WHY **MEDICAL DEVICE MANUFACTURERS MUST LEAD ON CYBERSECURITY** IN AN INCREASINGLY CONNECTED HEALTHCARE SYSTEM

Abbott

THE CHERTOFF GROUP

About Abbott

Abbott is a global healthcare company devoted to improving life through the development of products and technologies that span the breadth of healthcare. With a portfolio of leading, science-based offerings in diagnostics, medical devices, nutritionals, and branded generic pharmaceuticals, Abbott serves people in more than 150 countries and employs approximately 94,000 people.

As healthcare becomes increasingly interconnected and data-driven, connected medical devices provide patients and physicians with information to better manage conditions, which improves outcomes and reduces the overall cost of care. No matter how technologically advanced we become, patients come first. Our goal is to ensure our devices, products, and systems meet the highest security standards and that commitment governs how we approach cybersecurity across our business.

We take a broad and deep approach to ensuring safety and security. Because technology and threats continue to evolve, we are constantly evaluating and adapting security measures with the goal of ensuring our patients receive the highest quality care. Our cybersecurity program is built on four key elements, including: cybersecurity-embedded design, constant threat and risk analysis, testing by internal and external experts, and partnering with industry. For more information about Abbott, visit **www.abbott.com**

About The Chertoff Group

The Chertoff Group is a premier global advisory firm focused on security and risk management. The Chertoff Group helps clients grow and secure their enterprise through risk management, business strategy, and merchant banking services.

With a particular focus around security and technology, The Chertoff Group provides a broad array of professional services to help our clients at every stage of the business lifecycle. We leverage our deep subject matter knowledge around important policy matters and security operations to build and execute effective strategies that enable companies to capture new opportunities and create lasting competitive advantage. For those organizations that require tactical security support, we work hand-in-hand with clients to better understand today's threats and assess, mitigate and monitor potential dangers and evolving risks in order to create more secure environments for their business operations.

Headquartered in Washington D.C., The Chertoff Group also maintains offices in Menlo Park and New York City. For more information about The Chertoff Group, visit **www.chertoffgroup.com**

Neil Harbisson is internationally regarded as the world's first cyborg. Born with complete color-blindness, Harbisson has leveraged rapid technological advancements to augment his physical condition. For over a decade, a Bluetooth-enabled, antenna-like sensor implanted into his skull has translated visible and invisible wavelengths into vibrations, which Harbisson perceives as sounds. Far from succumbing to his disability, Harbisson has exploited the capabilities of implantable devices such that the breadth of his "vision"—which covers the full electromagnetic spectrum—actually exceeds that of regular humans.[1]

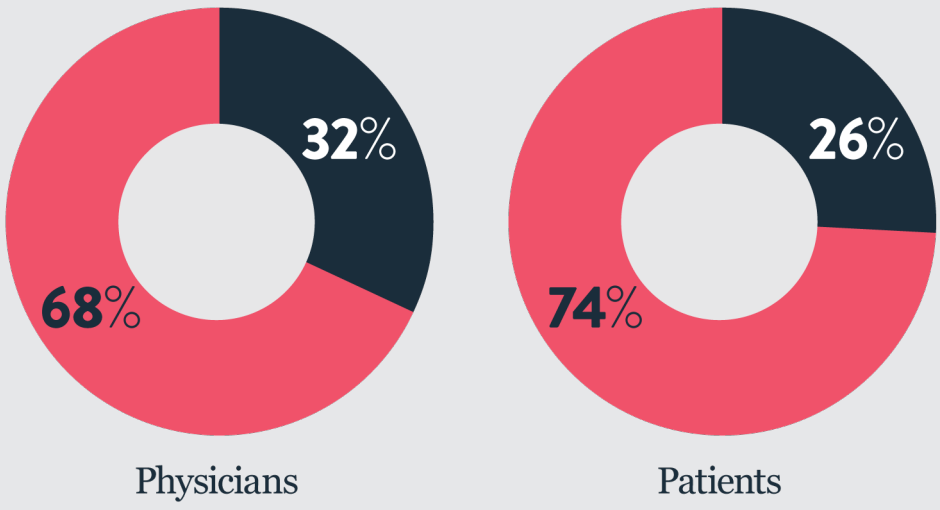
Harbisson is one of many patients reaping the benefits of increased connectivity in the healthcare industry. Connected medical devices—such as pacemakers and insulin pumps that communicate with other networks and devices over the Internet—provide patients and physicians with technology to better manage chronic conditions, improve outcomes, and reduce the overall cost of care[2]. They limit the need for doctor visits, shorten the length of hospitalizations, and enable early detection of potential concerns by sharing vital health data and empowering patients to manage aspects of their own care[3]. According to a new survey conducted by Brunswick Insight—which polled 200 patients with implanted medical devices and 350 physicians—technological innovation in the health sector has done more to improve quality of life than in any other sector tested. More specifically, 81% of patients and 66% of physicians responded that innovation in the healthcare space has "improved the quality of my life."

Although connectivity offers tremendous benefits, it also increases cybersecurity risk exposure. Hollywood's version of this risk played out in a 2012 episode of Showtime's Homeland, when terrorists hacked the vice president's Internet-connected pacemaker to accelerate his heartbeat and induce a fatal heart attack. Critics speculate that the plot idea emerged after former Vice President Dick Cheney, citing concerns over hacking, disabled his implanted defibrillator's wireless reprogramming capabilities. Cheney's concerns were not entirely unfounded—indeed, security researchers have discovered vulnerabilities across the implanted medical device ecosystem and identified key challenges associated with patching systems, device updates, and data privacy[4]. At present, however, risks associated with exploitation of connected medical devices remain largely hypothetical—confined thus far to experiments and dramatizations.

Although isolated studies[5] have demonstrated theoretical success of hacking, the current probability of exploiting connected medical devices to conduct a successful cyberattack on a large scale is likely low. Such an attack would not only require deep technical knowledge and close proximity between attacker and victim, but would also rely on a chain of actions to bypass multiple security controls—no vulnerability generally offers a single point of failure[6]. Despite these hurdles, cybersecurity threats cannot be eliminated completely, and given the critical life-dependent nature of many of these devices, the amount of risk the healthcare community chooses to accept must be thoughtfully considered throughout the product lifecycle.

Currently, 74% of patients and 68% of physicians consider the health benefits of connected medical devices to outweigh their associated risks. To preserve such high levels of trust in the value of connected devices and encourage further industry innovation, the medical device community must be prepared to address concerns over technological dependencies—including such critical matters as the potential for data exposure or device compromise. Patients and physicians broadly agree that strengthening the cybersecurity of connected medical devices is an industry-wide responsibility, to be tackled through close collaboration between industry and government rather than through discrete efforts by individual companies[7]. In the United States, an industry-wide approach to maintaining trust in the efficacy and security of healthcare products and services requires the support of the Food and Drug Administration (FDA), device manufacturers, security researchers, and healthcare providers.

Majority see the benefits of connectivity outweighing any potential risks



Source: Brunswick Insight survey

This white paper evaluates the risk-benefit tradeoff of connected medical device use and calls on the medical device industry to come together to proactively develop mitigation measures designed to identify and reduce potential vulnerabilities in the device architectures underlying today's digital health ecosystem. While both patients and physicians consider the health and cost savings benefits of connected devices to outweigh their potential cybersecurity risks, as noted above, both groups also recognize the importance of developing standards and enhancing industry-wide collaboration and information sharing to anticipate and address emerging cyber challenges.

Benefits of Connected Devices

Despite the potential risks associated with medical devices, patients and physicians uniformly recognize the value of innovation in the healthcare industry, both for its effects on individual quality of life and for its enhancement of society writ-large. Innovation within the industry has already proven to advance the treatment of heart failure, improve accuracy and administration of insulin for diabetes patients, and enable remote monitoring to consistently track vital patient information.

In fact, a 2015 review[8] of the effects of remote monitoring on patients with cardiac implantable electronic devices (CIEDs) found consistent results across several large, randomized trials using different proprietary remote monitoring technologies: a reduction in health care visits, earlier detection of actionable events, and streamlined communication between patients and physicians. In one trial, remote monitoring reduced the number of scheduled and unscheduled hospital evaluations by almost 50% with no accompanying increase in death or related complications[9]. In another, remote monitoring reduced the incidence of inappropriate administration of cardiac shocks by over 50%[10]. Across studies, remote monitoring alerted physicians to changes in device function, human programming errors, early battery depletion, and unexpected failures, allowing patients to derive meaningful health and communications benefits from medical device connectivity.

Beyond these direct health benefits, implantable devices and remote monitoring solutions have also generated significant patient and hospital cost savings. At the 2015 Heart Rhythm Society Annual Scientific Sessions, researchers presented their analysis of the connection between remote monitoring and healthcare costs. Researchers evaluated 92,566 patients implanted with pacemakers,

Beyond these direct health benefits, implantable devices and remote monitoring solutions have also generated significant patient and hospital cost savings.

implantable cardioverter defibrillators, or cardiac resynchronization therapy devices and found that remote monitoring was associated with lower hospitalization costs per patient per year, shorter mean length of hospital stay (5.3 days versus 8.1 days), and fewer hospitalization events per patient per year[11]. Hospital costs, as well, were 30% lower among remote monitoring patients.

By wide margins, these findings fall in line with patients' and physicians' views on the value of connected medical devices. On-demand access to health data, real-time monitoring, early issue detection, agile treatment changes, cost savings, and reduced response time were among the benefits of healthcare innovation that 71% of patients cited as contributing to their feeling "more optimistic for the future.[12]" These benefits, coupled with the daily conveniences connected devices create, contribute to industry analysts' projection that use of connected devices or remote patient monitoring will grow at an annual rate of 47.9% and reach 50.2 million deployments by 2021[13].

It comes as no surprise that patients and physicians assess the overall benefits of connected medical devices to outweigh their potential cybersecurity risks. Maintaining strong device cybersecurity and mobilizing the healthcare industry to innovate as the cyber threat landscape continues to evolve are key drivers of maintaining this risk-benefit calculus.

Maintaining strong device cybersecurity and mobilizing the healthcare industry to innovate as the cyber threat landscape continues to evolve are key drivers of maintaining this risk-benefit calculus.

Connected Devices and Cyber Risk

Medical devices once operated independently of wireless networks and interacted only with patients and their healthcare providers. Today, connectivity underpins many of the technological advancements that have enhanced the life-saving capacity of medical devices. Features like wireless connectivity, remote monitoring, and near-field communication enable physicians to calibrate, adjust, and fine-tune implanted devices often without the need for invasive procedures. But these advancements can also serve as points of exposure in the Internet of Medical Things (IoMT)—the system of devices and networks that connect to support modern healthcare delivery.

Every networked system—from the retail sector to the financial services industry to governments—are subject to cyberattacks, so it is logical that the evolution of the IoMT has created opportunities for attackers to exploit connectivity in the healthcare sector.

The May 2017 "WannaCry" global ransomware cyber-attack offers a case study into the risks associated with increased healthcare connectivity. When a fast-spreading Internet worm infected vulnerable Windows machines across the globe, operations stalled at crippled utilities, businesses, and government agencies until a $300 BitCoin ransom payment resulted in the safe return of locked files[14]. The attack hit Britain's National Health Service (NHS) particularly hard—paralyzing its computer systems and putting patients' lives at risk across the country. More than 40 British healthcare trusts reported outages, leaving physicians without wireless access to patient data or the ability to communicate with and remotely monitor at-home patients—which 93% of patients and 95% of physicians consider an essential feature of medical devices[15]. Absent connectivity, doctors lacked insight into their patients' device performance. Hospitals had to deploy more resources to deliver lower-quality, more error-prone care.

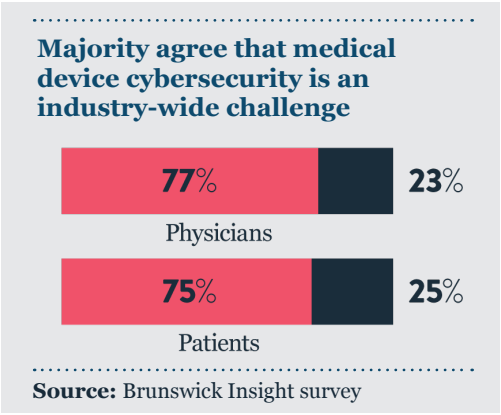
While the WannaCry breach was focused on the systems that connect providers to the information they need to do their jobs, it is a harbinger of the potential risks for connected medical devices.

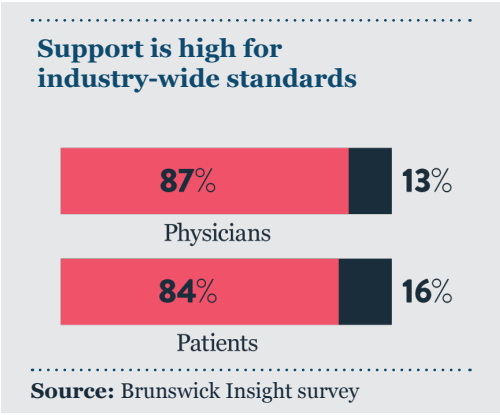
As the IoMT has grown[16], its associated potential cyber risks have expanded to include improper device configuration and potential malicious penetration. This growing risk surface requires medical device manufacturers to develop, embed, and update protections designed to ensure that product benefits continue to outweigh potential risks.

This growing risk surface requires medical device manufacturers to develop, embed, and update protections designed to ensure that product benefits continue to outweigh potential risks.

What Should Be Done?

Patients and physicians understand that cybersecurity risk management is an industry-wide responsibility, not a challenge to be handled as-needed by individual companies. A company-by-company approach to medical device cybersecurity could not only result in devices that have been developed based on widely differing risk tolerance levels, but could also inhibit the type of information sharing and collective risk identification and mitigation seen in other critical sectors, including the financial services and electric power industries. As a result, 84% of patients and 87% of physicians expressed support for an industry-wide approach to risk management based on shared standards. The similarity inherent in the design of many medical device ecosystems lends itself to this type of holistic, standards-based approach to cybersecurity.





In an exhaustive security evaluation of the implantable cardiac device ecosystem, which includes pacemakers, Implantable Cardioverter Defibrillators (ICD), Pulse Generators, and Cardiac Rhythm Management (CRM) tools, Billy Rios, founder of security firm WhiteScope, finds surprising similarities in the architecture and technical implementation of pacemaker systems across manufacturers. Specifically, Rios finds that several major pacemaker system vendors employ a similar architectural framework, including communication protocols, embedded device hardware, and device authentication mechanisms[17]. Given the fundamental similarities between systems, Rios recommends that manufacturers work together to share innovative cybersecurity designs and compete on user experience and health benefits rather than cybersecurity. In other words, cybersecurity should not function as a competitive differentiator, but as a uniform device enabler.

Of the 18 security issue areas Rios evaluates—among them RF activation, remote firmware updates, and encryption—he finds that most, if not all, security issues permeate the connected device ecosystem across vendors.

Of the 18 security issue areas Rios evaluates—among them radio frequency activation, remote firmware updates, and encryption—he finds that most, if not all, security issues permeate the connected device ecosystem across manufacturers. Rios notes that "as a whole, the implantable cardiac device ecosystem inherits security features associated with the underlying system-of-systems architecture." He adds that unless adequate security controls are implemented, weaknesses in technical architecture "have the potential to compromise the ecosystem's confidentiality, integrity, and/or availability—resulting in potentially negative consequences to patient care if those weaknesses are exploited." This highlights the need for an industry-wide approach to device security, as security efforts undertaken by individual companies—while potentially effective in isolation—may not be sufficient to address vulnerabilities stemming from device interdependencies.

As the main regulatory body responsible for the healthcare industry, the FDA began evaluating medical device connectivity issues in 2013 and ultimately established cybersecurity as a requirement for product approval. Although the FDA offers pre- and postmarket guidance on managing cybersecurity in medical devices, its stipulations have been derided as offering industry little more than a "tap on the shoulder" reminder. James Scott, a senior fellow at the non-partisan Institute for Critical Infrastructure Technology, notes that, "It's really up to the industry to actually do something[18]."

In May 2017, the FDA hosted a workshop to examine opportunities to "do something," with the goal of engaging with new and ongoing research, catalyzing collaboration among stakeholders, and identifying challenges to strengthening medical device cybersecurity. Those in attendance—including federal agencies, academia, medical device manufacturers, and other organizations—agreed that a thorough cybersecurity management policy is critical for healthcare organizations and medical device manufacturers. But what would such an industry effort look like? Recent experience in other industries, scholarship, and industry discussions point to information sharing networks and standards development as smart starting points.

What Does This Look Like?

Information Sharing

The FDA offers voluntary guidance on effective cybersecurity measures to assure medical device functionality and safety in an age of increasing interconnectedness. Like Rios, the FDA recommends information sharing forums—opportunities for manufacturers to join in sharing details about security risks and responses as they occur[19]. The National Health Information Sharing and Analysis Center (NH-ISAC) lays the foundation for the type of trusted community the FDA recommends—offering device manufacturers a forum for sharing cyber and physical security threat indicators—but the forum is less mature than other industry ISACs owing to the relative newness of the cyber threat to the healthcare industry[20]. This effort is particularly challenging for the healthcare sector as many industry providers are small or medium sized businesses with little to no cybersecurity expertise or ability to process significant amounts of information. According to the Healthcare Industry Cybersecurity Task Force's Report on Improving Cybersecurity in the Healthcare Industry, "there is no single entity within the health care industry that is currently resourced to provide a comprehensive information sharing solution to the entire industry[21]." Despite these challenges, more companies, particularly medical device manufacturers, should participate in, contribute to, and engage with the forum as a trusted community to foster the level of trust present in other industries. If, as Rios suggests, manufacturers were to level the cybersecurity playing field and compete on device performance, the NH-ISAC could foster a deeper level of industry engagement than has historically been possible.

More robust industry participation in the NH-ISAC could facilitate another important recommendation that emerged during the May 2017 FDA workshop: the creation of a Cyber Emergency Response Team (CERT) for the healthcare industry. Other industries leverage CERTs as specialized security operations centers that act on threat intelligence correlated by ISACs. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), for example, works to reduce risks within and across critical infrastructure sectors through partnerships with law enforcement agencies, intelligence agencies, and control systems owners, operators, and vendors. Whereas ISACs feed information to members, CERTs serve as emergency response elements that monitor and respond to suspicious activity to further strengthen an industry's cybersecurity risk posture.

While healthcare cybersecurity efforts are nascent, other industries, such as the electric power industry and financial services, have dealt with this threat longer and matured accordingly, providing promising models for fostering industry-wide and industry-government collaboration that the medical device industry can follow.

Information Sharing Case Study: The Electric Power Industry

The CEO-led Electricity Subsector Coordinating Council (ESCC) serves as the principal liaison between the federal government and the electric power sector, with the mission of coordinating efforts to prepare for and respond to national-level disasters and threats to critical infrastructure. The ESCC works across the electric power industry, with the government, and with other interdependent critical infrastructure sectors to deploy the latest tools and technologies to improve situational awareness and enable machine-to-machine information sharing. The National Infrastructure Advisory Council called the ESCC is a model for how critical infrastructure sectors can more effectively partner with government.

To support the mission of the ESCC, a Security Executive Working Group convenes monthly to accomplish the goals identified by the Council's leadership. In parallel, the government organizes around these goals with a commitment to aligning its efforts with industry's strategic priorities. Whereas the Electricity Information Sharing and Analysis Center (E-ISAC) serves as the industry's primary security communications and alerts channel, the ESCC offers a forum for industry leadership to collaborate with government on outlining roles and responsibilities, identifying R&D priorities, allocating resources efficiently, and ultimately spurring momentum.

Notably, the ESCC has assisted in developing a cyber mutual assistance program to aid electric companies in restoring necessary computer systems in the event of a regional or national cyber incident; developed a Transformer Transportation Emergency Support Guide to expedite the deployment of large spare equipment; and assisted in the execution of four national-level incident response exercises since 2015.

Information Sharing Case Study: The Financial Services Industry

The Financial Services Information Sharing and Analysis Center (FS-ISAC) offers a well-established model of successful industry-wide and industry-government information sharing. The FS-ISAC, which liaises with the Department of Homeland Security, Department of the Treasury, and U.S. Secret Service, provides an anonymous information sharing capability across the financial services industry. Upon receiving a submission, industry experts verify and analyze the reported threat and identify any recommended solutions before alerting FS-ISAC members. This procedure assures that member firms receive the most current threat information and best practices for guarding against known and emerging security threats.

Standards

Rios' discovery of common vulnerabilities across the medical device ecosystem speaks to the need for fair and enforceable industry cybersecurity standards. The electric power sector again offers a successful model for industry-government collaboration in this area.

Standards Development Case Study: The Electric Power Industry

In the electric power industry, responsibility for standards development rests with private companies as owners, operators, and experts in their field. The Energy Policy Act of 2005 empowered the Federal Energy Regulatory Commission (FERC) to oversee the reliability of the bulk power system, including the authority to approve mandatory cybersecurity reliability standards. The North American Electric Reliability Corporation (NERC), a not-for-profit international regulatory authority which FERC has certified as the nation's Electric Reliability Organization, develops and enforces standards to assure the reliability and security of the bulk power system. Through NERC, industry participants drive the standard creation process by leveraging a results-based approach focused on measurable performance, effective risk management strategy, and organizational capabilities. The process is open to anyone in industry, provides opportunity for comment and is done in a way that is timely and transparent to the public with the overall goal of ensuring our critical electric power operations remain reliable. While NERC drives standards development, FERC identifies the need for standards creation and directs NERC accordingly. The industry-government collaboration builds private sector representation and consensus into standards development.

There is significant opportunity for the medical device industry to come together and lead on the standards necessary to strengthen device security. Rios offers a sample set of questions in his report to aid vendors in evaluating the comprehensiveness of their security controls. The questions—some of which are included below—should be thought of as a starting point for medical device industry-driven security standards:

There is significant opportunity for the medical device industry to come together and lead on the standards necessary to strengthen device security.

Encryption and Data Storage:

- Is firmware on the home monitoring device packed, obfuscated, and/or encrypted?
- Are patient data stored unencrypted to the physician programmer?
- Are hardcoded infrastructure data present on the home monitoring device or physician programmer? How are the data stored?

Authentication:

- Are hardcoded credentials present on the home monitoring device or physician programmer? How are credentials stored? Are credentials universal in all devices?
- Is there a universal token that can be used to pair any home monitoring device with an implanted device? If deemed necessary to support patient care, what other security controls protect against an attacker initiating a spoofed session using a universal token?

Software Updates and Patch Management:

- Do the home monitoring devices implement a remote firmware update process? What security controls are used to authenticate the source of the firmware update to the home monitoring device?
- What process is used to ensure that a security update applied to a physician programmer for an implantable cardiac device application is verified and applied to all other implantable cardiac device applications on the physical programmer?

By using a common language—adhering to a common set of questions based on identified security vulnerabilities—manufacturers can ensure and convey to patients that security is appropriately integrated into the device design process, and that security has been thoughtfully considered during product development so that security measures can be updated as new potential vulnerabilities come to light in the future.

As new vulnerabilities emerge, however, industry must also have a standard process for evaluating whether newly-identified vulnerabilities present acceptable or unacceptable risks[22].

As security standards are put in place, they should include an ongoing assessment of threats and industry-accepted mechanisms for evaluating cyber risks against clinical benefits and uses. If industry agrees that existing vulnerability assessment tools like the Common Vulnerability Scoring System (CVSS) do not adequately account for factors unique to the clinical environment in which medical devices are used, industry should assist in the development of industry-specific standards for evaluating potential vulnerabilities.

Conclusion

No one company can claim to be hack-proof, but successful and responsible companies assess, mitigate, and constantly monitor the ever-present threats to critical assets. Device manufacturers, healthcare service providers, patients, and physicians share responsibility for creating a resilient healthcare network that embraces the benefits of innovation while mitigating its associated risks.

No one company can claim to be hack-proof, but successful and responsible companies assess, mitigate, and constantly monitor the ever-present threats to critical assets.

Medical device manufacturers, like the electric power sector, should take the opportunity to drive the development of standards now, before others take the lead. Device manufacturers know the critical operations of their devices better than anyone else. With increased information sharing, constant monitoring, and an informed understanding of the threats they face, device manufacturers can assess potential vulnerabilities and identify risk mitigation activities that will ultimately strengthen security while avoiding adverse consequences to patient care and future innovation.

Now is the time for the healthcare industry to come together as never before to implement trusted cybersecurity measures that will give physicians and patients the tools they need to make informed decisions about health management, and ultimately help maintain the trust and security that make these technology transformations successful.

References

1 https://www.theguardian.com/artanddesign/2014/may/06/neil-harbisson-worlds-first-cyborg-artist

2 Duke University Medical Center associate professor Jonathan Piccini found a 30% reduction in hospital costs and a lower mortality rate (4023 vs. 4679 per 100,000 patient-years) for patients with remote monitoring. Study available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4923102/

3 Piccini also found that patients with implanted devices and remote monitoring experienced fewer and shorter hospitalizations (5.3 days vs. 8.1 days): http://www.healio.com/cardiology/arrhythmia-disorders/news/online/%7B8ba0c947-dc16-428d-9308-6982d4287d75%7D/remote-monitoring-of-cardiac-devices-reduces-hospitalizations-costs

4 Michael Mimoso reviews research by Billy Rios and Jonathan Butts in his article, "Pacemaker Ecosystem Fails its Cybersecurity Checkup," available at: https://threatpost.com/pacemaker-ecosystem-fails-its-cybersecurity-checkup/125942/

5 Jay Radcliffe, a diabetic who experimented on his own equipment, found exploitable vulnerabilities in his remote-controlled insulin pump. See story here: http://usatoday30.usatoday.com/news/health/medical/health/medical/diabetes/story/2011/08/Insulin-pumps-medical-devices-vulnerable-to-hacking/49805796/1

6 WhiteScope's 2017 Security Evaluation of the Implantable Cardiac Device Ecosystem

7 Brunswick Insight found that three in four physicians (77%) and patients (75%) believe that cybersecurity risks posed by connected medical devices are an industry-wide issue, rather than an issue that is unique to certain companies in the healthcare space.

8 2015 HRS Expert Consensus Statement on Remote Interrogation and Monitoring for Cardiovascular Implantable Electronic Devices

9 The Lumos-T Reduces Routine Office Device Follow-Up Study (TRUST)—a study of 1000 ICD patients—found that home monitoring can safely reduce the number of scheduled nonactionable office device interrogations by 50% and provide early detection and notification of cardiac and/or device problems. Clinical trial information available at: https://www.ncbi.nlm.nih.gov/pubmed/20625110?dopt=Abstract

10 Potential Role of Home Monitoring to Reduce Inappropriate Shocks in Implantable Cardioverter-Defibrillator Patients due to Lead Failure study finds a 50% reduction in inappropriate administration of cardiac shocks among patients with remote monitoring. Abstract available at: https://www.scopus.com/record/display.uri?eid=2-s2.0-65249116913&origin=inward&txGid=F8C5192FF7C1FDFB3F4141564332768F.wsnAw8kcdt7IPYLO0V48gA%3a2

11 See a write-up of Duke University Medical Center associate professor Jonathan Piccini's presentation to the Heart Rhythm Society here: http://www.healio.com/cardiology/arrhythmia-disorders/news/online/%7B8ba0c947-dc16-428d-9308-6982d4287d75%7D/remote-monitoring-of-cardiac-devices-reduces-hospitalizations-costs

12 Brunswick Insight survey results

13 http://mhealthintelligence.com/news/7.1m-patients-use-remote-monitoring-connected-medical-devices

14 http://www.thedailybeast.com/articles/2017/05/12/stolen-nsa-tech-shuts-down-hospitals

15 Brunswick Insight survey results

[16] Market Research Firm Grandview Research assesses that the increasing prevalence of chronic diseases is boosting demand for connected medical devices. The firm estimates that the IoMT sector will grow to $410B by 2022. See report at http://www.grandviewresearch.com/press-release/global-iot-in-healthcare-market

[17] Full report available at: https://drive.google.com/file/d/0B_GspGER4QQTYkJfaVl-BeGVCSW8/view

[18] Scott discussed the medical device cybersecurity landscape with Wired in March 2017. See full article at: https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[19] See the FDA's Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff at: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

[20] Denise Anderson, Executive Director of the NH-ISAC, discusses the immaturity of healthcare cybersecurity efforts relative to other industries, explaining that the healthcare industry has only recently become a target of cyber-criminals. Article available at: http://www.healthcareit-news.com/news/how-sharing-security-intelligence-stops-healthcare-hackers-privacy

[21] Report available at: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[22] Recommendation made in the FDA's postmarket guidance, available at: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM482022.pdf

Brunswick Insight Survey Methodology

Brunswick Insight conducted a national online survey from April 7-14th of 200 patients with implanted medical devices and 350 physicians in the U.S.

01010111 01001000 01011001 00100000 01001101 01000101
01000100 01000101 01010110 01001001 01000011 01000101
01000110 01000001 01000011 01010100 01010101 01010010
01010011 01010100 00100000 01001100 01000101 01000001
01011001 01000010 01000101 01010010 01010011 01000101
00100000 01001001 01001110 00100000 01000001 01001110
01000101 01000001 01010011 01001001 01001110 01000111
01001110 01000101 01000011 01010100 01000101 01000100
01001000 01000011 01000001 01010010 01000101 00100000