Bloomberg BNA

Health IT Law & Industry Report™

APRIL 25, 2016

FDA's New Guidance on Cybersecurity for Medical Devices: Important Lessons for the Entire Healthcare Industry

By Jeremy Feigelson, Mark P. Goodman, Maura K. Monaghan, Jim Pastore, David Sarratt, Jacob W. Stahl and Jonathan Metallo

As the "Internet of Things" grows, the range of digital targets for malicious actors is growing with it.

Not long ago, researchers at the University of South Alabama reported the results of an exercise which confirmed that "a student with basic information technology and computer science background" could hack medical devices such as a pacemaker, defibrillator, or insulin pump, with devastating effects on the patient.

In the wake of this and similar warnings, the FDA issued "Postmarket Management of Cybersecurity in Medical Devices" (the "Postmarket Guidance").

While the guidance is technically non-binding and has not yet been finalized, it states that the failure to address cybersecurity vulnerabilities may be deemed a violation of the Food, Drug, and Cosmetic Act ("FDCA").

The guidance is directed to device manufacturers, but also emphasizes that securing devices is the responsibility of other stakeholders including health care facilities, providers, and patients.

All healthcare stakeholders therefore should take heed to the FDA's recommendations, particularly its strong encouragement to join Information Sharing and Analysis Organizations ("ISAOs") and to implement the NIST Cybersecurity Framework.

Jeremy Feigelson, Mark P. Goodman, Maura K. Monaghan and Jim Pastore are partners; David Sarratt and Jacob W. Stahl are counsel; and Jonathan Metallo is an associate in the New York office of Debevoise & Plimpton LLP.

General Principles of Effective Cybersecurity Management

Information Sharing Analysis Organizations

The Postmarket Guidance makes clear that companies in the healthcare industry should keep abreast of developments in cybersecurity.

To accomplish that task, the FDA "strongly recommend[s]" that stakeholders participate in ISAOs. ISAOs foster collaboration among private entities and the government on cybersecurity intelligence.

By joining ISAOs, stakeholders can share and disseminate information on cybersecurity vulnerabilities and exploits.

By joining ISAOs, stakeholders can share and disseminate information on cybersecurity vulnerabilities and exploits. *[Editors note: Software tools designed to take advantage of a flaw in a computer system, frequently for malicious purposes such as installing malware.]*.

The U.S. Government promoted the development of ISAOs in a February 2015 Executive Order, which directed the Department of Homeland Security ("DHS") to select a non-governmental organization to act as the ISAO Standards Organization that will issue a set of membership and operational best practices for all ISAOs.

The DHS has chosen as the Standards Organization a collaboration among the University of Texas at San Antonio, the Logistics Management Institute, and the retail Cyber Intelligence Sharing Center, though they have yet to issue any standard best practices for ISAOs.[1]

Nevertheless, DHS has provided some guidance as to its expectations for the best practices ISAOs will follow, based on four essential characteristics:

■ **Inclusive**: ISAOs' membership should be open to any business sector, to non-profit and for-profit organizations, and to those experienced and inexperienced in cybersecurity.

■ **Actionable**: ISAOs should provide their membership with automated, real-time information on cybersecurity threats and risks, with practical tips that members can effectively use to address these issues.

■ **Transparent**: ISAOs should provide clear information to prospective members on their operation and utility.

■ **Trusted**: ISAOs should allow members to request all their information and intelligence be treated as Protected Critical Infrastructure Information (''PCII''). PCII is protected from disclosure under the Freedom of Information Act or State Sunshine Laws, and is exempt from regulatory use and civil litigation.

Even without any guidance from the ISAO Standards Organization, a number of ISAOs have already been established, including those dedicated to specific business sectors.

Additionally, the Cybersecurity Information Sharing Act (''CISA''), which was passed last year, provides companies with further encouragement to participate in ISAOs.

CISA immunizes private companies from liability when sharing ''cyber threat indicators'' or ''defensive measures'' with DHS through certain specific means.[2] Cyber threat indicators and defensive measures are broadly defined to include any intelligence on cybersecurity vulnerabilities and any defense designed to defeat or mitigate cyber threats. One accepted method of sharing information with DHS under CISA is through an ISAO.

The FDA has tacitly endorsed one ISAO for those in the healthcare sector: the National Health Information Sharing & Analysis Center.

The FDA has tacitly endorsed one ISAO for those in the healthcare sector: the National Health Information Sharing & Analysis Center (''NH-ISAC''). In August 2014, the FDA and NH-ISAC entered a Memorandum of Understanding (''MoU'') describing terms of collaboration between their organizations for addressing cybersecurity in medical devices and the surrounding healthcare IT infrastructure.[3] The MoU serves as a broad outline of the goals of FDA and NH-ISAC collaboration, setting forth the intent of both organizations to share information on cybersecurity vulnerabilities and threats.

Membership in NH-ISAC provides healthcare stakeholders with a variety of tools to strengthen their cybersecurity defenses. Members in NH-ISAC receive access to a secure portal through which they can share information on cybersecurity threats and risks.

NH-ISAC also offers its expertise to design, develop, and implement cybersecurity exercises for member organizations hoping to test their defenses before any incident. Additionally, members can choose to have NH-ISAC monitor their public facing domain names and IP addresses for anomalous activity.

NIST Framework for Improving Critical Infrastructure Cybersecurity

Additionally, the FDA has joined other regulators in encouraging the adoption of the voluntary NIST Framework for Improving Critical Infrastructure Cybersecurity (the ''NIST Framework'').

The National Institute of Standards and Technology (''NIST''), an agency within the U.S. Department of Commerce, developed the framework in 2014 in response to a 2013 Executive Order charging Federal Government agencies with the improvement of cybersecurity in ''critical infrastructure organizations.''

The Executive Order broadly defined as ''critical'' any system or asset so important to the country that its ''incapacity or destruction . . . would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.''

The NIST Framework has quickly gained traction in the private sector, in critical and non-critical industries alike. Law enforcement and regulators, including the U.S. Federal Trade Commission, U.S. Securities and Exchange Commission, and the U.S. Department of Justice, have increasingly cited NIST as a key source of cybersecurity guidance for U.S. companies.

[1] ISAO Standards Organization, Products, https://www.isao.org/products/

[2] Note that any information shared must not contain ''personal information.'' While not defined in the Act, personal information refers to any data defined as protected by specific sectors, *e.g.*, protected health information under the Health Insurance Portability and Accountability Act (''HIPAA'').

[3] Memorandum of Understanding Between the NH-ISAC and the U.S. FDA Center for Devices and Radiological Health, August 26, 2014, *available at* http://www.fda.gov/AboutFDA/PartnershipsCollaborations/MemorandaofUnderstandingMOUs/OtherMOUs/ucm412565.htm.

The NIST Framework is focused on five core principles viewed as the basic building blocks for an effective cybersecurity program: Identify, Detect, Protect, Respond and Recover.

These principles guide companies in developing a plan for each phase of their cybersecurity strategy, from preparing for a potential breach, to detecting a potential breach quickly when it begins, and finally responding and recovering from a breach.

NIST offers these principles, like the entire framework, as a flexible tool for designing and strengthening cybersecurity. It can be specially tailored to the risk profile of the implementing company.

The NIST framework sets forth principles that help define the types of steps any company can take to strengthen its cybersecurity defenses, including:

- **Identifying** sensitive assets, vulnerabilities, personnel important in overseeing and executing in cybersecurity, and the risks facing the company from a possible cyber-attack;
- **Protecting** the company by training employees in cybersecurity awareness and implementing technical defenses to cyber-attacks;
- **Detecting** anomalies and potential security breaches in the company's system;
- **Responding** to a detected cybersecurity event to mitigate the harm and reviewing the lessons learned that can inform future defensive measures;
- **Recovering** from breaches if and when they happen.

When implementing these principles, healthcare stakeholders should focus on customizing them to industry-specific issues. For example, the ''identify'' step should involve the databases where sensitive patient health information (''PHI'') is stored.

Furthermore, in the case of a network that maintains PHI, the risk tolerance must be low because a PHI release may result in a HIPAA violation. The ''protect'' principle will require training employees to recognize potential cyber-attacks, such as malicious actors trying to obtain the password for a patient's online account with his or her medical insurer.

The Postmarket Guidance includes specific recommendations to medical device manufacturers on implementing the NIST Framework based on the medical device risk management framework described in the guidance. We will therefore discuss the risk management framework for medical devices before turning to how the NIST framework should apply to them.

Medical Device Manufacturers

Specific Guidance on Securing Medical Devices

The FDA describes in great detail how it expects medical device manufacturers will identify, assess, and respond to cybersecurity vulnerabilities. This description provides insight for all healthcare stakeholders on the cybersecurity standard of care the FDA believes that the healthcare industry should follow.

The FDA sets forth a framework focused on maintaining the ''essential clinical performance'' of medical devices, a term manufacturers should define with respect to individual devices. Manufacturers should work with others in the healthcare industry to identify device vulnerabilities and assess the risk posed to essential clinical performance.

The level of risk posed by a vulnerability will depend on an evaluation of (a) the ease of exploiting it and (b) the severity of the potential health impact that would follow. The FDA offers specific suggestions on the means for this evaluation:

- To evaluate a vulnerability's exploitability, the FDA cites the ''Common Vulnerability Scoring System'' (''CVSS'') as a useful tool for assessing the exploitability of vulnerabilities. CVSS was issued by the Forum of Incident Response and Security Teams (''FIRST''), a nonprofit organization consisting of member organizations from various industries. FIRST works to provide best practices and tools for responding to cybersecurity threats.
- To evaluate the severity of a vulnerability's potential health impact, the FDA recommends guidance from ISO entitled ''Medical devices—Application of risk management to medical devices.'' ISO is an independent, non-governmental international organization of national standards bodies that issues technological standards. The risk management scale for medical devices ranges from risks with negligible impact, which provide an ''inconvenience or temporary discomfort,'' to risks with a potentially catastrophic impact that ''results in patient death.''

The FDA expects manufacturers to use such tools to assess vulnerabilities as presenting a ''low,'' or controlled risk to a device's essential clinical performance, or a significant, ''uncontrolled risk.'' The guidance includes a matrix for evaluating vulnerabilities as a controlled or uncontrolled risk based on the exploitability and severity of the potential health impact.

On one end are clearly controlled risks, which involve vulnerabilities with a low risk of exploitation and a negligible impact to health. On the other end are clearly uncontrolled risks, which involve vulnerabilities with a high risk of exploitation and a potentially catastrophic impact on health.

These recommendations reflect a growing trend among regulators to be quite prescriptive on cybersecurity. For example, the New York Department of Financial Services communicated with a number of federal regulators late last year on the need for specific cybersecurity regulations in the financial services sector, suggesting mandates for the appointment of a chief information security officer and the implementation of multi-factor authentication.

The assessment of vulnerabilities as presenting a controlled or uncontrolled risk to essential clinical performance will determine how the manufacturer should respond to the issue, and whether the vulnerability must be reported to the FDA.

The assessment of vulnerabilities as presenting a controlled or uncontrolled risk to essential clinical performance will determine how the manufacturer should respond to the issue, and whether the vulnerability must be reported to the FDA:

Controlled Risks: If the manufacturer determines risks are controlled, any changes that it makes to medical devices—such as routine updates and patches—to address identified risks do not need to be reported to the FDA. With respect to Class III medical devices that require premarket approval, and for which periodic postmarket reporting is required, reports must disclose even routine changes.

An example of a controlled risk might involve the detection on a medical device of malware designed to collect Internet browsing information. If the malware poses no threat to the device's essential clinical performance, then the manufacturer does not need to report to the FDA its steps to address the malware, unless the malware affected a Class III medical device.

Uncontrolled Risks: If the manufacturer determines risks are uncontrolled, the risks and remediation should be reported to the FDA under 21 C.F.R. 806.10. However, the FDA indicates that it will not require reporting under this regulation when:

- No serious adverse events or deaths are known to be associated with the vulnerability;
- Within 30 days of learning of the vulnerability, the manufacturer implements changes or compensating controls on the device to bring the risk to an acceptable level and notifies users; and
- The manufacturer is a participating member of an ISAO, such as NH-ISAC.

Again, devices that require a periodic report must still disclose changes when they file that report. Manufacturers should also notify users about potential temporary fixes for the issue until the vulnerability is fully remediated. Further, if a manufacturer fails to address uncontrolled risks to a device's essential clinical performance, the FDA will assess the risk posed to patient health in evaluating whether a violation of the FDCA has occurred.

An example of an uncontrolled risk is a vulnerability that allows unauthorized users to reprogram a medical device in a way that could impair its medical function. Even assuming the device is not a Class III medical device, such a risk would require notification to the FDA unless no serious adverse events or deaths occurred, the manufacturer remediated and notified users within 30 days, and the manufacturer participates in an ISAO.

Implementing the NIST Framework for a Medical Device Manufacturer

An appendix to the guidance includes recommendations to medical device manufacturers on implementing the NIST Framework. These recommendations are based on the concept of ''essential clinical performance'' detailed in the guidance. Rather than offering a discrete set of recommendations for each principle, the FDA offers general guidance spanning several principles at once.

For example, the guidance urges manufacturers to **identify** the essential clinical performance of their devices and any signs of cybersecurity or quality problems with their devices, at least in part by incorporating into the device design some capability to detect attacks and capture forensic evidence.

To address both principles of **protect** and **detect**, manufacturers should assess vulnerabilities with tools such as CVSS, characterize identified threats and vulnerabilities in order to triage the issues to be remediated, generate summary reports on each identified vulnerability that include a risk analysis and threat report, and implement a process to assess cybersecurity issues both horizontally, *i.e.*, across all devices in their portfolio, and vertically, *i.e.*, on specific device components.

In **protecting, responding,** and **recovering** from cybersecurity incidents, manufacturers should establish mechanisms for communicating with users about vulnerabilities, remediate incidents in a way that is proportional to the magnitude of the problem, and validate remediation to ensure risks were properly mitigated.

This guidance on NIST implementation is not meant to cover all considerations that should inform use of the NIST Framework, but shows how the FDA's specific guidance for device manufacturers should fit within their use of NIST. In providing these recommendations, the FDA provides concrete examples of how it expects NIST will be used in the healthcare industry.

Impact of the Guidance

With the Postmarket Guidance, the FDA takes direct aim at imposing standards on medical devices, but it is a safe bet that neither the FDA nor other regulators will stop there.

The guidance itself emphasizes the shared responsibility of all healthcare stakeholders to address cybersecurity on an ongoing basis. Adopting the NIST Framework and participating in ISAOs seem wise steps for any business subject to FDA scrutiny.

Going forward, other regulators, the plaintiffs' bar and courts may also point to the FDA guidance as contributing to an emerging standard of care that could, in time, support legal liability under various theories.