Medical Devices and Cybersecurity
Mitigating Risks for Device Manufacturers
The integration of advanced information technologies in medical devices has transformed the healthcare industry, resulting in dramatic improvements in the efficiency and effectiveness of healthcare and related services. But this integration has fostered the emergence of a new set of challenges for patients, healthcare providers, and device developers and manufacturers. Today, the healthcare industry is a major target for hackers and cybercriminals, potentially compromising private and confidential healthcare data and placing the safety and health of patients at risk.

The healthcare industry has responded to this threat by investing billions of dollars each year on cybersecurity measures. And regulators have played a key role in helping to ensure the introduction of more secure connected medical device technologies through the implementation of requirements that address potential vulnerabilities. But technological innovation proceeds at a rapid pace, often outstripping the ability of industry or regulators to identify or defend against new risks and vulnerabilities. And, ironically, this increased exposure is occurring at the same time that regulators in some jurisdictions are seeking ways to facilitate the more rapid introduction of new and innovative products to market, efforts that include the partial easing of regulatory requirements for some technologies.

In this context, strengthening the security of connected medical devices against cyberattacks is a responsibility shared by all industry participants, including hospital administrators, healthcare providers, and device developers and manufacturers. For their part, device developers and manufacturers must do more than meet the minimum regulatory requirements in their efforts to protect confidential patient data and to help ensure the safety of patients. Instead, they need to thoroughly evaluate and address the potential cybersecurity risks associated with their products, not just during the product development stage but also throughout the products’ anticipated use lifetime.

This UL white paper discusses the strategies that the healthcare industry can adopt to improve connected medical devices' immunity to cyberthreats. The paper begins with an overview of the cybersecurity risks associated with medical devices, and the actions taken to date by regulators to reduce such risks. The white paper then discusses a number of specific strategies that device developers and manufacturers can adopt to make their products more resilient and to reduce their vulnerability to cyberattacks during actual use. The paper concludes with a summary of UL’s efforts to address the cybersecurity of connected medical devices.
The State of Today’s Medical Devices

In the 21st century, technology is as integral to the healthcare system as physicians and clinicians and is a major contributor to improved treatment outcomes and an overall better quality of life for patients. Advances such as telemedicine technologies are helping to increase the quality and efficiency of treatment options available for underserved and remote populations. And consumer-oriented wellness devices are giving people greater insight into how their behaviors can affect their health while also supporting the adoption of healthier lifestyle habits.

Just as technology developments in general have tracked greater integration with compatible systems and devices, today’s medical devices are increasingly connected. Unlike medical equipment and apparatus of the past, which were used independently of other systems, medical devices now fully leverage wired and wireless communications protocols to seamlessly integrate their operation with other medical devices and with information technology networks. Connected medical devices can facilitate the collection of critical healthcare data, promote treatment portability options and improve ease of use.

Along with connectivity, advances in software development have also played an important role in the evolution of medical devices. Software has long been incorporated into medical devices, but a host of software applications used for medical purposes that work independently of medical devices are now widely available. Examples of software as medical device (SaMD) applications range from smart phone apps that enable a user to view results from a medical device for diagnostic purposes to programs used to develop a medical treatment plan.

At the same time, a new generation of wearable devices are available to track vital signs and other human health data. Many of these wearables are marketed to consumers and can include activity trackers, smart watches and certain types of smart exercise equipment and are typically designed to help monitor and improve a user’s fitness or nutrition or to achieve other lifestyle or wellness goals. But wearables are also being used in a healthcare context to monitor patient vital signs either inside or outside a healthcare facility, providing greater mobility and independence for those patients who require longer term care and monitoring.
Unfortunately, these important advancements in medical device technologies have brought increased risks to patient health and safety. As of this writing (Spring 2018), there have been no reported instances of a hacked medical device resulting in patient injury or death. But there is still plenty of reason for concern.

Here are just a few example incidents:

- In late 2016, a major manufacturer of insulin pumps notified more than 100,000 users of a potential security vulnerability in one of its insulin delivery systems. The vulnerability, which was related to the system’s wireless communications capabilities, could allow an unauthorized third-party to alter a patient’s insulin dosage. Upon learning about the vulnerability, the company quickly contacted users of the device, warning them of the potential dangers and recommending specific steps to address the vulnerability.²

- In another instance, the WannaCry ransomware incident in May 2017 affected an estimated 200,000 Windows-based computer systems in medical facilities around the world. But, according to one report, the hacking also affected at least one brand of Windows-based medical devices, a “power injector,” which is a type of radiological equipment intended to improve imaging quality by delivering a contrast agent to a patient. The affected devices were reportedly restored to operational status within 24 hours, and the device manufacturer later released a software patch to address the device vulnerability.³

- In August 2017, the U.S. Food and Drug Administration (FDA) issued a product recall (specifically, a corrective action) in connection with a cardiac pacemaker implanted in an estimated 465,000 people in the U.S. An assessment of the potential cybersecurity vulnerabilities of the device determined that those vulnerabilities could allow an unauthorized user to modify the pacemaker’s programming commands. Under the terms of the FDA’s recall, the device manufacturer developed a firmware update that required an in-person patient visit with a healthcare provider for remediating the problem without removing the device. The FDA’s recall action in this case was reportedly the first time the agency had issued a device⁴ recall in connection with an identified cybersecurity vulnerability.⁵

These incidents are supported by findings of similar vulnerabilities identified by researchers. For example, a team in the United Kingdom and Belgium evaluated at least 10 different types of connected heart pacemakers/defibrillators and were able to gain the ability to turn off the devices, produce fatal shocks and access patients’ personal health data. This enabled them to not only steal patient information, but to also drain the devices’ batteries and to send messages to the devices altering their operation. While the researchers conducted their interceptions at relatively close range to the affected devices, they acknowledge that more sophisticated intercept equipment could facilitate device interference from hundreds of meters away, rendering the source of the attack more difficult to trace.⁶
Specific Areas of Cyber Vulnerability

With an average of between 10 and 15 connected medical devices per hospital bed in the U.S., the potential risk from cybersecurity vulnerabilities in connected devices should be readily apparent. Yet, many analysts note a continued emphasis by healthcare administrators on threats to the secure storage of patient data, and less awareness about cybersecurity challenges associated with connected medical devices or how to address them.

One of the most obvious vulnerabilities stems from the adaptation of legacy medical devices for use in connected environments. In many cases, these devices were not originally designed to protect against cyberthreats and therefore possess no integrated defense against attacks once they are connected to the Internet or other network. Such devices may also rely on outdated operating systems or other software that is no longer supported, or they may be connected to legacy computers that fall outside the scope of a healthcare institution’s IT policy control.

Other likely areas of vulnerability for connected medical devices are similar to those commonly identified with the use of connected technologies in other industries, such as those found in industrial control systems in manufacturing and production operations. In a study published in 2018, a security solution provider, evaluated potential vulnerabilities in tens of thousands of connected medical devices located in 50 hospitals and clinics throughout the U.S. The study covered a wide range of medical devices, including infusion pumps, imaging systems, ECG machines, patient monitors and dispensing systems.

According to the study’s findings, the majority of security issues associated with connected medical devices are related to a few key areas, as follows:

- **Outdated operating systems or software**—A total of 33 percent of security issues identified in connected medical devices were directly related to outdated operating systems or software. Specific vulnerabilities include failure to update Windows operating system software or using obsolete applications. Other potential issues arise from outdated or unpatched firmware.

- **Lateral movement**—Approximately 12 percent of security issues were associated with their failure to reduce or prevent lateral movement between devices across a given network.

- **Unprotected communications and weak passwords**—An estimated 11 percent of issues were linked to unprotected or insecure communications protocols and/or weak or insufficient user passwords.

- **Network segregation**—Approximately 3 percent of security issues were related to the lack of sufficient segregation of network segments intended for use for different purposes. Poor segregation provides expanded network access for unauthorized users.

- **User practice issues**—Finally, a remarkable 40 percent of security issues identified in the study were related to user practice issues. These include browser usages e.g., visiting risky or questionable websites on the Internet, and the use of applications that have not been thoroughly evaluated for cybersecurity vulnerabilities.

Clearly, the potential consequences of such vulnerabilities and security issues associated with connected medical devices can have a direct impact on the safety and health of patients and healthcare providers. But, even when such exposure does not lead to death or injury, the impact from cybersecurity attacks can compromise the privacy and security of confidential patient information, disrupt essential operations and procedures, and require significant financial investment to rectify. And for all parties involved, healthcare providers and device developers and manufacturers, successful breaches resulting from the failure to address known risks can result in adverse market publicity and loss of brand reputation, as well as potential legal exposure.
An Overview of Regulatory Efforts to Address Cybersecurity of Medical Devices

As with healthcare administrators, many regulators outside of the U.S. have focused most of their efforts on addressing potential threats related to the security of patient information rather than dealing directly with cyberthreats against connected medical devices. For example, the European Union’s (EU’s) General Data Protection Regulation (Regulation (EU) 2016/679, also known as the GDPR), harmonizes data privacy laws across the EU. Specifically, the GDPR imposes rigorous reporting requirements on any entity that collects the personal data of EU citizens, as well as strict notification requirements in instances of a cybersecurity breach that compromises the privacy of personal data.11

At the same time, the EU’s recently implemented Medical Device Regulation (Regulation (EU) 2017/745, or the MDR) and In-Vitro Diagnostic Medical Device Regulation (Regulation (EU) 2017/746, or the IVDR) have strengthened existing safety and post-market surveillance requirements for medical devices but do not expressly address cybersecurity considerations.

In contrast, the U.S. FDA has taken a more proactive approach in addressing cybersecurity issues for medical devices and has published several guidance documents addressing the agency’s pre- and post-market requirements specific to cybersecurity considerations. Issued in October 2014, the FDA’s initial guidance, “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices,”12 outlines cybersecurity considerations that medical device developers and manufacturers should consider during the initial design and development phases for new medical devices. The guidance recommends that device developers and manufacturers model their cybersecurity efforts on the core functions detailed in the “Framework for Improving Critical Infrastructure Cybersecurity,” developed by the U.S. National Institute of Standards and Technology (NIST) and published in 2014.13

This guidance also details the documentation related to the cybersecurity of a medical device that applicants should include in their submissions under the FDA’s premarket notification (510(k)) and premarket approval (PMA) programs. According to the guidance, specific documentation should include:

- Hazard analysis, mitigations and design considerations related to both intentional and unintentional cybersecurity risks that were evaluated during the design process, as well as a list of cybersecurity controls that were implemented;
- A “traceability matrix” that links the implemented controls to the identified cybersecurity risks;
- A summary plan for providing validated software updates through the expected useful life of the device;
- A description of the controls in place to assure the ongoing integrity of the medical devices software; and
- Instructions on the use of the device, and product specifications for recommended cybersecurity controls appropriate for its intended use.
A second FDA guidance, “Postmarket Management of Cybersecurity in Medical Devices,” was issued in December 2016, and covers issues related to the management of post-market cybersecurity vulnerabilities for marketed and distributed medical devices. This guidance emphasizes the importance of establishing a post-market management program for medical devices that includes the monitoring, identification and resolution of any identified cybersecurity vulnerabilities. The guidance also calls on device developers and manufacturers to implement a risk-based approach in assessing the extent of potential risk associated with an identified cyber vulnerability and in determining the steps required to mitigate that risk.15

In practice, the impact of these and other efforts by the FDA to address the cybersecurity of medical devices extends beyond the U.S. market. The FDA is a participant in the International Medical Device Regulators Forum (IMDRF), a voluntary consortium of national regulators representing major medical device markets around the world working to “accelerate international medical device regulatory harmonization and convergence.” The IMDRF’s medical device single audit program (MDSAP), which establishes a common set of requirements for the conduct of regulatory audits of device manufacturers’ quality systems, is just one example of the consortium’s efforts to harmonize regulatory frameworks.

In early 2018, an IMDRF working group published a proposed draft of a new guidance that expressly addresses cybersecurity risks. The guidance, “Essential Principles of Safety and Performance of Medical Devices and IVD Medical Devices,” represents a further effort by the IMDRF to support the global convergence of regulatory requirements through the adoption of fundamental design and manufacturing requirements for medical devices. Specifically, Clause 5.7.8 stipulates that medical devices:

“...should be designed, manufactured and maintained in such a way as to provide an adequate level of intrinsic immunity and/or resilience to deliberate attempts to gain unauthorized access to its safety related functions, its patient related data, its communication protocols and its ability to function as part of a connected system which enables it to operate as intended.”16

Although IMDRF documents do not have the effect of law in individual jurisdictions, IMDRF-participating regulators can be expected to evaluate their current requirements for medical devices for consistency with the fundamental requirements detailed in this guidance, gradually increasing awareness of the importance of cybersecurity in the design and use of medical devices.
Suggested Strategies for Minimizing Exposure

While actions by the FDA and IMDRF to strengthen cybersecurity requirements for medical devices may portend the prospect of additional regulatory oversight, the chief responsibility for minimizing the potential impact of cyberthreats remains with the healthcare industry, including hospital and healthcare center administrators, healthcare providers, and device developers and manufacturers, as well as patients and consumers. Indeed, the FDA’s guidance documents on cybersecurity of medical devices reinforce the importance of active collaboration between all stakeholders in identifying and addressing cybersecurity threats.

As noted previously, the FDA recommends that device developers and manufacturers model their cybersecurity efforts for medical devices around the five key functions identified in the NIST Cyber Security Framework, as follows:

• **Identify**—Develop the organizational understanding to identify and manage cybersecurity risks to systems, assets, data and capabilities, based on the findings of a comprehensive risk management assessment consistent with the unique requirements of the organization;

• **Protect**—Develop and implement the appropriate safeguards to ensure delivery of essential services, and to limit or contain the impact of a potential cyberattack;

• **Detect**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event, such as continuous security monitoring and detection processes;

• **Respond**—Develop and implement the appropriate activities to take action in connection with a detected cybersecurity event, such as those identified in an established response plan;

• **Recover**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

In addition, the FDA recommends the adoption of an effective post-market cybersecurity risk management program, which include the following key elements:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity, vulnerabilities and risk;
- Understanding, assessing and detecting presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;
- Clearly defining essential clinical performance to develop mitigations that protect, respond and recover from the cybersecurity risk;
- Adopting a coordinated vulnerability disclosure policy and practice; and
- Deploying mitigations that address cybersecurity risks early and prior to exploitation.

The FDA guidance on post-market management of cybersecurity of medical devices also strongly encourages device manufacturers to participate in a cybersecurity information sharing and analysis organization (ISAO) to facilitate the timely dissemination and sharing of cybersecurity information and intelligence among other industry participants and stakeholders. The National Health Information Sharing & Analysis Center (NH-ISAC) is one such organization that has entered into a Memorandum of Understanding with the FDA to facilitate the collection and timely dissemination of critical information related to the cybersecurity of medical devices.

While the above strategies are specifically intended for application by developers and manufacturers of medical devices, they are equally applicable to healthcare institutions and healthcare providers. As such, they represent a holistic approach to the control and management of cybersecurity risks associated with medical devices and systems, as well as the connected Health IT infrastructure.
There are a number of standards currently available that address key aspects of the safety and security of connected medical devices and related software. However, while compliance with these standards can be useful for dealing with the risks associated with cyberthreats to connected medical devices, they do not directly test the implementation or evaluate the effectiveness of the risk assessment process used by manufacturers to determine the breadth and extent of cyberthreats to which their devices might be exposed. Further, these standards do not provide clear and objective criteria to assess the actual effectiveness of product features designed to thwart the threats identified as part of the risk assessment.

This gap in addressing the full range of cybersecurity-related issues identified in the FDA’s guidance documents could compromise well-intentioned efforts by a device manufacturer to address potential cybersecurity vulnerabilities in their entirety. Further, it could complicate the FDA’s pre-market review of a medical device intended for sale or distribution in the U.S. market, potentially subjecting a device manufacturer to delays in the review process.

UL has been actively involved in efforts to assist the healthcare industry in addressing cybersecurity threats and in developing relevant standards to guide medical device manufacturers in meeting the cybersecurity requirements of the FDA and other regulatory agencies. For example, UL participated in the Health Care Industry Cybersecurity (HCIC) Task Force, organized by the U.S. Department of Health and Human Services (HHS), which produced a comprehensive report for Congress in 2017 on cybersecurity risks facing the healthcare industry that included a series of recommendations for addressing these risks.
In addition, UL’s 2900 series, Standard for Software Cybersecurity for Network-Connectable Devices, provides a comprehensive framework for the assessment of cybersecurity vulnerabilities and weaknesses, to minimize exploitation, address known malware, review security controls and increase security awareness and preparedness. First introduced in 2016, the UL 2900 series was developed to leverage and to complement other existing cybersecurity standards applicable to medical devices, and to address critical aspects of assessing cyberthreats as prescribed under the FDA’s medical device cybersecurity guidance documents. Specifically, UL 2900 standards emphasize the importance of providing objective evidence that sound cybersecurity protocols and practices have been implemented.

Currently, the UL 2900 series comprises several individual, inter-related Standards, as follows:

- **ANSI/UL 2900-1**: General Requirements for Network-Connectable Devices—Addresses general testing requirements applicable to all types of interconnected devices.

- **UL 2900-2-1**: Particular Requirements for Healthcare Systems—An industry-specific Standard, UL 2900-2-1 addresses specific testing requirements applicable to healthcare systems and medical devices.

- **UL 2900-3-1**: General Requirements for the Organization and Product Development Security Lifecycle Processes for Network-Connectable Devices (under development)—A process-specific Standard, UL 2900-3-1 addresses general testing of organizational processes for conducting a risk assessment to determine applicable cyberthreats.

In addition to being recognized by ANSI as an American National Standard, ANSI/UL 2900-1 has also been recognized by the FDA as a consensus Standard. As such, medical devices that have been certified in accordance with the Standard’s requirements are presumed to comply with the FDA’s related pre-market requirements for cybersecurity. The UL 2900 series of standards are also a core component of the UL Cybersecurity Assurance Program (CAP), which helps to identify security risks in a wide range of interconnected devices and systems through a holistic approach intended to mitigate cybersecurity risks. The UL CAP recognizes that healthcare facilities utilize a range of products in addition to medical devices, including power distribution/building management systems, consumer devices such as televisions, etc., and is therefore intended to cover many different assets critical to the security and protection of the national critical infrastructure.
The potential vulnerability of connected medical devices to cyberthreats is well-documented and a growing concern to the healthcare industry. In healthcare, the failure to promptly and thoroughly address the risks associated with compromised medical devices can have tragic consequences for patients and healthcare providers alike. As such, the responsibility for effective cybersecurity measures is shared by all industry participants and stakeholders, including healthcare institutions, healthcare providers, medical device developers and manufacturers, and patients and consumers.

For medical device developers and manufacturers, regulators in the U.S. are moving quickly to implement rigorous requirements intended to strengthen the cybersecurity of medical devices, and authorities in other major markets are establishing comparable regulations as well. Therefore, it is incumbent upon medical device manufacturers to work diligently to design mitigations for cyberthreats into the earliest stages of product development, and to implement effective post-market programs designed to identify and address new threats as they emerge.

For further information on UL's efforts to support the cybersecurity of medical devices, or to learn more about the UL 2900 series of standards, contact ULCYBER@UL.com. Or go to UL.com/cybersecurity.
End notes


End notes continued


15. It is important to note that guidance documents issued by the FDA are developed to provide insight in the agency’s current approach to the application of its rules and regulations, and do not have the force of law. However, they can be invaluable resources to industry in navigating the FDA’s pre-market submission process and can help to reduce the likelihood of delays or setbacks in obtaining FDA recognition.
