POLSINELLI

FDA Releases Final Cybersecurity Guidance for Medical Devices

By Jean Marie R. Pechette and Ken Briggs

Overview and General Principles

On October 2, 2014, the Food and Drug Administration ("FDA") finalized guidance describing the FDA's position on cybersecurity standards for medical devices. The guidance discusses cybersecurity principles pertaining to the development of medical devices, documentation that should be submitted with premarket applications, and recognized standards for medical device technology. The FDA pointed to the increasing prevalence of devices connected to system networks and the internet, and the frequent electronic exchange of medical device-related health information, as necessitating effective cybersecurity standards to assure medical device functionality and safety.

The guidance, titled "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (the "Cybersecurity Guidance"), is intended to supplement FDA's "Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices." The Cybersecurity Guidance describes the FDA's position as a cybersecurity framework to guide the development of medical devices: Identify, Protect, Detect, Respond, and Recover.

The Cybersecurity Guidance signals a major step towards specific cybersecurity requirements and regulations for medical devices. The FDA states that the standards described in the guidance are not yet required—but encouraged—for premarket approval. These activities are part of a manufacturer's cybersecurity vulnerability and management approach in conjunction with the software validation and risk analysis required by 21 CFR 820.30(g). The FDA explains that this approach should address at least the following elements:

- Identification of assets, threats, and vulnerabilities;
- Assessment of the impact of threats and vulnerabilities on device functionality and end users/patients;
- Assessment of the likelihood of a threat and of a vulnerability being exploited;
- Determination of risk levels and suitable mitigation strategies; and
- Assessment of residual risk and risk acceptance criteria.

Medical devices are being developed and used with more advanced technologies, all of which are vulnerable to a variety of security threats. These technologies provide a number of benefits including the enhancement of a device's functionality, the creation of more information and tools to treat a patient, and the promotion of personalized medicine. However, with more complex and cutting-edge technology comes the threat that a compromised device might not work in its intended way. Inadequate cybersecurity can result in device malfunction, loss of data availability or integrity, or exposure of other connected devices or networks to security threats, all of which may have the potential of resulting in patient illness, injury, or death. The Cybersecurity Guidance is the FDA's most recent step in addressing these concerns, but more significant and detailed requirements are likely to follow. Thus, industry stakeholders should prepare for these developments now.

Cybersecurity Safeguards

The Cybersecurity Guidance describes high-level standards that manufacturers should consider in the development of medical devices.

Identify and Protect

The FDA explains that the first step is to identify the vulnerabilities associated with a device, taking into account the device's intended use, the presence and intent of its electronic data interfaces, its intended environment of use, the type of cybersecurity vulnerabilities present, the likelihood the vulnerability will be exploited (either intentionally or unintentionally), and the probable risk of patient harm due to a cybersecurity incident. The second step is to balance between the cybersecurity safeguards and the usability of the device in its intended environment of use (e.g., home use versus health care facility use). For example, the security controls should not unreasonably hinder access to a device intended for use during an emergency situation. In other words, the cybersecurity of a medical device is an integral consideration in the safety and efficacy of a device. The Cybersecurity Guidance pertains to premarket determinations, but it does not clearly preview the FDA's position about cybersecurity threats discovered when the product is on the market.

Limit Access to Trusted Users Only

The safeguards described by the FDA are standard measures in the security industry. The safeguards fall generally into those designed to restrict access to the information or device only by intended persons, to ensure trusted content, and to preserve functionality (or avoid injury) in the event a device is compromised.

Safeguards implemented for the purpose of restricting access to a device will be of a different quality or character depending on the nature of the device. Standard safeguards, including those referenced by the FDA, are the abilities to:

- Limit access to devices through the authentication of users (e.g., user credentials, biometrics);
- Use automatic timed methods to terminate sessions within the system where appropriate for the use environment;
- Use role-based authorization privileges (e.g., caregiver, system administrator or device role;
- Use appropriate authentication (e.g., multi-factor authentication to permit privileged device access to system administrators, service technicians, maintenance personnel);
- Strengthen password protection by avoiding "hardcoded" password or common words (i.e., passwords which are the same for each device, difficult to change, and vulnerable to public disclosure) and limit public access to passwords used for privileged device access;
- Provide physical safeguards where appropriate (e.g., locks on devices and their communication ports to minimize tampering); and
- Require user authentication or other appropriate controls before permitting software or firmware updates, including those affecting the operating system, applications, and anti-malware.

Devices that integrate more types of technologies may require additional safeguards to limit access to the device by intended persons. Additional safeguards may involve virus protection management, transmission security, data encryption, and other software/firmware standards. These safeguards become enormously more complex when the device is designed to be accessed by other electronic components throughout the medical device's lifecycle as one compromised device can corrupt another. For example, certain devices may connect, via wireless connection or otherwise, to a physician's computer or even a patient's mobile phone. The security of these ancillary devices will necessarily impact the cybersecurity considerations for the actual medical device.

Ensure Trusted Content

Safeguards to ensure trusted content should also be considered. The Cybersecurity Guidance describes the following safeguards:

- Restrict software or firmware updates to authenticated code. One authentication method manufacturers may consider is code signature verification;
- Use systematic procedures for authorized users to download version-identifiable software and firmware from the manufacturer; and

- Ensure capability of secure data transfer to and from the device, and when appropriate, use methods for encryption.

The generality of the safeguards described by the FDA does not reflect the complexity of actually implementing the safeguards let alone predicting their need. Wireless devices, devices intended to be used by patients, and devices transmitting information periodically to a third-party all require different considerations during development and throughout the device's lifecycle.

Detect, Respond, Recover

The ever-evolving world of cybersecurity demands continual evaluation for devices even after premarket approval is obtained. The Cybersecurity Guidance does not discuss the FDA's position on remediation of security incidents, but the FDA does explain that such considerations should be documented even as early as the premarket process. The FDA discussed the following standards in connection with a compromised device:

- Implement features that allow for security compromises to be detected, recognized, logged, timed, and acted upon during normal use;
- Develop and provide information to the end user concerning appropriate actions to take upon detection of a cybersecurity event;
- Implement device features that protect critical functionality, even when the device's cybersecurity has been compromised; and
- Provide methods for retention and recovery of device configuration by an authenticated privileged user.

The Cybersecurity Guidance describes FDA-recognized consensus standards dealing with information technology and medical device security. The FDA has not indicated whether these standards are to be considered merely for guidance or whether the standards set a minimum level of compliance.

Cybersecurity Documentation

The Cybersecurity Guidance describes categories of documents that should be provided during the premarket process. In the premarket submission, manufacturers should provide the following information related to the cybersecurity of their medical device:

- Hazard analysis, mitigations, and design considerations pertaining to intentional and unintentional cybersecurity risks associated with the device, including specific risks considered in the design and a specific list and justification for all cybersecurity controls;
- A traceability matrix correlating the risks and the proposed controls;

- A summary describing the plan for providing validated software updates and patches as needed throughout the lifecycle of the medical device to assure its continued safety and effectiveness. (Note that the FDA typically will not need to review or approve medical device software changes made solely to strengthen cybersecurity);
- A summary describing controls in place to assure the medical device software will maintain its integrity from the point of origin to the point at which the device leaves the control of the manufacturer;
- Device use instructions and product specifications related to recommended cybersecurity controls appropriate for the intended use environment. The FDA has not explained the measures it will use to assess the safety of the device through the documents describing a device's cybersecurity.

This documentation should be carefully developed and maintained. The documentation would necessarily contain specific discussions of the cybersecurity strengths and weaknesses of the device and the underlying reasoning for the implementation of the controls. The manufacturer's judgments about reasonable and appropriate safeguards—made prior to market availability—may become relevant and material in any lawsuit involving a compromised device. Assessments of what safeguards are reasonable and appropriate will take on an analysis, and will face challenges, of a much different quality than those relating to the design of a device or the properties of a drug. Further, the information developed in anticipation of the premarket approval process and disclosed to the government may provide a blueprint of the weaknesses that can be exploited to gain access to a patient's or provider's information or to obtain proprietary information about the device itself.

Investing in Cybersecurity Standards

Medical device cybersecurity is an emerging concern. Cybersecurity standards for medical devices will predictably track the security standards in other industries and even subsets of the healthcare industry. The Cybersecurity Guidance reflects safeguards similar to those for health information established and rigorously enforced through the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The medical device industry should expect more specific standards to be expressed by the FDA in the near future, and should anticipate changes to these standards. Manufacturers and developers should not wait for the FDA to publish more specific or technical guidance before considering cybersecurity safeguards in their devices. Waiting for the FDA to promulgate required safeguards—instead of these advisory safeguards—may set development back years depending on the nature and adaptability of the product. Industry stakeholders, including providers and manufacturers, should develop medical devices in anticipation of the evolving cybersecurity environment: devices perceived as secure today might not be secure tomorrow.

Enforcement of these standards is even more unpredictable given the overlap between the FDA's cybersecurity standards and the security standards established under HIPAA. These overlapping frameworks may expose stakeholders to liability by more than one regulatory agency, both of which may have different mitigation and remediation requirements for the same security event. Further, inadequate cybersecurity of medical devices may expose stakeholders to very serious liability from any patient injuries that arise from the inadequate safeguards. Given the uncertain, but potentially very severe, liability relating to cybersecurity, mitigation and remediation of any threats to a device's cybersecurity should be a primary consideration at all phases of development. The Cybersecurity Guidance helps navigate premarket considerations, but it should not be the only reference consulted in the evaluation of appropriate safeguards.

Industry stakeholders should educate themselves on various regulatory expectations and standards of cybersecurity in the development of a product. Doing so will maximize a device's security while on the market and will preserve adaptability as the standards evolve. Investing in cybersecurity safeguards will maximize the stakeholder's ability to mitigate exposure to enforcement actions, efficiently move through the approval process, and minimize the costs in the event of compromise.