor hiring practices or may not be enforcing sufficient background checks on their own staff, either of whom may introduce a threat into the network.
- **Mobile health (mHealth) app/HIS/other software developer** — The hospital/clinic may not have control or knowledge about the security of the code or the developers' coding practices, whether the developer has ensured enough safeguards are in place to prevent the discovery or exploitation of vulnerabilities in their apps or software. Taken further back up the supply chain, the operating system used in various segments in healthcare networks can have vulnerabilities.
- **Outdated and unpatched firmware in medical devices/equipment** — The hospital/clinic may not realize that even medical devices/equipment have an embedded firmware that must be updated when necessary, or that they may be infected with malware. Threat actors can leverage these open security holes to either compromise the hardware or move laterally inside the network.
- **Previous employees or non-core services staff** — The hospital/clinic may not have control over the behavior of previously employed staff (if IT has not terminated their access completely) or current vendor staff to check whether they are abusing access privileges or are using hospital resources in an unsecure manner. They may even take advantage of weak authentication procedures knowing what they do about internal processes.

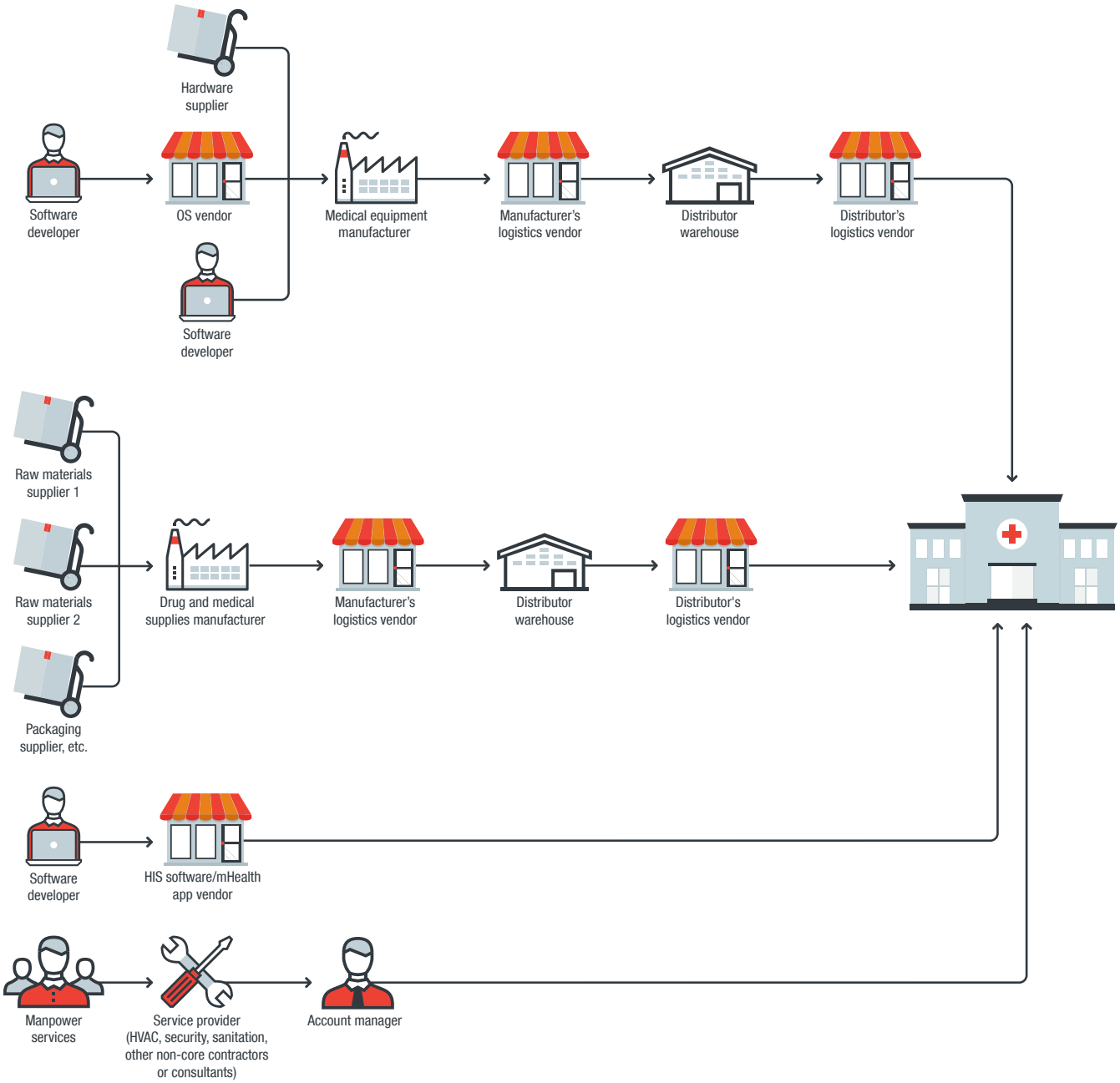


Figure 16. Hospital supply chain diagram

What types of attacks are most common in hospital supply chains?

Supply chain threats arise as a result of outsourcing suppliers, and the lack of verifiable physical and cyber security practices in place at the suppliers. Suppliers do not always vet personnel properly, especially companies that have access to patient data, hospital IT systems, or healthcare facilities. Vendors do not always vet their own products and software for cybersecurity risks, and may also be outsourcing resources as well. This allows perpetrators to exploit sensitive information across the supply chain. We have identified the seven major supply chain threat vectors that perpetrators may use in the healthcare industry:

Firmware attacks on devices

Perpetrators can access and modify the firmware source code of a medical device to add backdoors, which can then be pushed out via existing auto-update mechanisms. Firmware updates are done separately from the medical device's software, which requires patients to visit their doctor or healthcare facility to implement the changes. In August 2017, over half a million pacemakers needed a firmware update to protect users from hackers controlling the pace, depleting batteries, and allowing connections to the device through Wi-Fi.[47] In early 2015, a certain type of infusion pump was found to have a vulnerability that allowed unauthenticated users root access. The infusion pumps did not verify the authenticity of the firmware updates prior to installing them.[48] In 2013, over 300 medical devices across 40 vendors were found to have issues that could allow unauthorized users to modify the device's firmware.[49] These devices were found to have hard-coded passwords. These types of firmware attacks could allow a perpetrator to change the medical device's functionality, thus putting the patient health at risk. Many medical device manufacturers do not have patching procedures to update firmware.

Compromises to mHealth mobile applications

There are more than 250,000 mHealth apps for Android™ and iPhone® devices.[50] mHealth mobile apps can be compromised to change functionality, deliver fatal-level dosage, expose personal health data, penetrate other company systems, and cause Health Insurance Portability and Accountability Act (HIPAA) violations. A report by Arxan revealed that 84 percent of FDA-approved mobile health apps tested had at least two critical security vulnerabilities while U.K.'s NHS had 86 percent.[51] The top two vulnerabilities found were a lack of binary protection and insufficient transport layer protection. mHealth apps also have the risk from their third-party companies that supply services for hosting, server, and cloud solutions. An IBM and Ponemon Institute report in 2015 revealed that 50 percent of large organizations did not have a budget for protecting mobile apps. According to a device management company research, 22 percent of IT budgets are invested in mobile app security testing and 50 percent of healthcare facilities say they do not control all the mHealth apps installed on their

networks. The research suggested healthcare companies are spending more resources on the development of the applications and hardly any on security testing.[52] mHealth apps are not required to report any breaches to the HHS public site, making tracking of any compromise harder to address.

Compromising source code during manufacturing

Perpetrators can access and modify the source code of a vendor by installing a backdoor or rooting the device. Because hospitals tend not to test device security before installing it on their networks, this can cause malware infections, exfiltration of data, sharing data with third-party vendors or advertisers, etc. Malware has been installed on Original Equipment Manufacturers (OEMs) products before but no data about incidents involving medical devices have been publicly disclosed as of 2017. However, many hospitals use non-medical devices like thumb drives and mobile devices on the network that may not go through a cybersecurity review process. In 2015, over 17,000 Chinese Android tablets sold on Amazon and other retailers were found infected with the Cloudsota Trojan at the operating level, so it couldn't be removed.[53] Researchers in early 2017 discovered multiple Android phones from Samsung, Lenovo, and LG were pre-installed with malware somewhere along the supply chain. Malware detected included Loki, Slocker, a mobile ransomware, infostealers, and adware.[54] In 2016, a healthcare organization unknowingly sent 37,000 malware-infected USB thumb drives to their offices nationwide. The manual of procedure codes for that year included the flash drive on the back pocket.[55]

Insider threats from hospital and vendor staff

Insider threats can be intentional, for example data theft, or unintentional, for example, accidental disclosure or disposal of records. Insiders could be motivated by money, ideology, coercion, ego, revenge, and politics. Hospitals perform background checks on staff before the onboarding process, but this is sometimes outsourced to third parties who may not have accurate details. Third-party vendors, seasonal staff, and contractors who work at hospitals may not have the same level of background checks performed. In 2012, a third-party background check company settled for $2.6 million dollars for errors in consumer background checks.[56] Also, background checks should be performed regularly and not just once when an employee is first hired. Hospital staff interacts with hundreds of vendors on a daily basis; unfortunately hospitals can't always vet who is on the other side of these conversations. Likewise, employees that have left or changed jobs may still have access to critical systems if the IT team or account administrator neglects to terminate their system accounts in a timely fashion. Sixty percent of breaches in February 2017 were the result of insider threats. This number dropped to 44 percent in March 2017 according to a report from Protenus Breach Barometer.[57] Stolen patient information from a Florida hospital ER department was used to file fraudulent tax returns after a former employee, who worked in maintenance and

housekeeping, copied names and social security numbers (SSNs) back in 2012.[58] Another healthcare organization, this time in Atlanta, had a senior audit advisor send copies of patient healthcare records to their personal email account. According to the former employee, after being caught, the patient records were sent for "future employment references."[59]

Compromises to websites, EHR, and internal hospital software

Perpetrators can attempt to compromise hospital websites, EHR software, and internal portals used by hospital staff and vendors. Web-based EHR systems suffer from many common vulnerabilities that might give attackers access to backend systems and data. In 2016, a hacker modified the code to a third-party vendor's server being used to store credit card information of patients paying a hospital in California, compromising 714 patients' billing and health information.[60] In June 2016, an EHR cloud service used by multiple hospitals was compromised and malware installed on their systems. More than 260,000 patients were notified that diagnosis codes, treatments, social security numbers, address, information about appointments, and contact information were exposed.[61]

Spear phishing from trusted email account

A perpetrator can gain control of vendor credentials and send clients emails that appear legitimate. The U.S. Internal Revenue Service (IRS), in February 2017, warned hospitals of W-2 phishing scams. A cybercriminal sends an email, pretending to be an executive or payroll staff, and asks for a list of all employees and their W-2 information. In some cases, the email also requests a wire transfer to an account as part of a business email compromise (BEC) attack.[62] This phished information was used to file fraudulent tax returns.[63] In early 2017, several healthcare organizations in the U.S. became victims of W-2 phishing scams. W-2 data were offered for sale on multiple underground forums and dark web sites in 2017.[64]

Third-party vendors

Third-party vendors have credentials that include logins, passwords, and badge access, all of which can be compromised. Third-party vendors sometimes also store physical records, hospital office equipment, and medical devices. A hospital in Illinois had transitioned to EHR but stored paper copies of patient records and old office equipment in a building that was sold without them being notified. There were 8,300 patient records stored there that were eventually retrieved.[65] In 2009, a night shift security guard, whose hacker name is GhostExodus, installed a botnet in the hospital's HVAC controllers; he used his work access badge to enter the building he was supposed to be guarding.[66] Hackers breached a healthcare network in Alabama in May 2017, through a cloud hosting provider, which had an unpatched vulnerability. This allowed the hackers to access and exfiltrate cloud-stored patient information.[67]

These numerous breach examples should alert healthcare IT teams about the additional risks brought about by third-party connections — physical and digital — inside any adequately secured HIS. A risk-based vendor management program under a comprehensive enterprise risk management/governance framework will assist in minimizing supply chain threats. We provide more guidance in the recommendations section.

In the next section, we apply the DREAD threat modeling method to assist healthcare IT security teams in understanding the level of risk that certain threats carry in the healthcare environment.

Threat Modeling the Hospital Ecosystem

Threat modeling is a technique that has long been used by software developers to assess the security risks in their code. It can also be applied to systems and can be a very good tool for assessing overall system security. It provides a systematic approach to identifying, classifying, and quantifying the amount of risk presented by each evaluated threat.[68]

The modern hospital is a large, complex, interconnected ecosystem with thousands of endpoints and users. The size, complexity, and functions of this ecosystem create many, and at times unpredictable, attack surfaces. In this section we disseminate the common cyberattack vectors across critical systems inside hospitals and apply the industry-standard DREAD threat model to calculate the risk ratings for these vectors. The DREAD model allows IT teams to rate risks of these by looking at five categories: Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability.

Critical Systems Inside Hospitals

For our threat modeling exercise, we identified three broad categories of devices and systems that are used in hospitals. We further discuss these devices and systems in the Appendix section of this paper. This is by no means a comprehensive list of all the devices and systems present inside a hospital, but rather a broad cross section of them. Threat assessment for these three “broad” categories of devices and systems is expected to provide a good understanding of the everyday cyberthreats hospitals face, and help the IT staff and senior management prioritize and develop cyber defense strategies.

Category	Devices and Systems
Medical Devices	Imaging, e.g., MRI, CT, X-Ray, Ultrasound, etc. Infusion pumps Respiratory ventilators Anesthesia machines Heart-Lung machines Dialysis machines Robotic surgical tools Radiotherapy systems Active and passive monitoring systems
Information Systems	EHR/EMR systems Laboratory information systems Radiology information systems Picture Archiving and Communication Systems (PACS) Mobile health applications
Hospital Operations	Work order and staff scheduling systems Office applications, e.g., payroll, email, fileservers, databases, etc. Drug and equipment inventory systems Hospital paging systems Building control systems Barcode scanners and printers Automated drug dispensers Pneumatic tube transport system

Table 1. Categories of healthcare systems and devices

The DREAD Threat Model

Threat modeling allows us to apply a structured approach to security and to address the top risks that have the greatest potential impact on the application.[69] The DREAD threat model can be used to perform qualitative risk analysis.[70] **Qualitative risk analysis is opinion based**; it uses rating values to evaluate the risk level. For this exercise, we used our cybersecurity expertise and monitoring of the healthcare threat landscape to determine our rating of certain threats. We arrived at the risk rating for a given threat by asking the following questions:[71, 72]

- **D**amage potential — How great is the damage to the assets?
- **R**eproducibility — How easy is it to reproduce the attack?
- **E**xploitability — How easy is it to launch an attack?
- **A**ffected users — As a rough percentage, how many users are affected?
- **D**iscoverability — How easy is it to find an exploitable weakness?

We created the following threat ratings table for our hospital risk analysis.

	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker subverts the system and can inflict serious damage, that is, hospital operations are heavily affected, medical records systems are down, patients' lives are at risk, treatments are completely stopped or rescheduled.	The attacker subverts the system and can inflict moderate damage to hospital operations, or some departments are affected for short periods of time.	The attacker subverts the system and can inflict minor damage, that is, on systems that do not affect patients' health directly, such as billing systems, email, and the like.
R	Reproducibility	The attack can be reproduced every time.	The attack can be reproduced, but only within set limitations.	The attack is very difficult to reproduce, even with full knowledge of the security hole.
E	Exploitability	The attack requires little or no knowledge of the system in order to exploit it.	The attack requires a skilled operator with fundamental knowledge of the system in order to exploit it.	The attack requires an extremely skilled operator with in-depth knowledge of the system in order to exploit it.
A	Affected users	Majority of everyday users will be affected by the attack.	A good portion of everyday users will be affected by the attack.	A very small percentage of everyday users will be affected by the attack.
D	Discoverability	Published information readily explains the attack. Vulnerabilities are found in the most commonly used applications and systems.	Vulnerabilities are not common and only found in certain applications and systems. It requires skills to discover exploitable weaknesses.	Extremely difficult to discover vulnerabilities, and they are very difficult to weaponize. Extremely difficult to attack the applications and systems.

Table 2. Threat ratings table for hospital risk analysis

After answering the questions for a given threat, the risk rating was calculated by adding the ratings values. The overall risk is rated as follows:

- **High risk** if the score is between: 12 – 15
- **Medium risk** if the score is between: 8 – 11
- **Low risk** if the score is between: 5 – 7

Measuring the Risks of Cyberattacks Against Hospitals and Clinics

We applied the six cyberattack vectors that we discussed in the section *How are they attacking the healthcare industry?*, to the three categories of hospital systems that we introduced in Table 1. We assessed that these six cyberattack vectors are most likely to be used by cybercriminals against critical hospital systems, based on our analysis of past cyberattacks against hospitals. We excluded insider threats from our threat modeling exercise because it is primarily a human threat versus a cyberthreat. We assigned scores for realistic extreme scenarios, e.g., WannaCry outbreak, to the cyberattack vectors and calculated the risk rating using the DREAD threat model.

The threat modeling exercise is intended to help identify critical areas that need active monitoring and improved defenses. While specific cases may have different ratings, this overview helps us understand where the real areas of weakness — and therefore focus — should be.

Medical Devices

Attack Vectors	D	R	E	A	D	Rating
Spear phishing	-	-	-	-	-	Not applicable
Distributed denial of service (DDoS)	3	3	3	2	3	High
Vulnerability exploitation	3	1	1	2	1	Medium
Malware infection	3	2	2	2	2	Medium
Privilege escalation and misuse	3	1	2	2	2	Medium
Data manipulation	3	1	1	1	1	Low

Table 3. DREAD results for medical devices

Information Systems

Attack Vectors	D	R	E	A	D	Rating
Spear phishing	-	-	-	-	-	Not applicable
Distributed denial of service (DDoS)	3	3	3	3	3	High
Vulnerability exploitation	3	2	2	3	2	High
Malware infection	3	2	2	3	2	High
Privilege escalation and misuse	1	1	1	3	1	Low
Data manipulation	2	1	2	3	1	Medium

Table 4. DREAD results for information systems

Hospital Operations

Attack Vectors	D	R	E	A	D	Rating
Spear phishing	3	2	3	2	2	High
Distributed denial of service (DDoS)	3	3	3	3	3	High
Vulnerability exploitation	3	2	2	3	2	High
Malware infection	3	2	2	3	2	High
Privilege escalation and misuse	1	1	1	3	1	Low
Data manipulation	2	1	2	3	1	Medium

Table 5. DREAD results for hospital operations

Based on the results of our threat modeling exercise, we make the following observations:

- Even if some devices and systems are not directly being used in patient care, they can still be compromised and used as a leverage point to laterally move across the hospital network. Hospital networks are typically not set up as separate enterprise versus medical networks with a demilitarized (DMZ) in between for communications. In the simplest of cases, it may even be set up as a flat network. This opens up the possibility of device/system compromise via lateral movement from the Point of Entry (PoE) in the network.
- DDoS attacks via compromised systems and devices are a serious threat that is fairly easy to execute and requires no specialized knowledge about the devices and systems themselves. Perpetrators can potentially DDoS exposed devices and systems and knock them offline. Using an IoT search engine like Shodan, we have managed to find many devices and systems exposed on the internet.

- Medical device compromise stories make sensational news, but in reality, the probability of them getting compromised was assessed to be Low risk. This is because the medical devices themselves have specialized software, and in most cases, they won't be directly connected to the network. As reflected in our rating, the number of affected users in the event of a successful exploitation of a medical device is lower than for the other categories, so unless the threat actor intends to expend some time and effort to perform reconnaissance and launch a highly targeted attack, medical devices are not likely to be the avenue of choice for cybercriminals. On the flipside, the controllers for these devices will be connected to the hospital network and are susceptible to cyberattacks. So if the CT scanner controller gets compromised with ransomware, all CT scanning activities will stop.
- For medical devices we assessed, the greatest threat was DDoS attacks. Vulnerabilities, malware, and privilege escalation/misuse attacks are Medium risk because the devices are not guaranteed to be on the network, and attackers will require specialized knowledge for successful compromise. Data manipulation on these devices will be an extremely difficult task, and most perpetrators will instead target the controllers versus the devices themselves if they want to modify data.
- Spear phishing for medical devices and information systems is not directly possible, as these devices and systems are not designed to send/receive emails. On the other hand, a successful spear phishing campaign can laterally move from the PoE in the network and compromise these devices/system. Spear phishing attacks typically target a select few employees using specially crafted emails, but a successful attack will have far-reaching consequences inside the hospital ecosystem.
- Majority of the threats assessed for Information Systems and Hospital Operations were in the High risk category. There are several factors that contributed to these High risk ratings: the damage potential if these devices/systems are compromised is very high; these devices/systems directly impact almost everyone inside the hospital, patients, doctors, nurses, technicians, and orderlies; these systems are typically implemented using off-the-shelf software platforms, e.g., Windows, MySQL, etc.; vulnerabilities, even for Building Control Systems, are well known and there is a high likelihood, as we discovered in the case of WannaCry, the systems are NOT patched regularly.

Having examined the other moving parts in the healthcare ecosystem in the previous and current sections, we hope to have given IT teams a broader perspective of the existing weaknesses in healthcare networks. In the next section we outline an IT defense strategy and provide technical and non-technical recommendations to address the issues raised here.

Recommendations: IT Defense for Hospitals

Cyberattack and data breach prevention strategies should be considered an integral part of daily business operations at hospitals. Ultimately, no defense is impregnable against determined adversaries. Cyberattacks and data breaches are inevitable. Having effective alert, containment, and mitigation processes are critical. The key principle of defense is to *assume compromise* and take countermeasures:

- Quickly identify and respond to ongoing security breaches.
- Contain the security breach and stop the loss of sensitive data.
- Pre-emptively prevent attacks by securing all exploitable avenues.
- Apply lessons learned to further strengthen defenses and prevent repeat incidents.

The HITRUST CSF® takes into consideration the regulations and standards relevant to the healthcare industry, including HIPAA (Health Insurance Portability and Accountability Act), PCI-DSS (Payment Card Industry Data Security Standard), ISO (International Organization for Standardization), NIST (National Institute of Standards and Technology), and even GDPR (General Data Protection Regulation), folding their requirements and implications into a single, overarching security framework.[73] HITRUST CSF is a certifiable framework that is risk- and compliance-based. In the following sections, we examine the key technologies and strategies that need to be implemented in order to be certified, and thus be fully poised to prevent and detect the kinds of attacks that can hit healthcare organizations.

Technical Recommendations for Hospitals

Based on our research findings on the different types of cyberthreats faced by hospitals, we make the following recommendations for the implementation of defensive strategies that we consider a *mandatory minimum* for the hospital IT ecosystem.[74] Surely, each organization, even within the healthcare industry, will have a different set of challenges that may require additional due diligence that can only be recognized upon close analysis of the status quo and the particular organizational setup. However, given the competing priorities that healthcare IT teams have to contend with every day, it is important to emphasize that the following should be in place at the very least:

1. **Network segmentation** — This refers to splitting a network into multiple subnetworks to reduce congestion, limit failures, and improve security. Putting all the medical devices on a dedicated network, that is separate from the corporate network, reduces risks of lateral movement and improves overall security.
2. **Firewalls** — These are network security systems that control incoming and outgoing traffic based on an applied rule set. Firewalls monitor both ingress and egress traffic from unknown and bad domains and identifies applications or endpoints that generate or request bad traffic.
3. **Next-generation firewalls/Unified Threat Management (UTM) gateways** — These are network security products that unify multiple systems and services into a single engine or appliance. They can incorporate firewalls, Intrusion Prevention System/Intrusion Detection System (IPS/IDS), antivirus, web filtering, application control, and other solutions all in the same appliance. These devices analyze network traffic at line speed. UTM gateways generally have lower traffic throughput compared to next-generation firewalls.
4. **Antimalware solutions** — Scan files to detect, block, and remove malicious software such as viruses, Trojans, worms, keyloggers, ransomware, rootkits, and so on, from the system. Antimalware uses heuristics, generic, and specific signatures to detect known and unknown malware.
5. **Antiphishing solutions** — Email-filtering products that scan for and block incoming spam and phishing emails. Spear phishing is one of the top infection vectors. Some antiphishing solutions also use message sandboxes to screen for potentially malicious attachments.
6. **Breach Detection Systems (BDS)** — Security solutions focused on detecting intrusions caused by targeted attacks and other sophisticated threats designed to harvest information from the compromised systems. BDS analyzes complex attacks out-of-band, detecting, rather than preventing, network breaches. BDS can analyze network traffic patterns across multiple protocols, identify malicious domains, and uses emulation-sandboxing to model the behavior and impact of malicious files that are being dropped or downloaded.
7. **IPS/IDS** — Network security systems that examine traffic flow to detect and prevent network attacks. IDS are passive systems that generate a report when a known bad event is identified. IPS rejects the packet when a known bad event is identified. IPS/IDS monitors the entire network for suspicious traffic by analyzing protocols and doing deep packet inspection.
8. **Encryption technologies** — Software for the encryption and decryption of data in the form of files, email messages, or packets sent over a network. Encrypted network traffic will defeat MitM network-sniffing data theft attacks.
9. **Patch management (physical or virtual)** — Patch management software keeps endpoints, servers, and remote computers updated by applying the latest security patches and software updates. Virtual patch management uses a security enforcement layer to prevent malicious traffic from reaching

vulnerable systems. In a large environment where patches need to be thoroughly tested before applying, virtual patching provides the stopgap measure of filtering out malicious traffic attempting to exploit known vulnerabilities.

10. **Vulnerability scanner** — Automated tools that scan endpoints, servers, networks, and applications for security vulnerabilities that an attacker can exploit. One of the tried-and-tested ways malware does lateral movement is by exploiting vulnerabilities on the target machine it wants to infect. A vulnerability scanner scans and identifies unpatched vulnerable endpoints, servers, and applications, which the IT administrator can then patch.
11. **Deception technologies** — Custom-built honeypots that contain emulated versions of real devices found in the network. The main idea: if attackers moving inside the network compromise these vulnerable virtual devices, then the IT security team gets an early warning of potential network compromise. The compromised virtual devices also provide clues about the attacker's motives and end goals. Deception technology can be placed at the network, endpoint, application, or data level, and should be implemented as part of a layered defense strategy.
12. **Shodan scanning** — Shodan is a search engine for internet-connected devices. Shodan provides an easy one-stop solution to conduct Open-Source INTelligence (OSINT) gathering for different geographic locations, organizations, devices, services, etc. Software and firmware information collected by Shodan can potentially help identify unpatched vulnerabilities in the exposed cyber assets. Hospitals should monitor their IP ranges in Shodan to ensure their managed devices and systems are not exposed on the internet.

Non-Technical Recommendations for Hospitals

Making sure that IT staff are well-trained and have access to adequate resources translate well into the security team's ability to formulate a good defense strategy for the organization. Since new threats are always emerging, they must have the means to experiment and learn from mistakes so they can save the organization from the next big cyberattack or data breach.

An incident response protocol should also be in place, which prescribes the behavior desired from any employee that either discovers the security breach or receives the report. Additionally, a pre-established incident response team, composed of members from different functions such as technical, threat intelligence, human resources, legal, public relations and executive management, should be identified for quick mobilization.

Furthermore, social engineering training for all employees and relevant third-party partners can complement the technical recommendations in the previous section. Non-IT personnel, especially those in the healthcare industry, are much more attuned to physical, real-world threats because of the nature

of hospital operations, so an organization-wide initiative that raises awareness and actually tests hospital staff for social engineering attacks offline and online is a valuable component of an overall security strategy. These trainings or drills should be conducted regularly to keep the staff's insights learned fresh instead of just being a one-time campaign.

Managing Supply Chain Threats

To manage the growing risk of supply chain attacks, hospitals need to develop and keep improving their vendor and third-party risk management programs. We recommend the following activities:

- Perform vulnerability assessment of new medical devices, to determine if they pose any cyber risks or not, prior to connecting them to the hospital network. This assessment is to ensure that the functional integrity of the device has not been compromised on the manufacturer's end.
- Bring your own device (BYOD) programs should include authentication using network access controls (NAC) before allowing access to the network for an employee's mobile phones, tablets, and items like USB drives.
- Purchase medical devices from manufacturers who go through rigorous security assessment of the products during design and manufacture. This ensures the purchased medical devices have had proper vulnerability assessment done and poses a low risk inside the hospital network.
- Develop a plan for patching and updating code/firmware for devices implanted in patients and for hospital medical equipment.
- Perform risk assessment on all suppliers and vendors in the supply chain. Perform thorough background checks on all employees who may have physical access to computers or a medical device. This includes all temporary, contract, seasonal, and volunteer staff.
- Identify third-party vendor software and perform security and vulnerability testing to ensure they are safe from hackers. Penetration testing of the hospital network by professional pentesting companies is highly recommended.

Conclusion

Healthcare IT teams constantly struggle to strike a good balance between enabling continuous, efficient hospital operations through technology and ensuring that their networks are secure. The importance of keeping healthcare systems and data secure is further emphasized by the added burden of possibly incurring fines and penalties for non-compliance to regulations set forth in HIPAA or GDPR. Where must an IT team look first? Among the most pressing security issues, ransomware attacks appeared to have the most visceral impact, with affected hospitals having to suspend operations while recovering, but ransomware attacks are demonstrably not the only threat against healthcare networks.

One area that the healthcare industry needs to be more vigilant about is ensuring that the devices and systems it connects to the internet are not searchable publicly. Trend Micro was able to find a surprisingly high number of internet-exposed medical systems in the Shodan search engine. Among those Shodan findings were open ports, databases, medical systems, and network misconfigurations inside healthcare networks. While exposed cyber assets do not necessarily mean they are compromised, they do point cybercriminals in a specific direction if they want to find weaknesses in a target institution.

Supply chains are another overlooked component to hospital operations that can lead to a security compromise. The numerous moving parts that ensure that hospitals are able to deliver life-preserving services can also endanger those very services: vendors who are allowed to access the internal networks, non-core services which have physical access to the healthcare consoles, even as far back in the supply chain as a raw materials supplier or software developer for a device that is eventually shipped to and used in diagnosing patients. Healthcare IT teams must understand that, in order to cover these weaknesses in the supply chain, they must establish a strategy that identifies all the third parties that the hospital or clinic directly interacts with and regularly review these relationships based on pre-established risk-based standards, making recommendations or terminating use of their services if necessary.

When we did the DREAD threat modeling exercise on healthcare industry networks, we determined that, while medical device compromise may make sensational news when they actually occur, the reality is that the probability of them getting compromised is pretty low. The greater threat for medical devices is DDoS attacks, which can be easily executed. Threats against hospital information systems, like DDoS,

vulnerability exploitation, and malware infection, are high risk because they directly impact all hospital users and are easy to implement given the systems are typically off-the-shelf platforms.

Daily operations of the modern hospital are supported by a wide array of interconnected devices, systems, and applications all exchanging data. The HIS is the backbone of this data transfer and manages all aspects of a hospital's operation, including medical, administrative, financial, legal issues, and the corresponding processing of services. It is important to understand that each and every application and device running on the hospital network is a potential entry point for hackers targeting the hospital.

In the modern hospital, technology plays a critical role in patient care, the primary objective of hospitals, and thus, it strongly necessitates that cyberattack and data breach prevention strategies become an integral part of daily hospital operations. We recommend closely adhering to the HITRUST CSF, which encapsulates relevant standards and regulations into a single framework, giving healthcare organizations the means to prevent and detect current and emerging threats in the landscape. Cybersecurity should be given adequate priority by hospital administration and IT teams as it is unacceptable for patients' health to be jeopardized by the actions of profiteering and/or malicious hackers.

Appendix

Further Analysis of Damage Potential by Medical Equipment/System

Electronic health record (EHR) integration in smart medical devices enhances patient care and automates hospital services. But it also creates entry points for malware and cybercriminals. Interconnected medical devices can create significant cybersecurity risks that can result in corruption or breach of both patient data and protected health information, disruption of hospital operations, exposure of the hospital's network to the public internet, and damage to the organization's reputation, thus causing loss of revenue. Healthcare IT teams have to balance these security issues with the urgent life-or-death realities of enabling the operation of a medical facility.

According to the FDA's *Postmarket Management of Cybersecurity in Medical Devices* document, the FDA can only offer nonbinding recommendations and does not test nor validate the cybersecurity of a medical device. Likewise, NIST has made recommendations which organizations can implement voluntarily with regard to medical devices like wireless infusion pumps.[75] The medical device manufacturer is responsible for the validation of all design changes and cybersecurity vulnerabilities.[76] Common medical device vulnerabilities include weak passwords, default or hard-coded vendor passwords, unpatched systems, and outdated operating systems. In 2013, the Department of Homeland Security and ICS-CERT published an advisory that showed at least 300 medical devices across 40 manufacturers had hard-coded passwords with no option for users to change them.[77] In 2016, it was found that in the U.K., 90 percent of NHS hospitals were still running Windows XP, which is no longer supported for free by Microsoft, putting patients' safety at risk and allowing hackers to exploit them using ransomware like Petya and WannaCry.[78]

Based on our research, we have identified several pieces of equipment of interest, found in most healthcare facilities, that are at risk from cybercriminals, along with possible cyberattack vectors and how they pertain to our three critical areas of interest. Note that the scenarios we illustrate under damage potential do not express the relative likelihood of them happening or the existence of active attacks of this nature, but instead the possible ramifications *if* the devices or systems are indeed attacked. This analysis is useful for healthcare IT security teams conducting risk assessment for their own network of medical devices and systems.

Medical Devices

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Imaging (e.g., MRI, CT, X-ray, ultrasound)	Medical imaging refers to different technologies that are used to see inside the human body in order to diagnose and treat medical conditions. X-rays produce dense images such as bone and metal inside the body using electromagnetic waves. Magnetic resonance imaging (MRI) uses a magnetic field and radio waves to create images of the organs and tissues within the body. A computerized tomography (CT) scan is a series of cross-sectional X-ray images of the inside of the body that provide better details of soft tissues and blood vessels.[79] Ultrasound uses high-frequency sound waves to produce images, called a sonogram, using a probe.[80]	• Ransomware • DDoS • Privilege misuse • Data manipulation • Vulnerability exploitation	For example, MRI operations are locked out until ransom is paid. Patient appointments will need to be rescheduled. Data may be lost as a result of not paying ransom or not having a backup to restore MRI operations. MRI operations are disrupted or intermittent depending on the DDoS activity. This affects patient treatment. Cybercriminals can override and control the machine's operations such as power consumption, alarms, and EHR interfaces. Cybercriminals can modify or delete the MRI images associated with the patients' EHR.	• Patient health • Data privacy • Hospital operations

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Infusion pumps	Infusion pumps are medical devices used to deliver fluids into a patient's body in a controlled manner that can be integrated into the patient's EHR and pharmacy system. Modern infusion pumps include wireless 802.11 a/b/g/n integration.[81] Infusion pumps can include enteral (feeding tubes),[82] patient-controlled analgesia (PCA, or self-administered pain medication),[83] elastomeric (or balloon pumps used to deliver pre-determined amounts of medication),[84] syringe (uses a piston syringe as fluid reservoir),[85] and insulin pumps. Infusion pumps integrated with the EHR ensure the patient receives the correct medication and dosage. Connected infusion pumps can notify the pharmacy when the patient has finished medication or notify hospital staff of interruptions with the pump such as error messages and power supply status. They can also provide real-time data transmission to the patient's EHR, wirelessly or through connected internet. They can also update drug libraries.	• Privilege misuse • Ransomware • DDoS • Vulnerability exploitation	Cybercriminals can alter dosage, modify system alerts, and manipulate drug libraries. Infusion pump operations are locked out until ransom is paid. Data may be lost as a result of not paying ransom, or not having a backup. Infusion pumps cannot operate and hospitals will need to use a backup, most likely manual, method to deliver medication to patients, therefore slowing down treatment.	• Patient health • Hospital operations

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Respiratory ventilators	Respiratory ventilators are machines that help patients breathe by assisting the inhalation of oxygen into the lungs and the exhalation of carbon dioxide when they have lost the ability to breathe on their own.[86]	• Ransomware • DDoS • Privilege misuse • Vulnerability exploitation	Ventilator operations are locked out until ransom is paid. Patient appointments will need to be rescheduled. Data may be lost as a result of not paying ransom or not having a backup to restore ventilator operations. Patients' lives may be put at risk. Ventilator operations can go offline. Hospitals will need to use an offline device to continue life-saving operations. Patients' lives may be put at risk. Cybercriminals can modify the machine's operations such as oxygen, pressure, flow, and power. Patients' lives may be put at risk.	• Patient health • Hospital operations
Anesthesia machines	Anesthesia machines are devices that deliver a measured gas mixture and are used for general anesthesia on patients during surgeries.[87]	• Ransomware • DDoS • Privilege misuse • Vulnerability exploitation	Anesthesia machine operations are locked out until the ransom is paid. Surgeries will need to be rescheduled. The patient's life may be put at risk. Anesthesia operations can go offline or are available intermittently. Hospitals would need to use an offline anesthesia machine for the operation. Cybercriminals can modify the machine's operations to interfere with patient monitoring such as heart rate, ECG, blood pressure, and oxygen. The patient's life will be put at risk.	• Patient health • Hospital operations

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Heart-Lung machines	Heart-lung machines are devices used in open-heart surgeries to support the body during the surgical procedure — maintaining the circulation of blood and oxygen in the patient's body while the heart is stopped.[88]	• Ransomware • DDoS • Privilege misuse • Vulnerability exploitation	Heart-lung machine operations are locked out until ransom is paid. Surgeries will need to be rescheduled. Patients' lives are put at risk. Heart-lung operations can go offline or are available intermittently. Cybercriminals can modify the machines' operations to interfere with the heparin pump, thus affecting the patient's ability to clot. The patient's life will be put at risk.	• Patient health • Hospital operations
Dialysis machines	Dialysis machines purify a patient's blood to remove excess water and waste when the kidneys are damaged or missing.[89] Modern machines contain Ethernet, Wi-Fi, serial ports, data cards and USB ports to connect to legacy hospital information systems in order to transfer information to the patient's medical records and nurses' station.	• Ransomware • DDoS • Privilege misuse • Vulnerability exploitation	Dialysis machine operations are locked out until ransom is paid. Patient appointments will need to be rescheduled. Dialysis operations can go offline or are available intermittently. Cybercriminals can modify the machine's operations to interfere with the heparin pump, air sensors, pressure, and dialysate mixture. The patient's life will be put at risk.	• Patient health • Hospital operations
Medical lasers	Medical lasers are devices that use precisely focused light sources to treat or remove tissues using specific wavelength in cosmetic treatments, dermatology, eye surgeries, and dental procedures.[90]	• Ransomware • Privilege misuse • Vulnerability exploitation	Medical lasers cannot function until ransom is paid. Patient appointments will need to be rescheduled. Cybercriminals can alter power, energy, and tamper exposures. The patient can have adverse reactions or injures due to improperly configured machines.	• Patient health • Hospital operations

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Robotic surgical machines	Robotic surgical machines are devices that perform surgery using very small tools attached to a robotic arm with the control of a surgeon and a computer.[91]	• Ransomware • Privilege misuse • Vulnerability exploitation	Robotic surgical equipment cannot function until ransom is paid. Surgeries will need to be rescheduled. Cybercriminals can modify the system to cause uncontrolled movement of the robotic arms. Surgery would have to be modified and expertise may not be available. Patients' health may be at risk.	• Patient health • Hospital operations
Radiotherapy systems	Radiotherapy machines use high-energy radiation to destroy cancer cells and treat tumors anywhere in the body.[92]	• Ransomware • Privilege misuse • Vulnerability exploitation	Radiotherapy equipment cannot function until ransom is paid. Patient appointments will need to be rescheduled. Cybercriminals can modify the system to change radiation doses, power, and energy. Patient's health may be at risk due to adverse effects from misconfigured systems.	• Patient health • Hospital operations
Active and passive monitoring devices	Passive devices monitor patients' health while active devices interact with patients to administer a medical treatment. Passive medical devices include heart monitors, blood pressure machines, and pulse oximeters.[93] Sample active devices include MRI scanners, infusion pumps, and defibrillators.[94]	• Ransomware • Privilege misuse • Vulnerability exploitation	These devices cannot function until ransom is paid. Hospital would have to use offline devices to monitor patients' vital signs. Data may be lost as a result of not paying ransom. EHR can't be updated. Cybercriminals can alter the machine configurations to provide inaccurate results, thus jeopardizing the patient's health. Alert systems can be shut off. Machine data can be altered and disconnected from the EHR of the patient. Hospitals may need to go to paper records until issues are resolved.	• Patient health • Hospital operations

Hospital Information Systems

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
EHR/EMR databases	Electronic medical records (EMR) is a database that holds medical and clinical data obtained at the health providers' office, such as medical history, diagnoses, medications, immunization dates, and allergies. An EHR database holds a comprehensive patient history that allows the patient medical history to move with them, such as progress notes, diagnoses, medications, immunization dates, allergies, lab data, and imaging reports.[95]	• Data manipulation • Phishing attacks • Insider threat • Vulnerability exploitation • DDoS • Privilege misuse • SQL injections	Cybercriminals can modify the data to show inaccurate health records, putting the patient's health at risk. Cybercriminals can perform a phishing attack that gives them access to the system and allows them to extract data such as billing information and SSN. A current or disgruntled employee accesses the database to extract or manipulate data for malicious intent. DDoS attack can shut down services and access.	• Data privacy • Hospital operations • Patient health
Laboratory information systems	Laboratory information systems are computer software that manage and store clinical data for laboratories, and can include features to manage patient check-ins, order laboratory tests, and store patient information. Laboratory information systems can integrate with EHR systems.[96]	• Ransomware • DDoS • Data manipulation • Privilege misuse	System cannot function until ransom is paid. Patient appointments will need to be rescheduled. Data may be lost as a result of not paying ransom or not having a backup to restore operations. Access to the system may not be available or become intermittent. Data can be manipulated or deleted putting the patient's health at risk.	• Hospital operations • Data privacy

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Radiology information systems	Radiology information systems (RIS) are database software that manage digital images from radiology machines, provide reports, store previous radiology scans, submit medical claims, and provide detailed billing information. RIS can integrate with EHR systems.[97]	• Ransomware • Privilege misuse • Vulnerability exploitation	System cannot function until ransom is paid. Patient appointments will need to be rescheduled. Data may be lost as a result of not paying ransom or not having a backup to restore operations. Access to the system may not be available or become intermittent. Access to the patients' EHR may not be available. Data can be manipulated or deleted, putting the patient's health at risk. Loss of images can require redoing of radiology testing and prolonging patient care and diagnosis.	• Hospital operations • Data privacy
Work order and scheduling systems	Work order systems help maintain the hospital in working capacity, for instance, that the facilities are cleaned, medical procedures are scheduled, rooms are booked, and others. Scheduling systems help manage patient, nurses, and physician's schedules and appointments.[98]	• Privilege misuse • Vulnerability exploitation	Cybercriminals can extract or modify data and disrupt daily hospital operations.	• Hospital operations
PACS (Picture Archiving and Communications System)	A Picture Archiving and Communication System is a hospital-wide database system to store, retrieve, view, and share medical images.[99]	• Ransomware • Privilege misuse • Data manipulation	System cannot function until ransom is paid. Patient appointments will need to be rescheduled. Data may be lost as a result of not paying ransom or not having a backup to restore operations. Cybercriminals can extract and modify data. Patient images can be deleted requiring the patient to redo the examination. Patients' health may be at risk if imaging is needed for a life-threatening condition.	• Hospital operations • Data privacy

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Office systems (e.g., payroll, email, fileserver, etc.)	Office systems manage patient information like billing and insurance, registration, and reporting. These systems are also used in everyday hospital operations, e.g., email, accounting, fileservers, payroll, HR, etc.[100]	• BEC attack • Vulnerability exploitation • Ransomware	System cannot function until ransom is paid. Data may be lost as a result of not paying ransom or not having a backup to restore operations. Hospital staff's payroll may get disrupted. Hospital staff's PII data may get compromised.	• Hospital operations • Data privacy
Mobile health applications	Mobile health applications, also known as mHealth apps, are the use of mobile and wireless technology for medical care.[101]	• Vulnerability exploitation • Ransomware	Data can be manipulated, deleted, or extracted for malicious intent. Backend systems may get compromised with ransomware and the mHealth applications can no longer access patient data.	• Data privacy • Hospital operations

Other Systems

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Drug and equipment inventory systems	Centralized inventory system that allows the staff to check inventory, order supplies, and track expenses and works with other systems in conjunction, like automated drug dispensers and bar code systems.[102]	• Vulnerability Exploitation • Privilege Misuse • Data manipulation	Insiders can modify systems to physically steal medication and equipment. Cybercriminals can modify databases of inventory for malicious intent. Hospitals can run out medications and certain equipment needed for everyday operations if the data has been manipulated to show incorrect amounts of inventory are left.	• Hospital operations • Patient Health
Hospital paging systems	Paging systems provide communication between nurses and doctors for medical emergency or notifications.[103]	• Vulnerability exploitation • Privilege misuse	Cybercriminals can sniff communications for malicious purposes. Patients' PII can be exposed. Note: We discussed this security issue at great length in *Leaking Beeps: Unencrypted Pager Messages in the Healthcare Industry*.[104]	• Hospital operations

Equipment	Description	Cyberattack Vectors	Damage Potential	Critical Areas of Interest
Building control systems	A system that integrates HVAC, energy management, fire safety, air safety, and security in a centralized system.[105]	• Vulnerability exploitation • Ransomware • Privilege misuse	System cannot function until ransom is paid. Data may be lost as a result of not paying ransom or not having a backup to restore operations. Cybercriminals can gain administrative access to turn off, modify, and override building controls. If the hospital loses power, it may put patients' lives at risk. Hospital operations may halt for not having water, HVAC, lighting, and other necessary services.	• Hospital operations • Patient health
Barcode scanners and printers	Hospitals extensively use barcodes for inventory, tracking, and patient validation to prevent human errors.[106]	• Vulnerability exploitation	Data can be manipulated, deleted, or stolen for malicious purposes. If the barcode system is offline, hospitals will have to revert to paper for daily operations.	• Hospital operations
Automated drug dispensers	Automated dispensing machines that are computer-controlled to dispense and track prescription medications.[107]	• Insider threat • Vulnerability exploitation	Insiders can modify the system to physically steal medication. Wrong dosage or medication can be dispensed, putting the patient's health at risk.	• Hospital operations • Patient health
Pneumatic tube transport systems	Pneumatic tubes are an air transport system to transport lab paperwork, medication, and specimens to different parts of the hospital without requiring a person to deliver them.[108]	• Vulnerability exploitation • Insider threat • Privilege misuse	Items being transported can be sent to the wrong location, prolonging diagnosis or treatment of patients. Cybercriminals can change the direction to stop at a specific place to obtain the items being sent. Insider can obstruct delivery, change delivery location, and steal items being sent.	• Hospital operations • Patient health

References

1. Marcus Hutchins. (20 May 2017). *The Telegraph*. "NHS cyber attack: Everything you need to know about 'biggest ransomware' offensive in history." Last accessed on 19 July 2017 at http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/.

2. Megan Fisher, Alex Therrien, John Hand, and Bernadette McCague. (12 May 2017). *BBC*. "How cyber-attack is disrupting NHS." Last accessed on July 19, 2017 at http://www.bbc.com/news/live/39901370.

3. BBC News. (12 May 12 2017). *BBC*. "NHS cyber attack: 'My heart surgery was cancelled'." Last accessed on on 19 July 2017 at http://www.bbc.com/news/av/uk-39900677/nhs-cyber-attack-my-heart-surgery-was-cancelled.

4. BBC News. (13 May 2017). *BBC*. "NHS 'robust' after cyber-attack." Last accessed on on 19 July 2017 at http://www.bbc.com/news/uk-39909441.

5. Brian Krebs. (5 February 2014). *Krebsonsecurity*. "Target Hackers Broke in Via HVAC Company." Last accessed on 20 February 2018 at https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

6. Taylor Armerding. (13 October 2016). *CSOOnline*. "The OPM breach report: A long time coming." Last accessed on 20 February 2018 at https://www.csoonline.com/article/3130682/data-breach/the-opm-breach-report-a-long-time-coming.html.

7. Tara Seals. (7 November 2014). *Infosecurity Magazine*. "Home Depot: Massive Breach Happened via Third-Party Vendor Credentials." Last accessed on 20 February 2018 at https://www.infosecurity-magazine.com/news/home-depot-breach-third-party/.

8. Protenus. "Third Party Breaches in 2016 Pose Alarming Risk to Patient Data." Last accessed on 10 October 2017 at http://marketing.protenus.com/hubfs/Content/20160914_Databreaches.net_Full_BA_Report.pdf.

9. World Health Organization. (6 June 2016). *WHO*. "Global Health Observatory data repository." Last accessed on 2 August 2017 at http://apps.who.int/gho/data/view.main.SDG2016LEXREGv?lang=en.

10. Michael Riley and Jordan Robertson. (6 February 2015). *Bloomberg Technology*. "Signs of China-Sponsored Hackers Seen in Anthem Attack." Last accessed on February 23, 2018 at https://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack.

11. Industrial Control Systems Cyber Emergency Response Team. (2001). *ICS-CERT*. "Cyber Threat Source Descriptions." Last accessed on 9 March 2018 at https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions.

12. Susan Morrow. (2016.) *Infosec Institute*. "Insider Threats at Hospitals." Last accessed on 9 March 2018 at http://resources.infosecinstitute.com/insider-threats-at-hospitals/#gref.

13. Trend Micro. (2017). *Trend Micro Glossary of Terms*. "Spear-Phishing." Last accessed on 13 September 2017 at https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing.

14. Trend Micro. (2017). *Trend Micro Glossary of Terms*. "Business Email Compromise." Last accessed on 10 September 2017 at https://www.trendmicro.com/vinfo/us/security/definition/business-email-compromise-(bec).

15. Trend Micro. (2017). *Trend Micro Glossary of Terms*. "Distributed denial of service DDoS." Last accessed on 5 September 2017 at https://www.trendmicro.com/vinfo/au/security/definition/distributed-denial-of-service-ddos.

16. Natt Garun. (30 August 2017). *The Verge*. "Almost half a million pacemakers need a firmware update to avoid getting hacked". Last accessed on 1 October 2017 at https://www.theverge.com/2017/8/30/16230048/fda-abbott-pacemakers-firmware-update-cybersecurity-hack.

17. Pete Williams. (31 March 2017). *NBC News*. “MedStar Hospital Recovering After Ransomware hack”. Last accessed on 31 September 2017 at https://www.nbcnews.com/news/us-news/medstar-hospitals-recovering-after-ransomware-hack-n548121.

18. Eric McCann. (19 May 2014). *Healthcare IT News*. “Keylogger hack at root of HIPAA breach.” Last accessed on 15 October 2017 at http://www.healthcareitnews.com/news/keylogger-hack-root-hipaa-breach.

19. Tom Spring. (20 June 2016). *Threat Post*. “Conficker used in new wave of hospital IOT device attacks”. Last accessed on 10 October 2017 at https://threatpost.com/conficker-used-in-new-wave-of-hospital-iot-device-attacks/118985/.

20. John Leyden. (22 November 2017). *The Register*. “Hospital info thief malware puts itself into a coma to avoid IT bods.” Last accessed on 10 October 2017 at https://www.theregister.co.uk/2016/11/22/healthcare_trojan/.

21. Dissent. (23 September 2017). *Databreaches.net*. “Smart Physical Therapy hacked by TheDarkOverlord.” Last accessed on 2 October 2017 at https://www.databreaches.net/ma-smart-physical-therapy-hacked-by-thedarkoverlord/.

22. Claire Groden. (4 August 2015). *Fortune*. “Hackers could go after medical devices next.” Last accessed on 11 October 2017 at http://fortune.com/2015/08/04/hackers-medical-devices/.

23. Privacy Rights Clearinghouse. (2017). *Privacy Rights Clearinghouse*. “Data Breaches.” Last accessed: August 4, 2017. https://www.privacyrights.org/data-breaches.

24. Kelly Sheridan. (16 Feb 2017). *DarkReadking*. “MEDJACK.3 Poses Advanced Threat to Hospital Devices.” Last accessed on 9 March 2018 at https://www.darkreading.com/endpoint/medjack3-poses-advanced-threat-to-hospital-devices/d/d-id/1328172?.

25. Sam Clements. (26 April 2013). *Vice*. “Is Shodan Really the World’s Most Dangerous Search Engine?” Last accessed on 26 September 2017 at https://www.vice.com/en_uk/article/9bvxmd/shodan-exposes-the-dark-side-of-the-net.

26. John Matherly. (August 2017). *Leanpub*. “Complete Guide to Shodan.” https://leanpub.com/shodan.

27. NCCIC Incident number INC000010146067. (1, October 2017).

28. DICOM. (2018). *Dicom*. “Home.” Last accessed on 9 March 2018 at http://www.dicomstandard.org/.

29. Dan Goodin. (21 October 2015). *ArsTechnica*. “New attacks on Network Time Protocol can defeat HTTPS and create chaos.” Last accessed on 1 October 2017 at http://arstechnica.com/security/2015/10/new-attacks-on-network-time-protocol-can-defeat-https-and-create-chaos/.

30. Aanchal Malhotra, Isaac Cohen, Erik Brakke, and Sharon Goldberg. (October 2015). *Boston University*. “Attacking the Network Time Protocol.” Last accessed on 1 October 2017 at http://www.cs.bu.edu/~goldbe/papers/NTPattack.pdf.

31. IETF. (May 1983). J. Postel and J. Reynolds. *IETF*. “Telnet Protocol Specifications”. Last accessed on 19 March 2018 at https://tools.ietf.org/html/rfc854.

32. Internet Engineering Task Force. (1985). “File Transfer Protocol.” Last accessed on 9 March 2018 at https://tools.ietf.org/html/rfc959.html.

33. Microsoft. (2017). “Understanding the Remote Desktop Protocol.” Last accessed on 9 march 2018 at https://support.microsoft.com/en-us/help/186607/understanding-the-remote-desktop-protocol-rdp.

34. Jon Oliver. (19 September 2016). *TrendLabs Security Intelligence Blog*. “A Show of (Brute) Force: Crysis Ransomware Found Targeting Australian and New Zealand Businesses.” Last accessed on 1 October 2017 at http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps/.

35. Contributing members of the UPnP forum. (2008). *UPnP Forum*. “UPnP Device Architecture 1.1.” Last access on 9 March 2018 at http://upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.1.pdf.

36. Microsoft. (28 March 2003). *Microsoft TechNet*. “What Is SNMP?” Last accessed on 1 October 2017 at https://technet.microsoft.com/en-us/library/cc776379%28v=ws.10%29.aspx.

37. John McCormick. (11 April 2001). *TechRepublic*. “Lock IT Down: Don’t allow SNMP to compromise network security.” Last accessed on 1 October 2017 at http://www.techrepublic.com/article/lock-it-down-dont-allow-snmp-to-compromise-network-security/.

38. Kelly Jackson Higgins. (22 May 2014). *Dark Reading*. “SNMP DDoS Attacks Spike.” Last accessed on 1 October 2017 at http://www.darkreading.com/attacks-breaches/snmp-ddos-attacks-spike/d/d-id/1269149.

39. H. Michael Newman. (1998). *BACnet*. “BACnet: Answers to Frequently Asked Questions.” Last accessed on 9 March 2018 at http://www.bacnet.org/FAQ/HPAC-3-97.html.

40. Tridium. (2018). *Tridium*. “Niagara 4.” Last accessed on 9 March 2018 at https://www.tridium.com/en/products-services/niagara4.

41. Allen-Bradley. (2017). *Rockwell Automation*. “Classic 1785 PLC-5 Programmable Controllers.” Last accessed: October 1, 2017. http://literature.rockwellautomation.com/idc/groups/literature/documents/um/1785-um001_-en-p.pdf.

42. HealthIT.gov. (September 22, 2016). *HealthIT.gov*. “Benefits of EHRs.” Last accessed on 15 August 2017 at https://www.healthit.gov/providers-professionals/electronic-medical-records-emr.

43. NIST. (2017). “Framework for Improving Critical Infrastructure Cybersecurity.” Last accessed on 8 March 2018 at https://www.nist.gov/sites/default/files/documents/2017/12/05/draft-2_framework-v1-1_without-markup.pdf.

44. FDA. (6 May 2015). *AccessGUDID*. “ABOUT AccessGUDID.” Last accessed on 20 October 2017 at https://accessgudid.nlm.nih.gov/.

45. Bar Code Graphics Inc. *Bar Code Graphics*. “FDA UDI & GS1.” Last accessed on 8 March 2018 at https://www.barcode.graphics/fda-udi-mandate/.

46. Arthur Allen. (8 August 2016). *Politico*. “FDA guidance could improve cybersecurity.” Last accessed on 20 October 2017 at http://www.politico.com/tipsheets/morning-ehealth/2016/08/fda-guidance-could-improve-cybersecurity-fbi-skeptical-of-medical-board-compact-ig-investigates-cyber-in-dod-health-care-215749.

47. Nat Garun. (30 August2017). *The Verge*. “Almost half a million pacemakers need a firmware update to avoid getting hacked.” Last accessed on 21 October 2017 at https://www.theverge.com/2017/8/30/16230048/fda-abbott-pacemakers-firmware-update-cybersecurity-hack.

48. Sophos. (5 May 2015). *Naked Security*. “Bugs in the hospital: how to pwn your own pethidine machine.” Last accessed on 20 October 2017 at https://nakedsecurity.sophos.com/2015/05/05/bugs-in-the-hospital-how-to-pwn-your-own-pethidine-machine/.

49. US-CERT. (13 June 2013). *ICS-CERT*. “Medical Devices Hard-Coded Passwords.” Last accessed on 23 October 2017 at https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01.

50. Scrypt Inc. (2017). “Mobile health & HIPAA: Playing it safe in 2017.” Last accessed on 20 October 2017 at https://www.docbookmd.com/wp-content/uploads/2017/08/WhitePaper_MobileHealthHIPAA.pdf.

51. Judy Mottl. (10 January 2016). *Fierce Healthcare*. “Report: FDA-approved mobile health apps pose security risk.” Last accessed on October 17, 2017 at http://www.fiercehealthcare.com/mobile/report-fda-approved-mobile-health-apps-pose-security-risks.

52. Codified Security. (3 January 2017.) *Codified Security*. “Mhealth apps are a priority, what about security?” Last accessed on 9 March 2018 at https://codifiedsecurity.com/mhealth-apps-are-a-priority-what-about-security/.

53. Mary-Ann Russon. (12 November 2015). *IBM Times*. "Stop buying cheap Chinese Android tables on Amazon- they come infected with malware." Last accessed on 22 October 2017 at http://www.ibtimes.co.uk/amazon-selling-least-30-brands-cheap-chinese-android-tablets-infected-cloudsota-malware-1528442.

54. Dan Goodin. (11 March 2017). *Ars Technica*. "Malware found preinstalled on 38 Android phones used by 2 companies." Last accessed on 9 March 2018 at https://arstechnica.com/information-technology/2017/03/preinstalled-malware-targets-android-users-of-two-companies/.

55. Jessica Davis. (29 April 2016). *Health IT News*. "American Dental Association sends malware-infected USB drives to its members." Last accessed on 8 March 2018 at http://www.healthcareitnews.com/news/american-dental-association-sends-malware-infected-usb-drives-its-members.

56. Sheryl Harris. (8 August 2012). *Cleveland.com*. "HireRight to pay 2.6 million for errors in background reports on consumers." Last accessed on 22 October 2017 at http://www.cleveland.com/consumeraffairs/index.ssf/2012/08/hireright_to_pay_26_million_fo.html.

57. Evan Sweeny. (19 April 2017). *Fierce Healthcare*. "Survey: Hospital IT execs see employees as their biggest security threat." Last accessed on 23 October 2017 at http://www.fiercehealthcare.com/privacy-security/survey-hospital-it-execs-see-employees-as-their-biggest-security-threat.

58. Robby Mitchell. (29 November 2012). *Tampa Bay Times*. "Feds: IDs stolen from Tampa ER patients used for Tax fraud." Last accessed on 20 October 2017 at http://www.tampabay.com/news/publicsafety/crime/feds-ids-stolen-from-tampa-er-patients-used-for-tax-fraud/1263939.

59. Infosec Institute. (4 September 2016). *Infosec Institute*. "Insider threats at hospitals." Last accessed on 23 October 2017 at http://resources.infosecinstitute.com/insider-threats-at-hospitals/#gref.

60. Cara Johnson. (26 May 2017). *Tehachapi News*. "Security breach leads to release of information used to pay TVHD, Adventist Health." Last accessed on 24 October 2017 at http://www.tehachapinews.com/news/security-breach-leads-to-release-of-information-used-to-pay/article_875d2a22-4253-11e7-9162-5b5d79529238.html.

61. Databreaches.net. (28 June 2016). *Databreaches.net*. "264,000 and counting: Hack of HER/EMR vendor leaves clients scrambling." Last accessed on 23 October 2017 at https://www.databreaches.net/264000-and-counting-hack-of-ehremr-vendor-leaves-clients-scrambling/.

62. Trend Micro. (30 August 2017). *Trend Micro Simply Security Blog*. "How Hackers have improved their BEC attack methods." Last accessed on 1 November 2017 at http://blog.trendmicro.com/how-hackers-have-improved-their-bec-attack-methods/.

63. Cheri Hummel. (7 February 2017). *California Hospital Association*. "IRS Warns Hospital of W2 Phishing Scam." Last accessed on 23 October 2017 at https://www.calhospital.org/cha-news-article/irs-warns-hospitals-w-2-phishing-scam.

64. Databreaches.net. (19 February 2017). *Databreaches.net*. "2016 W-2 data up for sale on dark web." Last accessed on 21 October 2017 at https://www.databreaches.net/2016-w-2-data-up-for-sale-on-the-dark-web/.

65. HIPAA Journal. (19 May 2017). *HIPAA Journal*. "Thomas Boyd Hospital: Potential HIPAA violations, theft allegations, no exposed PHI." Last accessed on 23 October 2017 at https://www.hipaajournal.com/boyd-hospital-dispute-property-sale-6554/.

66. Robert McMillan. (2 July 2009). *PCWorld*. "Security Guard Charged with Hacking Hospital Systems." Last accessed on 23 October 2017 at https://www.pcworld.com/article/167756/article.html.

67. Jessica Davis. (15 August 2017). *HealthCare IT news*. "Hackers breach third party cloud vendor TekLinks." Last access: 20 October 2017 at http://www.healthcareitnews.com/news/hackers-breach-third-party-cloud-vendor-teklinks.

68. John Cusimano. (2011). *SCADA Hacker*. "Assessing the Security of ICS Using Threat Modeling." Last accessed on 12 October 2017 at https://scadahacker.com/howto/howto-threatmodeling.html.

69. Microsoft. (June 2003). *Microsoft Developer Network*. "Chapter 3 Threat Modeling." Last accessed on 14 May 2017 at https://msdn.microsoft.com/en-us/library/aa302419.aspx.

70. David Czagan. (21 May 2014). *InfoSec Institute*. "Qualitative Risk Analysis with the DREAD Model." Last accessed on 14 May 2017 at http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/.

71. David Czagan. (21 May 2014). *InfoSec Institute*. "Qualitative Risk Analysis with the DREAD Model." Last accessed on May 14, 2017. http://resources.infosecinstitute.com/qualitative-risk-analysis-dread-model/.

72. Microsoft. (June 2003). *Microsoft Developer Network*. "Chapter 3 Threat Modeling." Last accessed on 14 May 14 2017 at https://msdn.microsoft.com/en-us/library/aa302419.aspx.

73. Datica. (2017). *Datica*. "HITRUST vs. HIPAA." Last accessed on 8 August 2017 at http://content.datica.com/hipaa-vs.-hitrust.

74. Numaan Huq. (11 March 2015). *TrendLabs Security Intelligence Blog*. "Defending Against PoS RAM Scrapers: Current and Next-Generation Technologies." Last accessed on 8 August 2017 at https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-defending-against-pos-ram-scrapers.pdf.

75. NIST (8 May 2017). *NIST*. "Securing Wireless Infusion Pumps." Last accessed 23 February 2018 at https://nccoe.nist.gov/publication/1800-8/VolA/.

76. FDA. (28 December 2016). *FDA*. "Postmarket Management of Cybersecurity in Medical Devices." Last accessed 11 August 2017 at https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf.

77. US-CERT. (June 13, 2013). *ICS-CERT*. "Medical Devices Hard-Coded Passwords". Last accessed on 10 August 2017 at https://ics-cert.us-cert.gov/alerts/ICS-ALERT-13-164-01.

78. Steve Ranger. (8 December 2016). *ZDNet*. "Windows XP: Why hospitals are still using Microsoft's antique operating system." Last accessed on 10 August 2017 at http://www.zdnet.com/article/windows-xp-why-hospitals-are-still-using-microsofts-antique-operating-system/.

79. Mayo Clinic. (25 March 2015). *Mayo Clinic*. "Clinic CT-Scan." Last accessed on 15 August 2017 at http://www.mayoclinic.org/tests-procedures/ct-scan/basics/definition/prc-20014610.

80. Mayo Clinic. (24 January 2015). *Mayo Clinic*. "Ultrasounds." Last accessed on 10 August 2017 at http://www.mayoclinic.org/tests-procedures/ultrasound/basics/definition/prc-20020341.

81. Laurie Blount. (22 June 2015). *Iatric Blog*. "Smart Pump Programming and EHR Integration – a roadmap for understanding." Last accessed on 10 August 2017 at http://blog.iatric.com/medical-device-integration/smart-pump-programming-and-ehr-integration.

82. Mayo Clinic. (August 16, 2017). *Mayo Clinic*. "Home enteral nutrition." Last accessed on 17 August 2017 at http://www.mayoclinic.org/tests-procedures/home-enteral-nutrition/home/ovc-20346383.

83. Mayo Clinic. (Unknown). *Mayo Clinic*. "Patient Controlled Analgesia PCA." Last accessed on 15 August 2017 at http://www.mayoclinic.org/patient-controlled-analgesia-pca/img-20008231.

84. Infuserve America. (Unknown). *Infuserve America*. "Elastomeric Pumps." Last accessed on 12 August 2017 at https://infuserveamerica.com/104/elastomeric-pumps/.

85. FDA. (23 February 2016). *FDA*. "Infusion Pump: Glossary." Last accessed on 15 August 2017 at https://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/InfusionPumps/ucm202502.htm#syringeinfusionpump.

86. NIH. (February 1, 2011). *NIH*. "What Is a Ventilator?" Last accessed on 12 August 2017 at https://www.nhlbi.nih.gov/health/health-topics/topics/vent.

87. News Medical Life Sciences. (Unknown). *News Medical Life Sciences*. "Anesthesia Machines." Last accessed on 15 August 2017 at https://www.news-medical.net/Clinical-and-Diagnostics/Anesthesia-Machines.

88. NIH. (8 November 2013). *NIH*. "What To Expect During Heart Surgery." Last accessed on 5 August 2017 at https://www.nhlbi.nih.gov/health/health-topics/topics/hs/during.

89. National Kidney Foundation. (2017). *National Kidney Foundation*. "Hemodialysis." Last accessed on 15 August 2017 at https://www.kidney.org/atoz/content/hemodialysis.

90. FDA. (30 November 2017). *FDA*. "Medical Lasers." Last accessed on 15 August 2017 at https://www.fda.gov/radiation-emittingproducts/radiationemittingproductsandprocedures/surgicalandtherapeutic/ucm115910.htm.

91. Medline Plus. (9 June 2015). *Medline Plus*. "Robotic surgery." Last accessed on 12 August 2017 at https://medlineplus.gov/ency/article/007339.htm.

92. Varian Medical Systems. (Unknown). *Varian Medical Systems*. "Radiotherapy." Last accessed on 10 August 2017 at https://www.varian.com/oncology/solutions/radiotherapy.

93. Med Cert. (unknown). *Med Cert*. "Non-active medical devices." Last accessed on 10 August 2017 at http://www.med-cert.com/en_non-active-medical-devices/.

94. TTP. (Unknown). *TTP*. "Medical Devices Saving lives, saving money." Last accessed on 12 August 2017 at http://www.ttp.com/medical-devices.

95. HealthIT.gov. (22 September 2016). *HealthIT.gov*. "Benefits of EHRs." Last accessed on 15 August 2017 at https://www.healthit.gov/providers-professionals/electronic-medical-records-emr.

96. NIH. (March 2016). *NIH*. "Laboratory Information Systems." Last accessed on 10 August 2017 at https://www.ncbi.nlm.nih.gov/pubmed/26851660.

97. Search HealthIT. (Unknown). *Search Health IT Tech Target*. "Radiology Information System (RIS)". Last accessed on 12 August 2017 at http://searchhealthit.techtarget.com/definition/Radiology-Information-System-RIS.

98. Mapcon. (Unknown). *Mapcon*. "Hospital Maintenance Management Software." Last accessed on 10 September 2017 at http://www.mapcon.com/us-en/hospital-healthcare-facility-maintenance-management.

99. Search HealthIT. (Unknown). *Search HealthIT*. "Picture Archiving and Communication System-PACS." Last accessed on 15 August 2017 at http://searchhealthit.techtarget.com/definition/picture-archiving-and-communication-system-PACS.

100. Policy Medical. (Unknown). *Policy Medical*. "Best Practices in Clinical Order Set Management for Hospitals." Last accessed on 12 September 2017 at https://www.policymedical.com/best-practices-clinical-order-set-management-hospitals/.

101. HIMSS. (5 January 2012). *HIMSS*. "Definitions of mHealth." Last accessed on 12 August 2017 at http://www.himss.org/definitions-mhealth.

102. World Health Organization. (2001). *WHO*. "Introduction to Medical Equipment Inventory Management." Last accessed on 15 September 2017 at http://apps.who.int/iris/bitstream/10665/44561/1/9789241501392_eng.pdf.

103. Cornell. (2017). *Cornell*. "Medical Reporting Paging." Last accessed on 10 September 2017 at https://www.cornell.com/MedicalReportingPaging.

104. Stephen Hilt and Philippe Lin. (2016). *Trend Micro*. "Leaking Beeps: Unencrypted Pager Messages in the Healthcare Industry." Last accessed on 27 February 2018 at http://www.trendmicro.it/media/wp/leaking-beeps-whitepaper-en.pdf.

105. Siemens. (2014). *Siemens*. "Total Building Solutions for Hospitals." Last accessed on 12 September 2017 at https://www.downloads.siemens.com/download-center/Download.aspx?pos=download&fct=getasset&id1=A6V10647452.

106. Wasp Buzz (24 January 2012). *Wasp Barcode*. "Barcode technology in healthcare: What you need to know." Last accessed on 12 September 2017 at http://www.waspbarcode.com/buzz/barcode-technology-healthcare/.

107. Esther Y Fung. (November-December 2009). *NIH*. "Do Automated Dispensing Machines Improve Patient Safety?" Last accessed on 12 September 2017 at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2827025/.

108. Chris Woodford. (7 February 2017). *Explainthatstuff*. "Pneumatic Tube transport." Last accessed on 14 September 2017 at http://www.explainthatstuff.com/pneumatic-tube-transport.html.

Created by:

TrendLabs

The Global Technical Support and R&D Center of TREND MICRO

TREND MICRO™

Trend Micro Incorporated, a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years experience, we deliver top-ranked client, server, and cloud-based security that fits our customers' and partners' needs; stops new threats faster; and protects data in physical, virtualized, and cloud environments. Powered by the Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit **www.trendmicro.com**.

HITRUST

HITRUST®

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, across a wide range of industries, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience.

HITRUST actively participates in many efforts in government advocacy, community building and cybersecurity education. For more information, visit www.hitrustalliance.net.

TREND MICRO™

Securing Your Connected World