Hogan Lovells

# Harmonizing cybersecurity for medical devices: International collaboration moves forward

9 October 2019

On 1 October 2019 the International Medical Device Regulators Forum (IMDRF) Medical Device Cybersecurity Working Group released a draft document titled "Principles and Practices for Medical Device Cybersecurity" (IMDRF draft). The document reflects the increasing concern evinced by cybersecurity events that have touched medical devices, hospitals, and health care networks. Recognizing the need for global convergence to address these threats, the IMDRF draft proposes a broad risk-based framework, with recommendations for harmonized standards and approaches.

Addressing cybersecurity vulnerabilities is a tricky business, as many stakeholders, including industry, government, and health care providers, among others, must work together. In many instances this involves complex retrofitting of existing systems and careful communication of complex situations. The need to tackle these challenges simultaneously around the world, while also being consistent with the concerns and requirements of a global set of regulators, emphasizes the need for harmonization. The IMDRF guidance provides recommendations for premarket considerations, managing postmarket risk, including with legacy devices, and for shared responsibility across the health care ecosystem. It is expected that working group member countries will adopt the approaches described in the IMDRF draft.

**Background**

The IMDRF working group on cybersecurity included participants from Australia, Brazil, Canada, China, Europe, Japan, Russia, Singapore, South Korea, and the United States. The development of the IMDRF draft to embrace broad standards and specific policies for adoption across jurisdictions was led by personnel from the U.S. Food and Drug Administration (FDA) and Health Canada. FDA and the competent authorities of the EU member states are dynamically engaged in addressing rapidly evolving cybersecurity challenges; the IMDRF draft provides a window into the IMDRF's current thinking, as well as pointing toward global market considerations. This work is in line with the IMDRF's growing interest in adopting global regulatory standards for connected medical devices, which has also been reflected in a number of other regulatory initiatives, such as adoption of the IMDRF framework for Software as a Medical Device.

The broadly stated principles in the IMDRF draft largely correspond to and consolidate the detailed approach outlined in FDA's two medical device cybersecurity guidances: "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" (premarket guidance), for which a draft update was issued in October 2018, and "Postmarket Management of Cybersecurity in Medical Devices" (postmarket guidance) from December 2016. The IMDRF draft also provides further emphasis in certain areas that were lightly addressed by FDA.

In the European Union, competent authorities of individual EU member states have also started to develop guidelines to address cybersecurity challenges in relation to medical devices. For example:

- The French competent authority, the ANSM (Agence National de Sécurité du Médicament et des Produits de Santé*)* published in July 2019 draft guidelines on cybersecurity of medical devices integrating software during their life cycle.
- At the EU level, the EU legislator has also adopted a number of new regulations that must be considered by manufacturers when assessing the cybersecurity risks for their medical devices.
- The EU Medical Devices Regulation (MDR), which will be applicable on 26 May 2020, includes specific requirements applicable to the management of cybersecurity in medical devices.

The IMDRF draft addresses the total product life cycle, recommending the security risk management process developed in AAMI TIR57:2016[1] and referencing a number of U.S. government and international standards as resources. The IMDRF draft draws on key components of existing FDA guidance, with some divergence, as discussed below.

Significantly, the IMDRF draft specifically excludes consideration of any risks to data privacy, instead focusing on cybersecurity risks to patient harm. As a result, it does not take into account myriad developments relevant to data protection requirements worldwide, such as the EU General Data Protection (GDPR) and California Consumer Privacy Act (CCPA), which include a number of data privacy and cybersecurity considerations for medical device manufacturers and others in the health sector.

## Premarket considerations

The overarching principles of the IMDRF draft are largely consistent with FDA's premarket guidance but organized in a slightly different fashion. The IMDRF draft includes a table of design principles with descriptions and examples containing the following elements: secure communications, data confidentiality, data integrity, user access, software maintenance, hardware or physical design, and reliability and availability. FDA's premarket guidance organizes design recommendations around "designing a trustworthy device," with emphasis on preventing unauthorized use; ensuring trusted content via code, data, and execution integrity; and design for timely detection and response to potential cybersecurity incidents. Both documents make extensive reference to the U.S. National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).

Like FDA's recommendations for protecting and detecting, the IMDRF draft calls out risk management, including the application of sound risk management principles that include security risk assessments, threat modeling, and vulnerability scoring. It also recommends security testing during design verification testing that involves targeted searches, technical security analyses, and a vulnerability assessment. The IMDRF document recommends the

[1] Principles for medical device security — Risk management.

development of a postmarket management strategy before market entry for monitoring of threats and responding to emerging cybersecurity threats that includes postmarket vigilance, vulnerability disclosures, patching and updates, recovery, and information sharing. In part, these control mechanisms are to be developed pre-commercialization and should be reflected in the recommended "Risk Management Documentation."

Most of the labeling recommendations in the IMDRF draft are taken nearly verbatim from FDA's premarket guidance, including FDA's references to a "Cybersecurity Bill of Materials," which the IMDRF draft refers to as the "Software Bill of Materials." Standards for disclosure of software components remain a sensitive area of contention among industry stakeholders, as there is a tension between transparency for users around security operations and potential proprietary and security compromises.

## Postmarket

Both the IMDRF draft and FDA's postmarket guidance stress the importance of shared responsibility and information sharing mechanisms in the postmarket ecosystem. The IMDRF draft takes a strong position in favor of cybersecurity information sharing, referring to it as a "foundational principle," encouraging organizations to participate, and at one point declaring that a default rule should be for organizations to share "any information that, if shared, would reduce the risk of patient harm or ensure continuity in healthcare delivery." The IMDRF draft calls for highly transparent formalized processes called Coordinated Vulnerability Disclosure for coordinating information vulnerabilities, mitigations and compensating controls, and disclosures to all relevant stakeholders, including customers, peer companies, government regulators, information sharing organizations, security researchers, and the public.

The IMDRF draft nonetheless acknowledges that such broad information sharing is not entirely risk-free; some companies have suffered damage as a result of exercising transparency when dealing with cybersecurity matters. In the medical device industry, where changing risks must always balance against the benefits of the product, it continues to be a matter of much consideration what and how cybersecurity risks are to be communicated and even whether such communications will serve to further increase the risk of a vulnerability.

FDA's postmarket guidance states that the agency will exercise enforcement discretion related to reporting requirements for manufacturers participating in an Information Sharing and Analysis Organization, among other criteria. Striking the proper balance between transparency critical to health systems and manufacturers' proprietary concerns most likely will continue to inform efforts to develop effective harmonized standards and local applications of cybersecurity regulations.

## Shared responsibilities

While FDA speaks to shared responsibilities of manufacturers, health care providers, hospitals, and the government, the IMDRF draft provides recommendations to health care providers (professional facilities and home health care environments) and patient environments for addressing vulnerabilities.

## Regulating risk

The IMDRF draft adheres to a risk-based approach to regulatory oversight, but does not prescribe specific applications of this approach, which for the United States are more detailed in the FDA guidances and referenced international standards. For example, FDA divides cybersecurity risk into "tier 1" and "tier 2" categories, for "higher" and "standard" cybersecurity risk. Similarly, the

IMDRF draft suggests broad principles for when remediation of vulnerabilities (i.e., software changes) need to be reviewed by regulatory authorities pre-release, including two questions:

1. Is the change proposed to solely strengthen cybersecurity and has been determined to not have any other impact on the software of device?

2. Is the change proposed to remediate or reduce the risk of a vulnerability associated with unacceptable residual risk related to patient harm?

## Legacy devices

As current events dramatically illustrate, devices still in operation marketed prior to current cybersecurity threats can pose particular cybersecurity challenges. The IMDRF draft speaks directly to the challenges posed by legacy devices to both manufacturers and health care providers. Most importantly, it recommends that devices be monitored for critical vulnerabilities and that manufacturers clearly communicate end of life and end of support dates when devices are provided and installed. While this does not completely get at the heart of the issue with the millions of devices that were released before cybersecurity became a heightened concern for the medical device industry and that remain in use, it does at least suggest some minimum expectations as to how manufacturers could be managing these legacy devices. For an in-depth discussion of FDA's growing concerns around postmarket cybersecurity of medical devices see the interview with Hogan Lovells partner Jodi Scott.

## Conclusion

Cybersecurity vulnerabilities in medical devices are a growing concern for manufacturers, governments, and health care providers alike. We expect that there will continue to be a steady and perhaps increasing pace of cybersecurity vulnerabilities being identified, with ensuing cyberattacks, disruptions, and breaches in medical devices. While regulators and manufacturers are making great strides in designing and developing medical devices with enhanced consideration for cybersecurity risks, there is still a great deal of existing products for which their cybersecurity controls may be outpaced by evolving threats and newly identified vulnerabilities. However, it is important to weigh the benefits of these products against the risks posed by identified cybersecurity vulnerabilities when considering how to respond to cybersecurity issues, as it is rarely advantageous to simply remove or disable vulnerable products, thereby fully eliminating the risk (and also any benefit they may provide).

Further, the hacking community is learning as fast as or faster than the medical device industry is developing and remediating product and it is important for the sake of the entire health care system that manufacturers, regulators, and health care systems coordinate and collaborate worldwide and that they be ever vigilant – ready to respond when the health care ecosystem comes under attack. All efforts at globalization and harmonization are beneficial to laying the groundwork that will allow manufacturers to do their part and respond quickly to threats and vulnerabilities.

## Contacts

**Jodi Scott**
Partner, Denver
**T** +1 303 454 2463
jodi.scott@hoganlovells.com

**Yarmela Pavlovic**
Partner, San Francisco
**T** +1 415 374 2336
yarmela.pavlovic@hoganlovells.com

**Paul Otto**
Partner, Washington, D.C.
**T** +1 202 637 5887
paul.otto@hoganlovells.com

**Fabien Roy**
Partner, Brussels
**T** +32 2 505 0970
fabien.roy@hoganlovells.com

**www.hoganlovells.com**