Homeland Security
National Protection and Programs Directorate
Office of Cyber and Infrastructure Analysis (OCIA)
Critical Infrastructure Security and Resilience Note

(U) January 24, 2017; 1000 EST

(U) HEALTHCARE AND PUBLIC HEALTH SECTOR CYBERDEPENDENCIES

(U) Prepared By: The U.S. Department of Homeland (DHS)/Office of Cyber and Infrastructure Analysis and the DHS/Office of Intelligence and Analysis.

(U//FOUO) The Department of Homeland Security (DHS) assesses that given the high value of patient information and proprietary data on the black market, the Healthcare and Public Health Sector will continue to be one of the primary targets for malicious cyber actors. Stolen health data sells on the black market for more than 10 to 20 times the price of stolen credit card data. DHS assesses that growth in the medical device market over the next 4 years will result in more devices connected to the Internet, and an increase in the number of cyber-related incidents that target those devices. This is partly because manufacturers do not place enough emphasis on the security of medical devices.

(U) Scope Note: This note informs infrastructure and cybersecurity analysts about the Healthcare and Public Health Sector's common cyber-dependent processes and the potential consequences of cyber-related incidents affecting those processes. Infrastructure is cyber-dependent when it relies on computers or information technology to support its physical operations and essential functions This note is not intended to serve as an exhaustive list or technical review of the dependencies. Analysis of complex, sophisticated, and distributed cyber intrusions against multiple Healthcare and Public Health Sector assets is beyond the scope of this note.

(U) This product was coordinated with the DHS/National Protection and Programs Directorate (NPPD)/Office of Infrastructure Protection/Sector Outreach and Programs Division; the DHS/NPPD/Office of Cybersecurity and Communications/National Cybersecurity and Communications Integration Center; the DHS Office of Intelligence and Analysis; and, the Department of Health and Human Services (HHS)/Office of the Assistant Secretary for Preparedness and Response.

(U) SECTOR BACKGROUND

(U) The Healthcare and Public Health Sector provides goods and services that are integral to maintaining local, national, and global health security. Further, the Healthcare and Public Health Sector constitutes a significant portion of the U.S. economy.[1] The Centers for Medicare and Medicaid Services, a federal agency within the HHS, estimates that 17.8 percent or $3.2 trillion of our Nation's Gross Domestic Product was spent on healthcare in 2015.[2]

(U) The Healthcare and Public Health Sector is large and diverse, spanning both the public and private sectors. It employs over 14 million workers who represent approximately 10 percent of the total U.S. workforce.[3] The Sector includes publicly accessible hospitals, research centers, suppliers, manufacturers, and other physical assets. The Sector also includes large and complex public-private information and communications technology systems required to finance care delivery and to support the rapid, secure transmission and storage of large amounts of

[1] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. P. 4. Accessed May 1, 2016.
[2] (U) Centers for Medicare and Medicaid Services, National Health and Expenditure Data. (2015). "National Health Expenditures 2014 Highlights." https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/highlights.pdf, accessed April 9, 2016.
[3] (U) Department of Labor, Bureau of Labor Statistics. (2015). "Current Employment Statistics." www.bls.gov/web/empsit/ceseeb1a.htm. Accessed November 6, 2015.

healthcare data. The Healthcare and Public Health Sector's critical infrastructure contains the following eight functional Subsectors:[4]

- (U) Direct Patient Healthcare—This is the largest Subsector within the Healthcare and Public Health Sector. It contains healthcare systems, doctors' associations, nurses' associations, and medical facilities. It employs 12 million people. This Subsector supports 5,686 registered hospitals with more than 900,000-staffed beds. Over 35.4 million citizens are admitted to these facilities annually.[5]
- (U) Health Information Technology—This rapidly growing field includes medical research institutions, information standards bodies, and electronic health records system vendors. In 2008, fewer than 5 percent of physicians e-prescribed[6] using electronic health records and only 9.4 percent of hospitals implemented a basic electronic health records system. By 2014, approximately 70 percent of physicians were e-prescribing using electronic health records, and 75.5 percent of hospitals adopted at least a basic electronic health records system. This represents a 66.1 percent increase in health information technology in a 6-year span.[7,8]
- (U) Health Plans and Payers—This Subsector consists of health insurance companies and plans, local and state health departments, and state emergency health organizations. This Subsector of the Healthcare and Public Health Sector employs over 500,000 people in the United States. In addition to private insurers, Medicare, Medicaid, and the Children's Health Insurance programs cover more than 100 million, or one-third, of individuals in the United States.[9]
- (U) Mass Fatality Management Services—This Subsector includes cemetery, cremation, and funeral home services. This Subsector of the Healthcare and Public Health Sector employs approximately 133,000 Americans, mostly in small businesses.[10] Approximately 86 percent of funeral homes are owned by families, individuals, or closely held companies, with an average of three to five full-time employees.[11]
- (U) Medical Materials—This Subsector includes medical equipment and supply manufacturers and distributors. Approximately 600,000 people in the United States work in support of the medical supply chain.[12]
- (U) Laboratories, Blood, and Pharmaceuticals—This Subsector contains both state and Federal Government and private sector assets. This Subsector includes pharmaceutical manufacturers, drug store chains, pharmacists' associations, laboratory associations, and blood banks. According to HealthIT.gov, 95 percent of pharmacies in the Nation are actively e-prescribing, and over 32 percent of new prescriptions are sent electronically.[13]
- (U) Public Health—This Subsector involves collaboration between Federal, State, local, tribal and territorial public health programs to improve the health of populations through education, policy, and community services. Public health networks guide local hazard and risk assessments, develop mitigation plans and strategies, facilitate joint public-private sector planning and exercising, and conduct response and recovery operations.[14]
- (U) Federal Response and Program Offices—This Subsector involves the Critical Infrastructure Protection partnership that relies on Federal Government's policy development, funding opportunities, and coordinating activities. The Healthcare and Public Health Sector Government Coordinating Council

---

[4] (U) Department of Homeland Security and Health and Human Service. (n.d.). "Healthcare and Public Health Sector-Specific Plan, 2016," https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. P. 5. Accessed May 1, 2016.
[5] (U) American Hospital Association. (2015). "Fast Facts on U.S. Hospitals." www.aha.org/research/rc/stat-studies/fast-facts.shtml. Accessed November 6, 2015.
[6] (U) According to the Health and Human Services Office of the National Coordinator, e-prescribing is the electronic transmittal of a prescription to a pharmacy from the prescriber.
[7] (U) Health and Human Services. Office of the National Coordinator for Health Information Technology. (2015). *ONC Data Brief*, No. 23. "Adoption of Electronic Health Record Systems Among U.S. Non-Federal Acute Care Hospitals: 2008-2014." www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf. p.1. Accessed November 6, 2015.
[8] (U) Health and Human Services, Office of the National Coordinator for Health Information Technology. (2014). *Data Brief*, No. 18. "E-Prescribing trends in the United States." www.healthit.gov/sites/default/files/oncdatabriefe-prescribingincreases2014.pdf. p. 1. Accessed November 6, 2015.
[9] (U) Health and Human Services, Centers for Medicare and Medicaid Services. (2015). "Understanding and Preventing Provider Medical Identity Theft." www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/Provider-Education-Toolkits/Downloads/understand-prevent-provider-idtheft.pdf. p. 3. Accessed November 6, 2015.
[10] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. p. 5. Accessed May 1, 2016.
[11] (U) Ibid.
[12] (U) Ibid.
[13] (U) Ibid.
[14] (U) Ibid. p. 6

includes diverse federal partnerships from several departments including HHS, the Department of Defense, and the other lifeline Sectors including Energy, Water and Wastewater Systems, Transportation Systems, and Communications.[15]

(U) CYBER SUPPORTED PROCESSES

(U//FOUO) The Healthcare and Public Health Sector relies on a number of processes that are supported by information communication technology. These processes allow for cost-effective measures and real-time data transmission and enhance the efficiency of health care delivery; however, these processes are susceptible to a number of cyber threats.[16] The following are examples of health information technology processes that are potentially vulnerable to cyber attacks:

- (U) Insurance and medical billing and claims technology, electronic health records, and personal data
- (U) Public health data and emergency management systems
- (U) Medical device, including life-sustaining equipment functionality[17]
- (U) Inventory tracking, delivery, stockpiles, and supply chain
- (U) Security and access control systems
- (U) Hospital operations, including the ability to admit or treat patients
- (U) Heating, ventilation, and air conditioning (HVAC) environmental controls
- (U) Digital health and telemedicine
- (U) Proprietary information

(U) CYBERSECURITY INCIDENTS IN THE HEALTHCARE AND PUBLIC HEALTH SECTOR

(U//FOUO) The Healthcare and Public Health Sector is increasingly dependent upon electronic health records and the secure storage and transmission of personal data to dictate care, maintain patient records, and control financial operations.[18] Public health and emergency management systems, medical devices, inventory systems, and facility controls are increasingly connected to computer networks, which amplifies their vulnerability to cyber intrusions and cyber-related incidents.[19,20,21] Malicious cyber actors could harvest personal data, corrupt information, or affect physical security. Larger-scale disasters or attacks on the electronic backbone or supporting infrastructure could eliminate data access across the entire Healthcare and Public Health Sector.[22] In addition, intellectual property theft through cyber intrusions can threaten competitiveness, innovation, and research and development, particularly in areas where proprietary research provides a competitive advantage.[23] Appendix A provides a list of the general types of cyber-based threats. Appendix B lists the types of cyber-based exploits that malicious cyber actors may use against the Healthcare and Public Health Sector.

[15] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. p. 6. Accessed May 1, 2016.
[16] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. p. 9. Accessed May 1, 2016.
[17] This note uses the Food and Drug Administration's definition of medical device. For the full definition, please visit http://www.fda.gov/AboutFDA/Transparency/Basics/ucm211822.htm.
[18] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. p. 5. Accessed May 1, 2016.
[19] (U) For this note, OCIA used the National Institute of Standards and Technology (NIST) Special Publication 800-61 definition of a cyber incident, which is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.
[20] (U) U.S. Department of Commerce. (2012). National Institute of Standards and Technology – Special Publication 800-61 Revision 2, "Computer Security Incident Handling Guide." p. 60. Accessed October 21, 2016.
[21] (U) The U.S. Federal Government uses the NIST definition to define a cyber incident.
[22] (U) Department of Homeland Security and Health and Human Services. (2016). "Healthcare and Public Health Sector-Specific Plan." https://www.dhs.gov/sites/default/files/publications/nipp-ssp-healthcare-public-health-2015-508.pdf. p. 10. Accessed May 1, 2016.
[23] (U) Ibid.

(U) The following sections contain threat and consequence information associated with the potential effects of cyber-related incidents on healthcare and public health cyber-dependent processes. These sections outline the effects using the information security attributes of confidentiality, integrity, or availability.

(U) CYBER INCIDENTS AFFECTING MEDICAL DATA

(U//FOUO) Electronic Health Records can contain personal data such as names, birth dates, addresses, Social Security numbers, insurance policy numbers, diagnosis codes, billing information, employment information, and income. Criminal and nation-state cyber actors use malware to exfiltrate personally identifiable information (PII), protected health information, and intellectual property data from healthcare companies for illicit financial gain, stock manipulation, or industrial espionage. Malicious cyber actors sell stolen electronic health records on the black market for more than 10 to 20 times the price of stolen credit card data.[24,25] Malicious cyber actors can use this data to open new credit accounts, access an individual's personal financial accounts, falsify medical identities to buy prescription drugs or medical equipment, or file fraudulent claims with insurers.

(U//FOUO) Some methods of attack used by malicious cyber actors against the Healthcare and Public Health Sector include ransomware or distributed denial-of-service attacks (DDoS). New ransomware variants display increasingly advanced function and capabilities such as targeted delivery techniques, obfuscation mechanisms, persistence capabilities and backup system deletion tools that likely constitute a high threat to the Healthcare and Public Health Sector.

- (U//FOUO) According to a Federal Government official, advanced persistent threat malware infected eighty percent of U.S. healthcare network systems in late August 2015. DHS Industrical Contorl Systems Cyber Emergency Response Team (ICS-CERT) uncovered a total of 1.66 gigabytes of data staged for exfiltration. One system contained 290 malware samples, with 76 samples being unique.[26]
- (U//FOUO) On June 23, 2016, the criminal hacker group known as Armada Collective sent an email to a U.S. healthcare company based in Rhode Island threatening to conduct a DDoS attack if the company failed to pay a ransom in Bitcoin. As of mid-October 2016, State officials reported the company did not pay the ransom and a DDoS attack did occur.[27]
- (U//FOUO) A ransomware attack in March 2016 compromised a U.S.-based hospital using an outdated server vulnerability, according to a state government official with direct access to the information. The cyber actors used administrator-level access to locate and encrypt more than 100,000 files on 4,000 systems, including 600 servers. This attack denied hospital personnel access to sensitive files for two days, according to the same reporting.[28]
- (U) On February 5, 2016, malicious cyber actors encrypted access to patient medical records and other essential computer systems at a Los Angeles, California hospital. Hospital administrators paid the cyber actors a ransom of $17,000 to regain access to their computer systems.[29]

(U) Table 1 shows the potential effects of cybersecurity breaches and exfiltration of medical data.

[24] (U) Reuters. (2014). "Your Medical Record Is Worth More to Hackers Than Your Credit Card." www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924#Wxhu02qUHKAgy1HQ.97. Accessed November 30, 2015.
[25] (U) *NetworkWorld.* (2015). "Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers." www.networkworld.com/article/2880366/security0/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html. Accessed November 30, 2015.
[26] (U//FOUO) DHS IIR 005 0233 16/DHS CYB; 28 AUG 2015; Source is a Federal Government employee with direct access to the reported information. Extracted information is U//FOUO.
[27] (U//FOUO) DHS IIR 4 045 0004 17/RI; 22 NOV 2016; DOI 23 JUN 2016 – 15 OCT 2016; (U//FOUO) Alleged Cyber Hacking Group Threatening Distributed Denial of Service Attack on a Rhode Island-based Healthcare company if Bitcoin Payment is not Received; Extracted information is U//FOUO.
[28] (U//FOUO) DHS; IIR 4 044 0044 16; 190218Z MAY 2016; DOI 20-22 MAR 2016; (U//FOUO) Ransomware Infecting a US-Based Hospital via an Internet Protocol Address Resolving to Russia; Extracted information is U//FOUO.
[29] (U) *International Business Times.* (2016). "Ransomware Hackers a Bigger Threat than Ever, Forcing Hospitals and Police to Pay Hostage Fees." http://www.ibtimes.com/ransomware-hackers-bigger-threat-ever-forcing-hospitals-police-pay-hostage-fees-2319822. Accessed March 21, 2016.

(U) The contents of this table are U//FOUO.

(U//FOUO) TABLE 1— POTENTIAL EFFECTS OF CYBERSECURITY INCIDENTS RELATED TO MEDICAL DATA

Medical Data			
Types of Medical Data	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Electronic Health Records	An adversary has protected health information, financial information. Companies have regulatory compliance and litigation concerns.	An adversary can alter records.	An adversary can provide or deny access to records, and in some cases may demand payment for access to records.
Billing Systems	An adversary has protected health information, financial information. Companies have regulatory compliance and litigation concerns.	An adversary can alter records and commit billing fraud.	An adversary can provide or deny access to billing systems.
Electronic Prescriptions	An adversary has protected health information, financial information. Companies have regulatory compliance and litigation concerns.	An adversary can alter records and falsely issue or change the type of prescription drugs.	An adversary can provide or deny access to electronic prescriptions systems.
Proprietary Information (e.g., pharmaceuticals, research and development on medical devices)	An adversary has trade secrets, such as proprietary drug formulas.	An adversary can alter, delete, or sell proprietary information.	An adversary can provide or deny access to proprietary information.

(U) CYBER INCIDENTS AFFECTING MEDICAL DEVICES

(U//FOUO) In 2015, the global medical device market had an estimated net worth of approximately $4 billion; the United States accounted for 43 percent of the market.[30] According to open-source reporting, by 2020, the global medical device market will be worth around $5 billion.[31] This projected growth will result in more medical devices connected to the Internet, and an increase in the number of cyber-related incidents that target medical devices. This is partly because manufacturers do not place enough emphasis on the security of medical devices.[32]

(U//FOUO) Medical devices infected with malware can provide malicious cyber actors with access to hospital networks and infrastructure, which may allow the theft of personal information, the denial of the device's availability, or the loss of integrity through the insertion of false information into the device itself. Further, the compromise of medical devices could allow malicious cyber actors to gain access to hospital systems through backdoors on a network. Once inside the network of a hospital or medical facility, a cyber actor could gain access to patient health records, proprietary data, and access to other devices.

[30] (U) U.S. Department of Commerce, International Trade Administration. The Medical Technology Industry in the United States, https://www.selectusa.gov/medical-technology-industry-united-states. p 1. Accessed October 28, 2016.
[31] (U) Huang, Jason. (2016). "TrendForce Anticipates Soaring Growth for Global Medical Device Market as Healthcare and ICT Industries Converge." *TrendForce.* http://press.trendforce.com/node/view/2368.html. March 10, 2016, accessed October 24, 2016.
[32] (U) Jones, Russel L. and Coughlin, S. (2013)."Deloitte, Issue Brief: Networked medical device cybersecurity and patient safety – perspectives' of health care information cybersecurity executives." p. 8. Accessed October 28, 2016.

- (U) In May 2015, TrapX, a cyber security firm, released a report detailing "extensive compromise of a variety of medical devices including X-ray equipment, picture archive and communications systems, and blood gas analyzers" in three different hospitals. Cyber attackers infected the medical devices with malware, which enabled them to access the hospital networks and exfiltrate confidential data and protected health information. TrapX believed the malware could move laterally and target additional medical devices operating on the network.[33]
- (U//FOUO) The ICS-CERT Advanced Analytic Lab on January 6, 2016 verified that malware found by TrapX was an 'Allaple worm' variant beaconing to a command and control internet protocol from a medical environment with comprmised medical devices according to ICS-CERT forensic reports and a private security firm. Malware found in a hospital setting as recently as November 2016 was specifically designed to install backdoors in medical devices, move laterally to spread the infection to hospital networks, and exfiltrate protected health information, according to the TrapX private cybersecurity firm.[34]
- (U//FOUO) In February 2014, two separate United States Air Force network security entities were alerted to the presence of a password-stealing malware on a medical device picture archiving and communications system.[35]

(U) The contents of this table are U//FOUO.

(U//FOUO) TABLE 2— POTENTIAL EFFECTS OF CYBERSECURITY INCIDENTS RELATED TO MEDICAL DEVICES

Medical Devices			
Types of Medical Devices	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Picture Archiving and Communication System	An adversary can access patient electronic images delivered from a varierty of medical imaginging instruments such as computed tomography (CT) scanner, magnetic resonance imaging (MRI) scanners, and X-rays.	An adversary can alter device specifications or turn off the device.	An adversary can provide or deny access to records, and in some cases may demand payment for access to records.
Infusion Pumps	A hacker can access sensitive patient record information through a device's connection with a medical facility or commercial vendor.	A hacker can change the dosages of drugs delivered to patients and alter the pump's display screens to indicate a safe dosage was being delivered.	An adversary can provide or deny access to the medical device, and in some cases may demand payment for proper device functionality.

(U) CYBER INCIDENTS AFFECTING BUSINESS MANAGEMENT SYSTEMS

(U//FOUO) Business management systems are the policies, practices, procedures, and processes used by a company or organization to perform management tasks and activities.[36] Business management systems include

[33] (U) *Computerworld.* (2015). "MEDJACK: Hackers Hijacking Medical Devices to Create Backdoors in Hospital Networks." www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html. Accessed December 23, 2015.
[34] (U//FOUO) ICS-CERT; E-mail; 21 JAN 2016; DOI 28 AUG 2015; RFI on IIR 4 005 0233 16 from I&A; Email interaction between intelligence collector, ICS-CERT, and intelligence analyst. Extracted information is U//FOUO.
[35] (U//FOUO) 35th Intelligence Squadron; 2 SEP 2014; Network Intelligence Report; Extracted information is U//FOUO.
[36] (U) FitSM – Standards for lightweight IT Service Management, "Part 0: Overview and Vocabulary," http://fitsm.itemo.org/sites/default/files/FitSM-0_Overview_and_vocabulary.pdf. p.7. Accessed October 24, 2016.

payroll management, inventory tracking systems, and supply chain management. Malicious cyber actors can gain unauthorized access to these systems in a variety of ways, such as weak passwords in remote desktop protocols and the access granted to third party vendors, associated universities, and subcontracted business associates. A cybersecurity incident that affects payroll could result in PII exposure, potentially leading to identity theft or financial losses for both the company and the individuals affected. Further, a cybersecurity incident that interrupts inventory and supply chain management systems could lead to resupply disruptions. This could result in the inability to process orders or the involuntary exposure of proprietary business information.

- (U//FOUO) On October 11, 2016, a cybercriminal hacker group claimed they stole over 3,500 electronic medical records (EMR) from a New York-based healthcare provider. According to open source reporting, the cybercriminals exploited a known vulnerability in an EMR software program that allowed unauthorized access to sensitive data. The group claimed the patient information was for sale on the public domain because the healthcare provider was reluctant to pay a ransom.[37]
- (U) In 2010, an individual hacked into a former employer's computer system, causing almost $17,000 in damage. The individual made numerous unauthorized intrusions into the computer system for Suncoast Community Health Centers in Ruskin, Florida. The individual deleted and moved files, changed administrative passwords and account names, removed access to infrastructure systems, tampered with pay and accrued leave rates on the payroll system, and compromised the network's firewall.[38]

(U) Table 3 presents the potential infrastructure effects of cybersecurity incidents related to internal business management processes such as payroll, inventory, and supply chain management.

(U) The contents of this table are U//FOUO.

(U//FOUO) TABLE 3— POTENTIAL EFFECTS OF CYBERSECURITY INCIDENTS RELATED TO BUSINESS MANAGEMENT SYSTEMS

Business Management Systems			
Business Management System Functions	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Payroll Management	An adversary has PII and financial information. Companies have compliance concerns.	An adversary can alter payroll actions and add or subtract payees.	The system will be out of service and may delay payments,
Inventory Management	An adversary knows the quantity of inventory in different locations.	An adversary can alter inventory data so that the company runs out or has too many orders.	The system will be out of service, possibly with inadequate manual inventory processes, which may lead to delays in accounting and resupply processes.
Supply Chain Management	An adversary knows the thresholds and status for inventory and the normal procedures for reorder. Some customer and business proprietary data may be stolen.	An adversary can disrupt supply chain management, cause an overorder or underorder, or redirect deliveries.	The system will be out of service and manual back-up systems will be used.

[37] (U//FOUO) OSIR-04001-0044-17; 28 OCT 2016; A hacking group exploits healthcare information systems and sells compromised electronic healthcare records on dark web; Overall document classification is U//FOUO. Source is a group of hackers who posts links to data stolen from U.S.-based healthcare providers. This is a new source whose information has not been evaluated. Extracted information is U//FOUO.
[38] (U) *Bradenton Herald.* (2010). "Palmetto Woman Gets 18 Months in Prison for Hacking Former Employer." www.bradenton.com/news/local/crime/article34498863.html. Accessed December 24, 2015.

(U) CYBER INCIDENTS AFFECTING BUILDING AND ACCESS CONTROL SYSTEMS

(U//FOUO) Building and access control systems are critical services that allow a building to meet the functional, security, and operational requirements of building occupants.[39,40] According to a December 2014 report by the Government Accountability Office, building and access control systems include closed circuit camera systems, access control systems (e.g., identification card readers, access control servers, or control panels), fire suppression systems, power and lighting control systems, and heating, ventilations, and air conditioning systems.[41] The compromise of these control systems may allow an adversary to gain unauthorized access to secured areas, deny access to authorized facility personnel, and decrease the ability of facility security to detect and respond to intruders.

- (U) According to a October 16, 2016 report, McAfee security report focusing on the Healthcare and Public Health Sector, activity on Dark Web forums show cybercriminals advertising a request for insiders employed at healthcare organizations to approve fraudulent payments from a popular credit-based payment service.[42]
- (U) In February 2009, a former contract security guard at the North Central Medical Plaza in Dallas, Texas, gained physical access to at least 14 computers, including a nurses station computer and a heating, ventilation, and air conditioning (HVAC) computer in a locked room. The individual installed a program on the computers that allow remote access. The indivdual also compromised the integrity of the computers by removing some security features (e.g., uninstalling anti-virus programs), which made the computer systems and related networks more vulnerable to attack. The individual installed malicious codes (bots) on most of the computers, and planned to use the compromised computers to conduct DDoS attacks and to send spam. The individual remotely accessed the HVAC computer five times and knew that modifying the computer controls could affect the facility's temperature. By modifying the facility's environmental controls, the individual could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. The individual could have also affected treatment regimes, including the efficacy of all temperature-sensitive drugs and supplies.[43]

(U) Table 4 presents the potential infrastructure effects of cybersecurity incidents related to building and access control systems.

(U) The contents of this table are U//FOUO.

(U//FOUO) TABLE 4— POTENTIAL EFFECTS OF CYBERSECURITY INCIDENTS RELATED TO BUILDING AND ACCESS CONTROL SYSTEMS

Building and Access Control Systems			
Functions of Building and Access Control Systems	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Access control authorization database	An adversary has PII[44] and general intelligence about who has access.	An adversary can alter or modify databases to allow for or deny access to individuals.	Inability to manage access updates.

[39] (U) National Institute of Building Sciences. (2015). "Learn the Techniques to Better Protect Building Control Systems." https://www.nibs.org/news/227903/Learn-the-Techniques-to-Better-Protect-Building-Control-Systems.htm. Accessed October 24, 2016.
[40] (U) Federal Facilities Council, "Cybersecurity Building Control Systems," http://sites.nationalacademies.org/cs/groups/depssite/documents/webpage/deps_160389.pdf. Accessed October 24, 2016.
[41] (U) United States Government Accountability Office, Federal Facility Cybersecurity. (2014). "DHS and GSA Should Address Cyber Risk to Building and Access Control Systems." http://www.gao.gov/assets/670/667512.pdf. Accessed October 25, 2016.
[42] (U) *Intel Security.* (2016). "Health Warning: Cyberattacks are targeting the health care industry." Source is a for-profit security company
[43] (U) Federal Bureau of Investigation. (2011). "Former Security Guard Who Hacked Into Hospital's Computer System Sentenced to 110 Months in Federal Prison." www.fbi.gov/dallas/press-releases/2011/dl031811.htm. Accessed December 28, 2015.
[44] (U) Personally identifiable information. Access controls sometimes require authentications at the time of establishing an account that would include personally identifiable information.

Building and Access Control Systems			
Functions of Building and Access Control Systems	**Loss of Confidentiality**	**Loss of Integrity**	**Loss of Availability**
Access privileges	An adversary has PII and specific intelligence of patterns of movement.	An adversary can alter or modify an individual's credentials to allow for or deny access.	Difficulty in operating automated access-control systems or triggering alarms. Possible denial of all entry and exit.
Programming set points for heating, ventilating, and air conditioning systems[45]	An adversary knows what the temperature settings are for various times of the day.	An adversary can reprogram environmental settings, which could harm patients and temperature-sensitive laboratory processes, drugs, and supplies.	Heaters or chillers persist in whatever state they were set for or may stop functioning; viruses may significantly slow response times.
Programming the schedule for lighting and any rules for response to sensors	An adversary knows the purpose of the lighting configuration during various times of the day and can infer with the settings when the building is likely unoccupied.	An adversary can reprogram the lighting configuration.	Lighting may persist in whatever state it was set for or may turn off; viruses may significantly slow response times.

(U) CYBERSECURITY CHALLENGES FACING THE HEALTHCARE AND PUBLIC HEALTH SECTOR

(U//FOUO) According to the Institute for Critical Infrastructure Technology, the Healthcare and Public Health Sector is one of the most targeted critical infrastructure sectors by malicious cyber actors.[46] In 2015, the Healthcare and Public Health Sector experienced more cyber-related incidents in terms of data breaches than the other 15 critical infrastructure sectors.[47] The Healthcare and Public Health Sector is also competing with the other critical infrastructure sectors to recruit and retain cybersecurity talent that can defend against and solve its cyber-related issues.[48]

(U//FOUO) In addition to keeping up with the cybersecurity implications of innovation, legacy systems create cybersecurity problems for the Sector.[49] Medical facilities and healthcare organizations pursue newer information technology (IT) systems but often retain older IT systems housing patient information because of incompatibility issues between the age of the systems. In other cases, smaller healthcare organizations retain older IT systems because of the financial cost of implementing new systems. Outdated systems, particularly those no longer supported by the original manufacturer, have the potential to become target vectors for malicious cyber actors to exploit and gain access to a healthcare organization's network.[50]

(U//FOUO) Healthcare and Public Health Sector cyber-supported processes involve the integration of dissimilar systems that rely on diverse technologies. The multifaceted integration will require networks of intricate security solutions for adequate defense. Organizations will at times apply complex solutions to create a defense-in-depth

[45] (U) HVAC; water heaters are likely to follow similar patterns to the HVAC.
[46] (U) Institute for Critical Infrastructure Technology. (2015). "Hacking Healthcare IT in 2016 – Lessons The Healthcare Industry Can Learn From the OPM Breach." http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf. p.1. Accessed December 27, 2016.
[47] (U) Ibid.
[48] (U) Ibid. p. 4.
[49] (U) Ibid. p. 3.
[50] (U) Ibid.

approach; however, these scenarios could create vulnerabilities through mismanagement and misconfiguration caused by a lack of end-user understanding.[51,52]

(U//FOUO) Building security in to medical devices and allocating the necessary time to test the product requires time and money, which can slow a device's entry into the market.[53] For a manufacturer, a delay in releasing the product could result in financial loss for a company in terms of revenue and future investment. In the end, the competition to enter the medical device market results in vulnerable medical devices that are in their nature used for patient health.[54]

(U//FOUO) While information sharing forums specific to this Sector exist, (e.g., Information Sharing and Analysis Organizations and the DHS Homeland Security Information Network), the Sector is challenged with limited reach because many healthcare organizations are not participating and remain unaware of the cyber threats and attacks being targeted against them.[55]

(U) PATH FORWARD

(U//FOUO) DHS assesses that given the high value of patient information and proprietary data on the black market, the Healthcare and Public Health Sector will continue to be one of the primary targets for malicious cyber actors. As the Sector becomes increasingly reliant on cyber-supported systems across all aspects of operations—medical data, medical devices, business management systems, and building and access control systems—the processes introduce a number of vulnerabilities that, if exploited, could result in adverse impact to healthcare facilities and organizations.

(U//FOUO) The Healthcare and Public Health Sector faces a number of cybersecurity challenges ranging from legacy systems to cyber workforce gaps that will remain a focus of continued collaboration between the public and private sector. The consequences from a successful compromise of varying effects, including economic loss and death, draws attention to the following recommendations intended to help organizations work toward a baseline cyber approach:[56,57]

- (U) Establish a security culture. On a regular basis, effectively and proactively train all users on the importance of data security.
- (U) Plan for the unexpected. Integrate cyber-specific response plans into existing emergency response plans.
- (U) Control physical access to information technology devices and systems, servers, and systems; protect mobile devices; and limit network access.
- (U) Control access to protected health information and personally identifiable information.
- (U) Install a firewall to restrict traffic flow and limit unauthorized access to networks.
- (U) Encrypt data to prevent unauthorized use and maintain confidentiality of data.
- (U) Install and maintain antivirus software to prevent compromise and data corruption.
- (U) Use strong, complex passwords; change them regularly; and do not allow computers to remember them.
- (U) Segregate data by maintaining separate, stand-alone servers.
- (U) Keep software patches current.

---

[51] (U) Grifantini, K. (2016). "Healthcare, Hacked." *IEEE Pulse.* http://pulse.embs.org/may-2016/healthcare-hacked/. p.1. Accessed December 30, 2016.
[52] (U) Ward, D. (2016). "Cybersecurity, Simplicity, and Complexity." *New American.* https://static.newamerica.org/attachments/12685-the-comic-guide-to-cybersecurity-and-simplicity/Comic%20Vfinal.5e00364a8df04b7e835ad030046dc5da.pdf. p.7. Accessed December 30, 2016.
[53] (U) Burns, A.J., Johnson, M.E. and Honeyman, P. (2016). "A Brief Chronology of Medical Device Security." *Communications of the Association of Computing Machinery*, Vol. 59, No. 10. http://cacm.acm.org/magazines/2016/10/207766-a-brief-chronology-of-medical-device-security/fulltext. p .7. Accessed December 28, 2016.
[54] (U) Commission on Enhancing National Cybersecurity. (2016). "Report on Securing and Growing The Digital Economy." https://www.whitehouse.gov/sites/default/files/docs/cybersecurity_report.pdf. p. 7. Accessed December 22, 2016.
[55] (U) Health Information Trust Alliance. (2015). "Health Industry Cyber Threat Information Sharing and Analysis." https://hitrustalliance.net/documents/cyber_intel/CTX/CTXFindings_Oct_2015.pdf. p. 8. Accessed December 30, 2016.
[56] (U) Health and Human Services. (2015). "Top 10 Tips for Cybersecurity in Health Care." www.healthit.gov/providers-professionals-newsroom/top-10-tips-cybersecurity-health-care. Accessed November 24, 2015.
[57] (U) Department of Homeland Security US-CERT. (2005). "Protecting Aggregated Data." www.us-cert.gov/security-publications/protecting-aggregated-data. Accessed November 30, 2015.

(U) APPENDIX A: SOURCES OF CYBER-BASED THREATS

(U) The contents of this table are U.

(U) TABLE 5—SOURCES OF CYBER THREATS[58]

Threat Source	Description
State Actors	State actors are most capable, active, and dangerous cyber adversaries due to their access to advanced tradecraft and technical expertise. State actors employ cyber operations to gain a competitive advantage in trade, conduct industrial espionage, and to achieve persistent compromise in foreign networks.
Cybercriminals	Capability comes close to state actors. Profit is typically the sole motivation. Known for the commoditization of malware and exploit tools to reduce technical barriers to carry out criminal activity, such as ransomware and theft of PII.
Criminal Hackers	Low to moderate level of capabilities and lacks the funding and resources compared to that of state actors and cybercriminals. Their cyber activity consists of advancing their political or ideological agenda.
Terrorists	Least capable cyber threat source. Relies on simple online tools to conduct cyber attacks. Use the internet for recruitment and propaganda.

[58] (U) U.S. Department of Homeland Security, Office of Intelligence and Analysis. (n.d.). "Cyber Threats to the Homeland."

(U) APPENDIX B: TYPES OF CYBER-BASED EXPLOITS

(U) The contents of this table are U

(U) TABLE 6—TYPES OF CYBER EXPLOITS[59]

Type of Exploit	Description
Denial of Service	An attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
Distributed Denial of Service	A variant of the denial-of-service attack that uses numerous hosts to perform the attack.
Phishing	A digital form of social engineering that uses authentic-looking but fake emails to request information from users or to direct them to a fake Website that requests information.
Trojan Horse	A computer program that appears to be legitimate, but has a hidden and potentially malicious function that evades security mechanisms by, for example, masquerading as a legitimate program a user would likely execute.
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the user A virus might corrupt or delete data on a computer, use an e-mail program to spread itself to other computers, or even erase everything on a hard disk. Unlike a computer worm, a virus requires human involvement (usually unwitting) to propagate.
Worms	A self-replicating, self-propagating, self-contained program that uses network mechanisms to spread from computer to computer Unlike a computer virus, a worm does not require human involvement to propagate.
Exploits Affecting The Information Security Supply Chain	The installation of hardware or software that contains malicious logic (like a logic bomb, Trojan Horse, or a virus) or an unintentional vulnerability (the result of an existing defect, such as a coding error) or that may be counterfeited may exploit the information security supply chain A supply chain threat can also come from a failure or disruption in the production of a critical product, or a reliance on a malicious or unqualified service provider for the performance of technical services.

(U) The Office of Cyber and Infrastructure Analysis (OCIA) provides innovative analysis to support public and private-sector stakeholders' operational activities and effectiveness and to inform key decisions affecting the security and resilience of the Nation's critical infrastructure. All OCIA products are visible to authorized users at HSIN-CI and Intelink. For more information, contact OCIA@hq.dhs.gov or visit http://www.dhs.gov/office-cyber-infrastructure-analysis

(U) PDM16011

[59] (U) Government Accountability Office. (2014). "Federal Facility Cybersecurity: DHS and GSA Should Address Cyber Risk to Building and Access Control Systems." *Report to Congressional Requesters*, GAO-15-6. www.gao.gov/assets/670/667512.pdf. p. 29. Accessed December 31, 2015.

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu