Building A More Secure Connected Healthcare Environment

ABOUT THE CHERTOFF GROUP

The Chertoff Group is a premier global advisory firm focused on security and risk management. We apply our security expertise, technology insights and policy intelligence to help clients build resilient organizations, gain competitive advantage and accelerate growth. The Chertoff Group helps clients understand the effects of changes in security risk, technology and policy to inform business strategy. Our trusted approach, proven methodology and deep understanding for security effectiveness enables clients to reduce cyber and physical risk, protect critical assets and position their enterprise for growth.

For more information, visit **www.chertoffgroup.com**

ABOUT ABBOTT

Abbott is committed to helping people live their best possible life through the power of health. For more than 125 years, Abbott has brought new products and technologies to the world – in nutrition, diagnostics, medical devices and medicines – that create more possibilities for more people at all stages of life. Today, 99,000 of us are working to help people live not just longer, but better, in the more than 150 countries we serve.

As healthcare becomes increasingly interconnected and data-driven, connected medical devices provide patients and physicians with information to better manage their health, which improves outcomes and reduces the overall cost of care. No matter how technologically-advanced we become, people 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 the people who use our products 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.**

Introduction

The healthcare sector is in the midst of a major transformation, including changing demographics, an evolving public policy environment and rapidly advancing technology. A core element of this technology change is the advent of connected healthcare, which is empowering physicians to deliver superior results and extend patient lives.

We now have a wirelessly connected hospital ecosystem that allows for the seamless integration of medical devices and data through Electronic Health Records (EHRs), remote monitoring technology, implantable and wearable devices, diagnostic and imaging tools, among many other examples. Medical professionals are leveraging these new technologies and devices to transform the way they interact with patients, provide care and improve patients' quality of life. Studies have shown that connected healthcare yields significant improvements in patient outcomes, including substantial reductions in hospitalization, mortality rates and medical costs.[i]

Of course, as with any other internet-enabled technology, enhancing connectivity for medical devices also means increased cybersecurity risk. The same powerful technology that multiplies the value of medical devices and data can also jeopardize connected healthcare's integrity and availability if not managed and understood effectively by all stakeholders within the connected environment. This paper explores new research on the perceptions and awareness of medical device cybersecurity by various healthcare delivery stakeholders, and the ways all members of the healthcare ecosystem can work together to mitigate cybersecurity risk while preserving the benefits of connected medical devices for the patient.

IMPACT OF CONNECTED MEDICAL DEVICES

The benefits of connected medical devices on patient outcomes is profound. Using these devices, physicians gain access to more data and better correlation capabilities to glean more powerful insights and draw more precise conclusions. Prevention and diagnosis of disease is especially affected. The richness of the data delivered by connected devices improves clinical decision-making, transforming physician diagnostic capabilities further towards the predictive.[ii] Key benefits include:

- **Timeliness.** Connected medical devices supply physicians and medical providers with immediate, actionable data that can help inform medical decisions and determine proper treatment.
- **Accuracy.** Automatic transmittal of data eliminates user errors that can accompany manual recording of medical device information.
- **Patient convenience and ownership.** Remote monitoring of chronic diseases enables patients to avoid trips to doctors' offices and hospital stays, while also enhancing medication adherence (e.g., through patient alerting and related capabilities) and patient engagement.
- **Access.** Geographic or logistical challenges that previously prohibited potential patients from receiving care no longer impede treatment. Smaller, lighter, more portable devices make healthcare accessible to those in underserved communities, rural areas and developing countries – to patients who need it most.
- **Cost.** National health spending in the United States is projected to grow at an average rate of 5.5 percent per year for 2017-26 and to reach $5.7 trillion by 2026.[iii] Connected devices can help mitigate rising costs through efficiencies in data collection and treatment monitoring.

> "The richness of the data delivered by connected devices improves clinical decision-making, transforming physician diagnostic capabilities further towards the predictive."

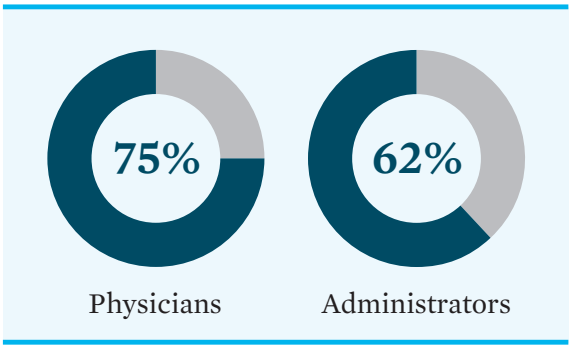
CYBERSECURITY AND THE CONNECTED HOSPITAL

As described earlier, enhancing connectivity in any environment introduces greater cybersecurity risk. U.S. hospitals, on average, have 10 to 15 connected devices per bed. A large hospital, which can have 5,000 beds or more, may manage 50,000 devices.[iv] These devices operate in an "always on" environment, often with few physical access controls due to constantly changing settings and workflow requirements where easy access to life-saving technology is the paramount concern. The burden to train patients and to maintain updated and functioning devices rests on time-constrained hospital staff.

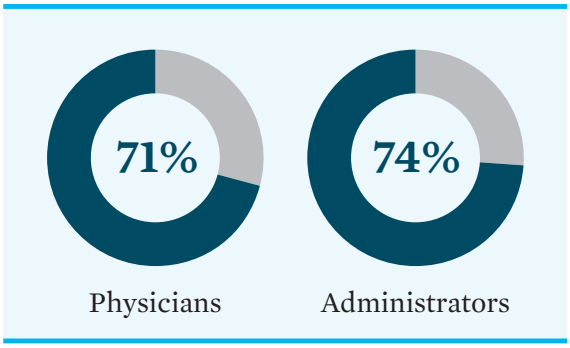
A first step to addressing cybersecurity risk in today's connected hospital is to understand the perceptions of key stakeholders within that ecosystem. In 2018, Brunswick Insight partnered with global health technology company Abbott to conduct a national survey of 400 physicians, information security executives and hospital administrators across a range of hospital types and sizes to better understand how these healthcare delivery stakeholders think about medical device-related security, identify gaps in awareness and understanding and determine effective solutions. Key findings of the survey include:

- **Physicians and hospital administrators emphasize cybersecurity importance in the connected healthcare environment.** Physicians and hospital administrators see cybersecurity as a priority – one that is directly tied to patient outcomes and areas of concern including: (1) disruption of hospital operations and healthcare delivery; (2) incorrect or uninformed therapy decisions; (3) compromised patient safety; (4) loss of patient data; and (5) compromised patient privacy.
- **While they agree on importance of cybersecurity, physicians and administrators view cybersecurity through slightly different perspectives.** Physicians tend to be more focused on patient decisions, where hospital administrators are most concerned with compliance. Administrators also are twice as likely to say they are familiar with potential cybersecurity risks associated with connected implanted medical devices than physicians.

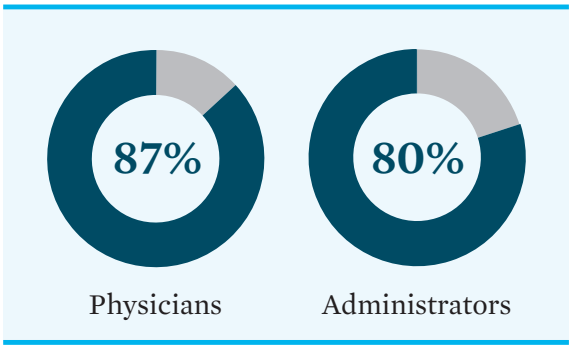
Physicians and administrators feel underprepared on cybersecurity



Physicians and hospital administrators view medical device cybersecurity as a shared responsibility



Benefits of connected medical technology outweigh the risks



- **Physicians and administrators feel underprepared on cybersecurity.** According to the survey, 75 percent of physicians and 62 percent of hospital administrators feel inadequately trained or prepared to combat cybersecurity risks. Second only to having appropriate levels of cybersecurity staffing, physicians and administrators see user training and awareness as a substantial challenge.
- **Physicians and administrators view medical device cybersecurity as a shared responsibility.** For several years, the U.S. Food and Drug Administration (FDA) has emphasized that medical device security is a shared responsibility between manufacturers, healthcare delivery organizations (HDOs), clinicians and regulators. Seventy-one percent of physicians and 74 percent of hospital administrators view cybersecurity as a shared responsibility among stakeholders operating in the healthcare ecosystem.
- **Communication about medical device cyber-related vulnerabilities needs to improve.** Only 15 percent of physicians and 45 percent of administrators have seen or read any advisories relating to medical device security in the last six months. For those who are familiar with advisories, both physicians (52 percent) and administrators (64 percent) say advisories help them feel more comfortable responding to cybersecurity risks.
- **Everyone agrees on the importance of standards.** While administrators are more likely than physicians to understand practicalities of how to leverage the procurement process to drive cybersecurity outcomes, both agree on the importance of baseline industry-wide medical device cybersecurity standards. Eighty-two percent of physicians and 73 percent of administrators believe there should be an industry-wide set of standards and language that gives physicians and their patients confidence in the safety of connected devices.

While acknowledging the potential risks that can occur as a result of connected medical technologies, the benefits of connected medical devices on patient outcomes remain paramount. Regardless of the type of machine or device, there is overwhelming support for connected medical technology with 87 percent of surveyed physicians and 80 percent of surveyed hospital administrators agreeing that the benefits of connected medical technology outweigh the risks.

ACTIONS UNDER WAY TO CLOSE THESE CYBERSECURITY GAPS

The U.S. FDA, other federal agencies and organizations such as the MITRE Corporation are actively advancing efforts to address some of these concerns.

- **Premarket and postmarket cybersecurity guidance.** The FDA has issued postmarket guidance – and recently issued updated draft guidance on *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* – to help manufacturers identify and address cybersecurity risks in the design, labeling, documentation and postmarket management of medical devices.[v]
- **Response best practices.** The FDA recently partnered with MITRE to release a *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook* to educate stakeholders on processes to remediate and recover from cyber incidents.[vi] The *Playbook* provides a framework to help healthcare delivery organizations develop capabilities to prepare and respond to medical device cyber events, specifically focusing on issues that impact the functionality of a device.
- **Software transparency.** A detailed accounting of open source and commercial components, modules and libraries built into medical device firmware and software can help provide greater transparency into known and future vulnerabilities and thereby improve security. The National Telecommunications and Information Administration (NTIA) within the U.S. Department of Commerce has convened a multi-stakeholder working group to help improve software component transparency, including through a "software bill of materials."[vii] The initiative includes a Healthcare Proof of Concept in which several volunteers (including Abbott) are working to explore how Software Bill of Materials (SBOM) data can be generated, shared and used to reduce cybersecurity risk.

This work builds on several other efforts, including the 2017 Health Care Industry Cybersecurity Task Force mandated by the Cybersecurity Act of 2015, related work of the Healthcare and Public Health Government Coordinating Council, the formation of medical device-focused Information Sharing and Analysis Organizations and additional initiatives in Congress to advance progress in managing connected device cybersecurity risk.

WHERE IS MORE WORK NEEDED?

Managing these risks requires active engagement across the healthcare community. Engagement depends on informed awareness on the part of key stakeholders who coalesce to create a connected healthcare ecosystem in which devices, networks, data and healthcare delivery all intersect.

> "Industry should not compete on cybersecurity, but instead provide assurance to patients that any device meets the same high standard."

FDA Commissioner Scott Gottlieb recently acknowledged the need for public-private collaboration to address this issue, stating: "Securing medical devices from cybersecurity threats cannot be achieved by one government agency alone. Every stakeholder – manufacturers, hospitals, health care providers, cybersecurity researchers and government entities – all have a unique role to play in addressing these modern challenges."[viii]

Industry should not compete on cybersecurity, but should provide assurance to patients that any device meets the same high standard. A healthcare community-wide approach with leadership from industry, regulators and HDOs can help drive progress to give patients and physicians confidence in the cybersecurity of medical devices. Key areas to address include:

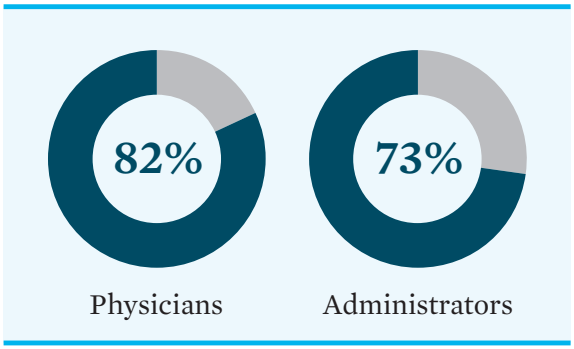
Standards and Cybersecurity by Design

To minimize the potential impact of cybersecurity vulnerabilities and ensure that devices can appropriately respond when vulnerabilities are discovered, security must be incorporated into the earliest phases of medical device design. Securing connected devices requires a combination of protective and responsive controls. Many security risk management approaches are complex, becoming highly technical very quickly. It is not reasonable to expect that physicians and patients will be able to evaluate the adequacy of cybersecurity in connected medical devices on their own.

Further, while some HDOs have invested in cybersecurity resources, the U.S. Department of Health and Human Services 2017 Report on Improving Cybersecurity in the Health Care

> “Security must be incorporated into the earliest phases of medical device design.”

Everyone agrees on the importance of standards



> “Manufacturers, HDOs and regulators must come together to establish standards for when and how medical device cybersecurity updates will be performed in order to balance cybersecurity risks with essential clinical and patient-care considerations.”

Industry found that most HDOs lack the infrastructure and financial resources to effectively apply cybersecurity protections to their networks and data.[ix] The Brunswick Insight/Abbott survey also shows that three-quarters of physicians feel underprepared and under-trained to deal with cybersecurity threats. However, all surveyed groups agreed that they want an industry-wide set of security standards to include consistent language and meaningful guidelines that will help provide assurance in the safety of connected medical devices for both physicians and patients.

The FDA’s draft premarket guidance represents an important step in this direction. To make this guidance more effective; however, industry and HDOs must engage in the process and ensure such guidance is implementable as a practical matter. There are several key areas that will require engagement from stakeholders across the healthcare ecosystem to ensure that these critical cybersecurity protections can be effectively implemented. These include:

- **Authentication.** Many cyber incidents involve a compromise of credentials and risk-based authentication provides a critical layer of security. However, authentication solutions can also introduce another layer of friction, both in acute environments as well as more generally with users unfamiliar with the technology. The healthcare community must collectively think through the clinical work flow issues such as: What does this look like in a clinical environment? How do we enable secure authentication in critical emergency situations? Authentication must be implemented in an effective manner that mitigates risk without jeopardizing timely delivery of healthcare services. This tension cannot be an excuse for business-as-usual on authentication, but creative solutions will require collaboration between industry, regulators and other stakeholders.
- **Cybersecurity updates.** The topic of when and how to perform cybersecurity updates of medical devices is one that has received significant attention in recent years. This well-deserved attention is in part due to the cybersecurity risks introduced by unpatched and outdated devices, but also because of the complexity involved with performing these updates in the clinical environment. Medical device manufacturers have built products that have been able to

perform clinically over long periods of time. With implanted devices, longevity is a critical requirement that minimizes other patient health risks, such as those caused by having to go through multiple procedures, in addition to reducing healthcare costs. Manufacturers, HDOs and regulators must come together to establish standards for when and how medical device cybersecurity updates will be performed to balance cybersecurity risks with essential clinical and patient-care considerations. A key component of this discussion needs to be not only when updates will occur but how they will occur. Efficient mechanisms for the distribution and application of updates need to be identified to minimize the burden on resource constrained HDOs that need to update large numbers of devices across a complex clinical environment.

- **Forensic evidence capture.** Mechanisms for capturing security event information to support incident investigation and response have long been used in the enterprise security area. This information is valuable to support investigations and incident response as well as the continuous improvement of security protections. However, the implementation of forensic evidence capture in medical devices is in its infancy. The evolution of technology and connectivity, coupled with evolving cybersecurity threats, has increased the urgency of enhancing such capabilities for medical devices. Doing so will require close coordination between manufacturers, physicians and HDOs with a level of information sharing that does not yet exist in healthcare. The FDA's focus on information sharing and incentives through their postmarket guidance is a good starting point to expand future efforts in this area.

These are just a few of the areas that will require strong industry engagement and collaboration. To ensure the potential value of connected health technology is realized by physicians and patients, the entire industry must come together to develop common standards and practices that will give users confidence in the cyber safety of medical devices.

Cybersecurity Incident Response

Even the best cybersecurity protections cannot guarantee the discovery of every vulnerability and the prevention of every security incident. Cybersecurity professionals know the risks of a cyber-related event and that having a good response capability is necessary. Additional attention and investment are needed to determine appropriate protocols and processes for identifying and responding to vulnerabilities in a timely manner, while supporting safe clinical care. A coordinated effort is required between manufacturers, physicians, HDOs and regulators to ensure appropriate and timely responses to identified vulnerabilities. Efforts may include:

- **Cybersecurity Bill of Materials.** The recently released draft of the updated FDA premarket guidance recommends manufacturers provide a Cybersecurity Bill of Materials (CBOM) to improve transparency and enable more timely vulnerability identification and remediation.[x] Exactly what form this takes should be dictated by a collaborative, industry-wide effort that includes manufacturers, HDOs and regulators. Ultimately, any software bill of materials (whether the CBOM recently proposed by FDA, or an SBOM like those being developed by various other stakeholder groups) must be in a form that allows it to be usable by HDOs to effectively respond to vulnerabilities and appropriately mitigate risk in the clinical environment, and not disclose confidential or proprietary information that could be misused.

> "A coordinated effort is required between manufacturers, physicians, HDOs and regulators to ensure appropriate and timely responses to identified vulnerabilities."

- **Risk evaluation.** Mechanisms for evaluating postmarket cybersecurity vulnerabilities in medical devices are still evolving. Traditional mechanisms for evaluating risk that calculate the chance or likelihood that something will fail do not translate effectively when evaluating cybersecurity vulnerabilities. FDA postmarket guidance provides several options including the Common Vulnerability Scoring System (CVSS). However, there are challenges when applying these models in healthcare environments. MITRE is currently working with industry on a healthcare specific CVSS.[xi] The Association for the Advancement of Medical Instrumentation has developed a draft Technical Information Report on

postmarket risk management for medical devices.[xii] These efforts must come together to produce a consistent and usable mechanism for evaluating cybersecurity risks in medical devices. HDOs and physicians need to participate in these efforts to ensure that information provided by manufacturers is understandable and applicable in a clinical environment.

- **Stakeholder communication.** There are currently several mechanisms for communicating medical device vulnerability information. These include: Department of Homeland Security Computer Emergency Response Team advisories, FDA safety communications and communications directly from the manufacturer. As part of the Brunswick Insight/Abbott survey, respondents were asked whether they had seen or read any advisories related to medical device vulnerabilities in the last six months. As noted above, only 15 percent of physicians and 45 percent of hospital administrators recalled seeing a vulnerability advisory in the last six months. Clearly, more work is needed to ensure that communications about device vulnerabilities reach the right stakeholders, at the right time and with the right information to drive an effective response.

With the multiple and interconnected stakeholders involved in responding to medical device vulnerabilities, it will be essential for all these stakeholders to work together to ensure that information related to vulnerabilities and responsive actions is clear, timely and available.

Education and Awareness

The Brunswick Insight/Abbott survey highlights a common theme across all stakeholders in their desire for more information and training when it comes to managing cybersecurity risk in their environment. When asked to rank the importance of actions medical device manufacturers can take to improve medical device cybersecurity, 62 percent of physicians and 70 percent of hospital administrators report more training for hospital staff and patients as the most important action. This response is seen as substantially more effective than other options such as providing more updates/patches, increasing software transparency and providing third-party certifications.

The connected healthcare ecosystem must engage across all stakeholders to increase awareness and understanding of cyber risks. Currently, most communication on cybersecurity occurs between manufacturers, HDOs and physicians. As patients interact more directly with technologies like wearables and mobile applications, it will become even more critical for patients to understand the cybersecurity risks and how to protect themselves. Just as personal hygiene is a critical aspect of good health, digital hygiene will be critical for patients to ensure their medical technology continues to operate effectively. As healthcare delivery and treatment becomes more patient-centric, the industry needs to offer clear communication and instructions – no matter the manufacturer – to help patients understand the benefits and risks of these devices and the proper cyber hygiene necessary to protect themselves and their data. Education and awareness efforts must stress that every stakeholder has a role to play and must commit to assuming accountability and playing their part.

“The connected healthcare ecosystem must engage across all stakeholders to increase awareness and understanding of cyber risks.”

Conclusion

Connected medical devices hold tremendous promise for greater efficiency and better patient outcomes. The pace of medical advancement will only accelerate as we incorporate the next wave of technologies, including potentially exponential jumps in computing power, the introduction of artificial intelligence and the development of smaller, more precise sensors. Some have forecasted that "we're going to see more medical advances in the next decade than happened in the past century."[xiii] To ensure we can harvest the power of these innovations in the future, we must work to build and maintain a secure foundation for the connected healthcare environment. Stakeholders want to operate in an environment in which implementing the necessary security assurances is intuitive, risk-based and trusted. Just as with healthcare delivery, medical cybersecurity should be focused on the patient.

The healthcare ecosystem must embrace a shared responsibility and imbue a collaborative culture of security. Working together will give all stakeholders – physicians, administrators, patients and manufacturers – the necessary tools, training and confidence to make well-informed risk management decisions resulting in a higher quality of care and an ultimately safer and more secure connected health community for all.

"To ensure we can harvest the power of these innovations in the future, we must work to build and maintain a secure foundation for the connected healthcare environment."

REFERENCES

[i] Slotwiner D, Varma N, Akar JG, et al.: HRS Expert Consensus Statement on Remote Interrogation and Monitoring for Cardiovascular Electronic Implantable Devices. Heart Rhythm 2015; 12:e69–e100

[ii] https://www.aplusaresearch.com/single-post/2018/03/02/Why-digital-devices-are-the-future-of-healthcare

[iii] https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/Downloads/ForecastSummary.pdf

[iv] https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

[v] https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

[vi] Id

[vii] https://www.ntia.doc.gov/SoftwareTransparency

[viii] Statement from FDA Commissioner Scott Gottlieb, M.D. on FDA's efforts to strengthen the agency's medical device cybersecurity program as part of its mission to protect patients, October 1, 2018

[ix] https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[x] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf

[xi] https://www.fda.gov/downloads/MedicalDevices/NewsEvents/WorkshopsConferences/UCM560511.pdf

[xii] http://s3.amazonaws.com/rdcms-aami/files/production/public/FileDownloads/WhitePaper/Postmarket_Risk_Management_120816.pdf

[xiii] http://wadhwa.com/2016/10/25/future-medical-breakthroughs-may-come-from-an-unexpected-industry/


The
Chertoff
Group


Abbott