Medical Device Cybersecurity Report

Advancing Coordinated Vulnerability Disclosure

MDIC
MEDICAL DEVICE INNOVATION CONSORTIUM

202-828-1600 | www.mdic.org | info@mdic.org

ACKNOWLEDGEMENTS

This report was prepared by the Medical Device Innovation Consortium (MDIC) in collaboration with Luke Dembosky, Jeremy Feigelson, Mark P. Goodman, Maura K. Monaghan, Paul D. Rubin, Jacob W. Stahl, Mason Fitch, and Melissa Runsten of Debevoise & Plimpton LLP, and John deCraen of Alvarez & Marsal.

The MDIC Steering Committee for this project included Randy Schiestl, PMP (Boston Scientific), Suzanne Schwartz, MD MBA (FDA), Pamela Goldberg, MBA. (MDIC), Seth Carmody, PhD (FDA), and Lisa Griffin Vincent, PhD MA (MDIC).

Table of Contents

I. Introduction 1

II. Scope 2

III. Key Findings Regarding the Development and Implementation of CVD Policies 3

IV. FDA Legal Obligations Supporting the Need for CVD Policies and Portals 6

A. Cybersecurity Risk Management Programs and the Quality System Regulation 7

B. Reporting Cybersecurity Vulnerabilities to FDA: Regulatory Overview 7

1. Mandatory Medical Device Reporting 8

2. Reporting Medical Device Changes (Corrections and Removals) 8

C. FDA Safety Communications, Warning Letters, and Recalls 10

1. FDA Public Health Action Case Study: Infusion Pump Systems Safety Communications 10

2. FDA Public Health Action Case Study: Implantable Cardiac Pacemaker Safety Communications, Recalls, and Warning Letter 11

V. Role of an ISAO 12

VI. Other Legal and Commercial Considerations Supporting the Need for Effective Cybersecurity Practices 13

A. Product Liability 13

B. Securities Fraud Claims Against Publicly Traded Companies 15

C. Federal Criminal Enforcement 17

D. Privacy and Data Breaches 17

E. Class Actions Based on Economic Losses 19

F. Class Actions Based on Compromised Patient Data 21

G. Risk of Ransomware and Other Disruptive Attacks 22

H. The Potential Risk of Litigation Should Not Dissuade MDMs From Disclosing Vulnerabilities 22

I. Commercial Benefits to Developing Effective Cybersecurity Practices 23

VII. Developing an Internet-Based Portal for Receiving Medical Device Vulnerability Reports 23

VIII. Best Practices from Interviews 26

A. A Corporate Culture that Recognizes the Importance of Product Security. 26

B. A Properly Structured and Supported Product Security Team. 26

C. A Premium on Strong Customer Relationships and a Reputation for Prioritizing Patient Safety. 27

D. A Thorough, Well-Documented Assessment of Each Cybersecurity Vulnerability Reported to the MDM. 27

E. A Clear Policy and Procedure for Proactively Disclosing Vulnerabilities. 28

F. Treating Security Researchers as Partners Rather than Adversaries. 29

IX. General Cybersecurity Risk Management Principles 30

X. General Cybersecurity Operational Considerations 30

XI. Conclusion 31

I. Introduction

The Medical Device Innovation Consortium (MDIC) is the first non-profit public-private partnership created with the sole objective of advancing medical device regulatory science. As part of that mission, MDIC retained Debevoise & Plimpton LLP (Debevoise)[1] and Alvarez & Marsal (A&M)[2] to prepare this report encouraging the adoption of coordinated vulnerability disclosure (CVD) policies by medical device manufacturers (MDMs) in an effort to promote medical device cybersecurity and patient safety. CVD policies establish formalized processes for obtaining cybersecurity vulnerability information, assessing vulnerabilities, developing remediation strategies, and disclosing the existence of vulnerabilities and remediation approaches to various stakeholders—often including peer companies, customers, government regulators, cybersecurity information sharing organizations, and the public. This report addresses the importance of CVD policies for MDMs and stakeholders across the medical device ecosystem, including the creation of publicly available online portals to solicit vulnerability information.

Debevoise and A&M interviewed a wide range of stakeholders for this report, including large and small medical device companies, leading security researchers with extensive medical device cybersecurity expertise, representatives of a medical device trade association, and the United States Food and Drug Administration (FDA) officials. Although this report is based in large part on the feedback obtained during these interviews, it also includes an assessment of publicly available information issued by FDA and other stakeholders.

As medical devices and healthcare environments become more sophisticated and interconnected through networks and information systems, the risk of medical device cybersecurity vulnerabilities impacting patient safety and privacy has increased significantly. Because of the increased risk in recent years, the government has become increasingly focused on the issue. FDA, for example, has taken significant steps to develop policies and guidance to assist MDMs in addressing cybersecurity-related regulatory issues. Similarly, Congress has held oversight hearings designed to identify emerging risks and continues to consider legislative solutions, while media and grassroots organizations have expressed concerns about emerging cybersecurity vulnerabilities (particularly in light of recent cybersecurity-related Safety Communications issued by FDA and high-profile breaches in the healthcare industry).

Not surprisingly, stakeholders in the medical device industry have taken notice and continue to closely examine how they can proactively address product security in an ever-changing environment to quickly and effectively reduce any risks posed to patients. As explained in comprehensive FDA guidance documents, medical device cybersecurity concerns must be addressed not only during the design and development of medical devices, but also throughout the device lifecycle as potential cybersecurity vulnerabilities emerge.

---

[1] Debevoise & Plimpton LLP is a global, full-service law firm with leading Cybersecurity & Data Privacy and FDA/Healthcare practices, as well as far-reaching legal expertise impacting the medical device and healthcare ecosystem, including government enforcement, litigation, and white collar/regulatory defense.

[2] Alvarez & Marsal is a premier global professional advisory services firm most notable for its work in turnaround management and performance improvement of the world's largest and highest-profile businesses as well as for being a market and thought leader in digital investigations and cybersecurity advisory services.

Virtually all software and networked products (including medical electrical equipment) are susceptible to cybersecurity vulnerabilities. Non-MDM technology companies have long recognized the need to identify, validate, assess, remediate, and disclose such vulnerabilities and have, for many years, created CVD policies to accomplish these goals. MDMs are also now increasingly managing cybersecurity risk through the adoption of CVD policies and processes.

The growing adoption of CVD policies is evidence of a maturing medical device industry that continues to enhance its communication, collaboration, transparency, and risk mitigation capabilities.[3] The CVD process provides MDMs with a platform for coordinated and consistent interaction with a wide array of external and internal stakeholders. External stakeholders include the individual or entity that identifies the vulnerability (often an independent security researcher), government agencies (in the United States, typically FDA and the Department of Homeland Security (DHS) National Cybersecurity Communications and Integration Center (NCCIC)[4]), industry-based information sharing and analysis organizations (ISAOs), and hospitals and other healthcare delivery organizations (HDOs). Internal stakeholders typically include information technology (IT), research and development (R&D), engineering, product security, quality, legal, regulatory affairs, marketing, corporate communications, public relations, medical affairs, and field representatives.

MDMs' adoption of CVD policies will ensure that communication among these internal and external stakeholders is organized and implemented consistently and effectively, rather than being implemented on an *ad hoc* basis during a potential crisis situation with significant time constraints and organizational and market pressures.

II. Scope

This report was created solely for informational purposes to promote and inform cybersecurity discussions among stakeholders in the medical device ecosystem.[5] Medical device cybersecurity issues can be highly complex and fact-specific and therefore should be assessed by each MDM on a case-by-case basis with experienced legal counsel, taking into consideration a wide array of issues, including the specific product and related technology at issue.

This report is also not intended to identify or resolve the broad spectrum of legal issues associated with postmarket medical device cybersecurity. This report identifies many, but not all, of the adjacent legal issues, including FDA legal requirements, Securities and Exchange Commission (SEC) disclosure obligations for publicly traded companies, the Health Insurance Portability and Accountability Act (HIPAA), Federal Trade Commission (FTC) and state law privacy obligations, product liability exposure, federal and state laws governing business practices, contractual implications, and the impact of the European Union's new General Data Protection Regulation (GDPR).

[3] For example, a group of MDMs is collaborating to draft a White Paper that will provide instructional guidance for CVD policy and process implementation. The White Paper will be released in conjunction with the Healthcare & Public Health Sector Coordinating Councils' Cybersecurity Working Group.

[4] The functions of the DHS Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) have been integrated into NCCIC. Advisories issued by NCCIC are still known as ICS-CERT Advisories for continuity purposes.

[5] This report is not intended to relay legal conclusions or provide legal advice on specific facts or matters. If you require legal advice, please consult a qualified attorney licensed to practice in your jurisdiction.

III. Key Findings Regarding the Development and Implementation of CVD Policies

- ***There are numerous benefits to establishing CVD policies.*** As a general rule, MDMs are strongly encouraged to develop and implement thorough CVD policies. CVD policies have the potential to significantly reduce cybersecurity risk to MDMs, patients, and other stakeholders in the healthcare system ecosystem. Reasons for developing CVD policies include the following:

    - CVD policies further MDMs' goal of improving patient health and safety while also demonstrating good corporate citizenship. They also result in better communication among internal and external stakeholders, increased transparency, and thoughtful decision-making related to risk mitigation. Without a CVD policy, MDMs may find themselves playing defense and making *ad hoc* decisions should a vulnerability with serious legal and commercial ramifications arise.

    - The legal and other benefits of CVD policies generally far outweigh any potential detriments. MDMs are potentially subject to legal exposure if: (i) they do not have adequate processes for receiving information about potential cybersecurity vulnerabilities or do not become aware of a particular vulnerability, or (ii) they become aware of a vulnerability but fail to take appropriate action to respond (including, as appropriate, disclosure and mitigation). The particulars of a CVD policy, as well as the decisions about how to apply it in any real-world circumstance, of course are subject to case-by-case assessment and legal review by each MDM.

    - FDA encourages the adoption of CVD policies, has issued guidance to assist MDMs in developing such policies, and has formally recognized International Organization for Standardization (ISO) standards for the development of CVD policies and processes. FDA may assess the premarket and postmarket management of medical device cybersecurity during facility inspections.

    - Many HDOs ask MDMs for information on product security and CVD programs as part of the diligence process and require disclosure provisions in their contracts with MDMs. A robust CVD program may make it easier to comply with these requirements.

    - As MDMs increasingly adopt CVD policies and the disclosure of cybersecurity vulnerabilities becomes more common, any negative perception associated with vulnerability disclosure should be lessened as such disclosures are likely to be seen as part of a responsible continuous quality improvement and risk management system.

- ***CVD policies should reflect the heightened safety issues associated with medical devices.*** Medical devices, unlike most other categories of technological products, are highly regulated by FDA and equivalent regulatory agencies in other jurisdictions. In addition, a compromised medical device may result in serious patient health and safety risks. Accordingly, MDMs' CVD policies must account for FDA regulatory requirements and the potential safety implications associated with medical device vulnerabilities.

- ***CVD policies need to involve the entire organization.*** An MDM wishing to establish a CVD policy must generate buy-in from company executives and board members as well as a range of internal stakeholders typically involved in the CVD process, such as the IT, R&D, engineering,

manufacturing, legal, marketing, product security, regulatory affairs, corporate communications, public relations, medical affairs, field representative, and quality teams.

- ***CVD policies need the right organizational structure.*** Consistent day-to-day execution of CVD policies depends on an appropriately supported product security team. It may be helpful to have a direct reporting channel from the product security team to the C-Suite, to create distinct teams for product security and for information security, and to establish close coordination between the product security and quality teams.

- ***There are a range of regulatory and legal considerations supporting the establishment of CVD policies.*** MDMs may be subject to far-ranging legal liability based upon the commercial distribution of a medical device with a vulnerability. Accordingly, it is critically important for an MDM to implement carefully crafted policies regarding how the MDM will identify and remediate vulnerabilities and how it will properly disclose vulnerabilities to relevant stakeholders. Failure to do so could expose an MDM to FDA enforcement, SEC enforcement, Department of Justice (DOJ) enforcement, product liability lawsuits, HIPAA liability, enforcement related to data breaches, commercial litigation, and class actions based on privacy violations or economic losses.

- ***MDMs should draft formal standard operating procedures (SOPs) to document the CVD policy.*** MDMs should create formal SOPs outlining the CVD policy so that critical process decisions are addressed prior to a vulnerability report, resulting in the efficient resolution of reported issues. Portions of the CVD policy may be incorporated into existing quality procedures for handling product complaints.

- ***Online portals can play a key role in the CVD process.*** Many MDMs use online portals to receive vulnerability reports from the public, including security researchers who specialize in identifying vulnerabilities. Portals should be easy to access, simple to use, and properly secured. The portal should clearly explain how to report a vulnerability and how information submitted on the portal will be used by the MDM, and should provide guidelines for submitter conduct and what the submitter can expect after a vulnerability is reported.

- ***Reported vulnerabilities should be assessed according to an established framework.*** It is essential that MDMs perform a thorough, well-documented assessment of each potential cybersecurity vulnerability reported to the MDM (whether through a portal or otherwise). Formal assessment is important not only to protect and enhance patient safety and to mitigate potential legal exposure, but also to maintain credibility with the healthcare and security research communities and government agencies, including FDA. This process should include a framework for efficiently validating the vulnerability and performing a security risk assessment (e.g., by using the Common Vulnerability Scoring System (CVSS) or a modified version developed for medical devices). MDMs also should have a process for assessing the vulnerability's potential impact on the safety and essential performance of the device and should consider whether the vulnerability may affect other similar devices.

- ***FDA and DHS are important collaboration partners.*** Both FDA and DHS NCCIC can be invaluable partners when considering the appropriate risk assessment, disclosure, and remediation related to a specific product vulnerability, even if regulations do not always require disclosure to the government. Stakeholders report positive experiences when interacting with both agencies.

MDMs may consider closely coordinating with the agencies early in the CVD process, particularly when a vulnerability may impact patient health. MDMs may also find it helpful to consult with FDA and/or DHS to determine whether a vulnerability should be publicly disclosed.

- ***How a vulnerability is disclosed carries both regulatory and strategic considerations.*** A CVD policy may require disclosure in certain circumstances or may allow a case-by-case assessment based on the specific situation. An MDM also may be required to disclose to certain parties, such as FDA, in certain situations.

    - FDA strongly encourages disclosure through DHS NCCIC (and/or an ISAO) regardless of the level of risk presented by the vulnerability. MDMs often choose to disclose vulnerabilities through DHS NCCIC for a variety of reasons, including security researcher expectations, FDA's encouragement of the process, and the collaborative nature of disclosure through DHS NCCIC. As a general rule, DHS will not issue an advisory without MDM input and consent as long as the MDM cooperates in the disclosure process.

    - MDMs should have an interim or long-term remediation plan in place prior to public disclosure, which may include solutions to remove a cybersecurity vulnerability from a medical device or compensating controls that mitigate the risk.

    - FDA may play a role in coordinating between stakeholders (e.g., the MDM, DHS NCCIC, the security researcher) to determine the appropriate timetable for public disclosure to ensure patient safety is not compromised by premature release of vulnerability information without first having in place a remediation plan or, at a minimum, mitigating measures to reduce the residual risk of patient harm to an acceptable level.

    - In addition to the MDM's disclosure, FDA may choose to issue a Safety Communication if a vulnerability presents a risk to public health. FDA coordinates with the MDM prior to issuance of a Safety Communication to ensure the communication is factually accurate and encourages the MDM to issue a concurrent communication to practitioners.

    - The MDM may conduct a voluntary recall of the device in cooperation with FDA to address safety concerns. FDA may strongly urge an MDM to conduct a recall in certain cases. A carefully conducted benefit-risk analysis is integral to a recall decision.

- ***Security Researchers should be treated with respect.*** Security researchers encourage MDMs to treat them as partners rather than adversaries and to communicate regularly with researchers during the coordinated disclosure process. Researchers can always choose to circumvent a company's coordinated disclosure process and instead report directly to DHS, FDA, and/or the public if they are unsatisfied with how the MDM handles and responds to reported vulnerabilities. In FDA's experience, security researchers in the medical device field are willing to work with the agency to ensure safety is not compromised and will understand if a disclosure should be delayed due to a safety concern.

IV. FDA Legal Obligations Supporting the Need for CVD Policies and Portals

As the primary regulatory authority for medical devices in the United States, in recent years FDA has emphasized the importance of medical device cybersecurity throughout the total product lifecycle. FDA has issued both premarket and postmarket guidance documents specifically related to the management of medical device cybersecurity, released multiple safety communications about cybersecurity risks related to specific medical devices on the market, and held extensive webinars and workshops to educate the public and to further collaboration with the medical device industry and ecosystem stakeholders. The agency's medical device cybersecurity initiatives are led by Suzanne Schwartz, M.D., M.B.A., Associate Director for Science and Strategic Partnerships at FDA's Center for Devices and Radiological Health (CDRH), and Seth Carmody, Ph.D., CDRH's Cybersecurity Program Manager.[6]

FDA encourages MDMs to establish CVD policies, including online portals, as part of a comprehensive cybersecurity risk management program. On December 28, 2016, FDA issued guidance titled *Postmarket Management of Cybersecurity in Medical Devices* (the "Postmarket Cybersecurity Guidance"),[7] intended to guide MDMs in identifying and handling cybersecurity vulnerabilities. The Postmarket Cybersecurity Guidance encourages MDMs to adopt CVD policies and practices, and to practice good cyber hygiene through regular risk review and reduction actions for marketed medical devices. The Postmarket Cybersecurity Guidance also emphasizes the necessity of industry collaboration to proactively address cybersecurity vulnerabilities and encourages MDMs to share risk information and intelligence through membership in an ISAO. The development of CVD policies is well aligned with FDA's "Case for Quality" initiative that supports the emerging trend toward proactive compliance focusing on continuous quality improvement, enhanced data transparency, and increased stakeholder engagement.[8]

FDA included the advancement of medical device cybersecurity in its 2018 *Medical Device Safety Action Plan* (the "Action Plan"). The Action Plan states that FDA plans to "[c]onsider new postmarket authority to require that firms adopt policies and procedures for coordinated disclosure of vulnerabilities as they are identified."[9] Although currently FDA only encourages the adoption of CVD policies through guidance, the agency's intention to seek authority to *require* such policies emphasizes the importance it ascribes to the coordinated disclosure process. FDA may also assess the premarket and postmarket management of medical device cybersecurity during facility inspections. It is therefore important that MDMs consider the adoption of CVD policies and practices if they have not already done so and draft formal SOPs to document their CVD policies.

The Action Plan also relays FDA's intent to explore the development of a CyberMed Safety (Expert) Analysis Board (CYMSAB), encompassing a broad range of expertise, to serve as a resource for MDMs

[6] Both Suzanne Schwartz and Seth Carmody have served in an advisory role to MDIC during the development of this report. FDA is a member organization in the MDIC public-private partnership.

[7] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf.

[8] *See* FDA, Case for Quality (2011), https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/MedicalDeviceQualityandCompliance/ucm378185.htm.

[9] FDA, *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health* 13 (2018), https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf.

and FDA by "assessing vulnerabilities, evaluating patient safety risks, adjudicating disputes, assessing proposed mitigations, serving as a consultative role to organizations navigating the coordinated disclosure process, and serving as a 'go team' that could be deployed in the field to investigate a suspected or confirmed device compromise at a manufacturer's or FDA's request."[10] The CYMSAB may therefore play an important role in future CVD practices by providing guidance and assistance to MDMs.

A. Cybersecurity Risk Management Programs and the Quality System Regulation

In the Postmarket Cybersecurity Guidance, FDA states that it is essential that MDMs implement comprehensive cybersecurity risk management programs and documentation consistent with the Quality System Regulation and current good manufacturing practices (CGMPs).[11] The critical components of such a program include:

- Monitoring cybersecurity information sources for identification and detection of cybersecurity vulnerabilities and risk (which may include the use of a portal and/or participation in an ISAO);
- Understanding, assessing, and detecting the presence and impact of a vulnerability;
- Establishing and communicating processes for vulnerability intake and handling;[12] and
- Adopting a CVD policy and practice (including processes for acknowledging receipt of the initial vulnerability report to the submitter).[13]

As part of an MDM's cybersecurity risk management program, FDA also recommends that MDMs incorporate elements consistent with the NIST Framework for Improving Critical Infrastructure Cybersecurity (i.e., "Identify, Protect, Detect, Respond, and Recover," addressed in more detail in Section X of this report).

B. Reporting Cybersecurity Vulnerabilities to FDA: Regulatory Overview

FDA urges MDMs to address cybersecurity during the design and development of medical devices as a first line of defense, by establishing a cybersecurity vulnerability risk management approach as part of the software validation and risk analysis required by the Quality System Regulation.[14] Even with the best

[10] *Id.*

[11] 21 CFR part 820.

[12] FDA has recognized ISO/IEC 30111:2013: *Information Technology – Security Techniques – Vulnerability Handling Processes* as a useful resource for MDMs.

[13] FDA has recognized ISO/IEC 29147:2014: *Information Technology – Security Techniques – Vulnerability Disclosure* as a useful resource for MDMs.

[14] 21 CFR Part 820; FDA, *Guidance for Industry and FDA Staff: Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Oct. 2, 2014). Premarket cybersecurity risk management is outside the scope of this report. The U.S. Department of Health & Human Services (HHS) Office of Inspector General (OIG) recently issued a report urging FDA to further integrate its review of cybersecurity into the premarket review process for medical devices. HHS OIG, *FDA Should Further Integrate Its Review of Cybersecurity Into the Premarket Review Process for Medical Devices* (Sept. 2018), https://oig.hhs.gov/oei/reports/oei-09-16-00220.pdf. In the report, OIG indicated that it is conducting an audit of FDA's plans and processes for responding to cybersecurity vulnerabilities affecting medical devices that are already on the market and that the results of this audit are forthcoming. *Id.* at 6.

preparation, it is expected that cybersecurity vulnerabilities will likely be identified during the often lengthy device lifecycle due to the dynamic nature of cyber threats. When an MDM becomes aware of a cybersecurity vulnerability, the MDM's obligations for reporting to FDA will depend in large part on the extent to which the vulnerability may pose a risk to human health and the severity of that risk.

1. Mandatory Medical Device Reporting

If the device may have caused or contributed to a death or serious injury, or has malfunctioned and the malfunction of the device or a similar device would be likely to cause or contribute to a death or serious injury if the malfunction were to recur, the MDM would be required under the Medical Device Reporting (MDR) Regulation to report the adverse event to FDA.[15] The MDR reporting process should already be in place through the MDM's quality program. Cybersecurity vulnerabilities that rise to this level of severity should be handled jointly by the quality and product security teams.

2. Reporting Medical Device Changes (Corrections and Removals)

Even if the MDM is not required to report the cybersecurity vulnerability as an adverse event, it still may need to report to FDA if it makes a change to the device to address the vulnerability. MDMs are generally required under 21 CFR part 806 to "report promptly to the [FDA] certain actions concerning device corrections and removals, and to maintain records of all corrections and removals regardless of whether such corrections and removals are required to be reported to FDA."[16]

For corrections and removals (such as software patches and updates) due to cybersecurity vulnerabilities, the situation is more nuanced. The Postmarket Cybersecurity Guidance addresses reporting requirements for cybersecurity vulnerabilities that have not caused or contributed to a death or serious injury (and thus are not addressed through the standard MDR reporting process for adverse events and serious product malfunctions). In the guidance, FDA acknowledges the burden of formal reports when issuing routine updates and patches for cybersecurity vulnerabilities and states that the vast majority of actions taken by manufacturers to address these cybersecurity vulnerabilities will not require a Part 806 report to FDA.

The Part 806 reporting requirement depends on whether the action is taken in response to a "controlled" or "uncontrolled" risk. The distinction between controlled and uncontrolled risk is based on an evaluation of the likelihood of exploitation, the impact of exploitation on the device's safety and essential performance, and the severity of patient harm if exploited. FDA expects MDMs to document their process for objectively and systematically assessing the cybersecurity risk and determining whether it is controlled or uncontrolled. FDA suggests using a matrix with combinations of "exploitability" and "severity of patient harm" to evaluate the risk, but acknowledges that in some cases the determination may not be entirely clear. The Postmarket Cybersecurity Guidance provides examples of controlled and uncontrolled risks.

Controlled risk is present when there is sufficiently low (acceptable) residual risk of patient harm due to a device's specific cybersecurity vulnerability. Device changes to address controlled cybersecurity risks, such as routine updates and patches, are generally considered to be device enhancements and not

[15] 21 CFR Part 803.

[16] 21 CFR 806.1(a).

corrections that would require reporting under Part 806.[17] In addition, device changes made solely to address a vulnerability that could lead to compromise of protected health information (PHI) are considered to be in the controlled risk category.

Uncontrolled risk is present when there is unacceptable residual risk of patient harm due to insufficient risk mitigations and compensating controls.[18] In the Postmarket Cybersecurity Guidance, FDA advises MDMs to remediate uncontrolled risk of patient harm to an acceptable level as quickly as possible and to implement mitigation and compensating controls when a fix is not feasible or immediately available. MDMs should also inform customers and the user community about the cybersecurity vulnerability, including steps they can take to mitigate the risk. FDA considers uncontrolled risks to require reporting under Part 806, but, in the Postmarket Cybersecurity Guidance, FDA said that it does not intend to enforce reporting requirements for a specific vulnerability when the following circumstances are met:

1) there are no known serious adverse events or deaths associated with the vulnerability;

2) as soon as possible but no later than 30 days after learning of the vulnerability, the MDM communicates with its customers and user community regarding the vulnerability, identifies interim compensating controls, and develops a remediation plan to bring the residual risk to an acceptable level;

3) as soon as possible but no later than 60 days after learning of the vulnerability, the MDM fixes the vulnerability, validates the change, and distributes the deployable fix to its customers and user community such that the residual risk is brought down to an acceptable level; and

4) the MDM actively participates as a member of an ISAO that shares vulnerabilities and threats that impact medical devices and provides the ISAO with any customer communications upon notification of its customers.[19]

FDA has indicated that, at least for now, DHS NCCIC can function as a proxy for an ISAO, as new ISAOs are presently being established. Accordingly, as long as an MDM reports a vulnerability to NCCIC, and

[17] If the device is a premarket approval (PMA) device with periodic reporting requirements under 21 CFR 814.84, the MDM should report information about cybersecurity vulnerabilities and associated changes to FDA in a periodic (annual) report.

[18] A cybersecurity compensating control is a safeguard or countermeasure deployed in lieu of, or in the absence of, controls designed into the device. These controls are external to the device design, configurable in the field, employed by a user, and provide supplementary or comparable cyber protection for a medical device. For example, if a third party could access the vulnerable device through an HDO's network, the compensating control might entail disconnecting the device from the network.

[19] FDA intends to consider the following in determining whether a manufacturer is an active participant in an ISAO: (1) the manufacturer is a member of an ISAO that shares vulnerabilities and threats that impact medical devices; (2) the ISAO has documented policies pertaining to participant agreements, business processes, operating procedures, and privacy protections; (3) the manufacturer shares vulnerability information with the ISAO, including any customer communications pertaining to cybersecurity vulnerabilities; and (4) the manufacturer has documented processes for assessing and responding to vulnerability and threat intelligence information received from the ISAO. This information should be traceable to medical device risk assessments, countermeasure solutions, and mitigations.

the vulnerability is publicized via a DHS ICS-CERT Advisory and an accompanying customer communication released by the MDM, FDA will treat the disclosure pursuant to the Postmarket Cybersecurity Guidance as if it were directed to an ISAO.

In the absence of remediation, FDA may consider a device with an uncontrolled risk of patient harm to have a reasonable probability of causing or contributing to serious adverse health consequences or death. Such a product therefore may be considered to be adulterated and/or misbranded, in violation of the Federal Food, Drug, and Cosmetic Act (FDCA), and subject to enforcement or other action.

C. FDA Safety Communications, Warning Letters, and Recalls

Two high-profile case studies illustrate the tools FDA can use when it responds to medical device cybersecurity vulnerabilities, which include:

Safety Communications: FDA may issue a Safety Communication if a vulnerability presents a risk to public health in order to ensure that healthcare providers, patients, and caregivers are adequately informed regarding the public health implications of the vulnerability along with essential remediation recommendations such as updates and patches. FDA will inform the MDM prior to issuance that it intends to issue a Safety Communication and will consult with the MDM to ensure the communication is factually accurate. FDA will also encourage the MDM to issue its own communication to healthcare practitioners simultaneously with a link to the FDA Safety Communication. DHS ICS-CERT Advisories are typically issued along with Safety Communications.

Warning Letters: Warning Letters are issued for violations of regulatory significance. Significant violations are those violations that may lead to enforcement action if not promptly and adequately corrected. A Warning Letter is the agency's principal means of achieving prompt voluntary compliance with the FDCA.

Recalls: A recall is ordinarily a voluntary action taken by a company to remove a defective device from the market and may be conducted on the company's own initiative or by FDA request. FDA's role in a recall is to oversee the company's strategy and assess the adequacy of the recall. FDA also has limited authority to issue a mandatory recall order in situations where an MDM refuses to conduct a voluntary recall, there is a public health risk, and other criteria are satisfied.[20]

1. FDA Public Health Action Case Study: Infusion Pump Systems Safety Communications

The first example of FDA action to address specific cybersecurity threats came on May 13, 2015, when FDA issued a Safety Communication addressing vulnerabilities in infusion pump systems. The computerized infusion pumps were designed for the continuous delivery of anesthetic or therapeutic drugs to the patient. The vulnerabilities had been first identified by a security researcher and could allegedly be exploited to remotely program the devices through an HDO's Ethernet or wireless network and result in the intentional over- or under-infusion of critical therapies. The Safety Communication stated that although FDA was not aware of any adverse events related to the alleged vulnerabilities, hospitals could reduce the risk of unauthorized access by taking a number of immediate actions such as

[20] 21 CFR Part 810.

isolating the devices from the hospital's wireless network. DHS ICS-CERT issued a similar advisory on the same day. The MDM responded by developing new versions of its infusion systems to mitigate the vulnerabilities.

On July 31, 2015, FDA issued a Safety Communication about similar vulnerabilities in a separate infusion system marketed by the same MDM.[21] FDA advised HDOs to stop using the identified infusion pump system and to transition to other systems. This was the first time FDA issued an advisory to discontinue the use of a medical device due to a cybersecurity vulnerability. The MDM had discontinued the manufacture and sale of the infusion system a month earlier, for reasons unrelated to the cybersecurity risk, and said it would work with customers to transition to other devices as quickly as possible. In the meantime, the MDM issued a software update to address the risk.

These Safety Communications demonstrate that FDA will not hesitate to act if it learns of vulnerabilities that have the potential of impacting public health. In addition, the multiple devices impacted by the vulnerabilities in this case underline the importance for MDMs of broadening vulnerability risk assessments to ensure that a vulnerability found in one device does not affect similar devices.

2. FDA Public Health Action Case Study: Implantable Cardiac Pacemaker Safety Communications, Recalls, and Warning Letter

The first FDA Warning Letter and medical device recalls related to a cybersecurity vulnerability came in 2017. These events were set in motion in August of the previous year, when the investment firm Muddy Waters Capital LLC ("Muddy Waters") published a report criticizing an MDM for allegedly failing to address cybersecurity flaws in its implantable cardiac pacemakers and the associated transmitter device. The transmitter device could wirelessly connect to a patient's pacemaker and send the data to the patient's physician. The Muddy Waters report alleged that this monitoring system could be exploited to cause the pacemaker to pace at a potentially dangerous rate or cause the pacemaker's battery to rapidly deplete.[22]

FDA launched an investigation of the alleged cybersecurity vulnerability shortly after Muddy Waters issued its report, leading to a Safety Communication issued on January 9, 2017.[23] DHS ICS-CERT issued an advisory the same day. The FDA Safety Communication was intended to inform patients, caregivers, and doctors about the cybersecurity risk and the available software patch (which would be applied automatically) intended to address and reduce the risk.

The story did not end there. On April 12, 2017, FDA issued a Warning Letter alleging adulteration due to nonconformity with CGMPs related to the mishandling of the cybersecurity vulnerabilities identified by Muddy Waters.[24] FDA concluded that the MDM failed to follow its own corrective and preventative

[21] https://web.archive.org/web/20161231151945/http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm?source=govdelivery&utm_medium=email&utm_source=govdelivery.

[22] http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/. The MDM filed a defamation lawsuit alleging that Muddy Waters intentionally disseminated false and misleading information about the pacemakers to lower the value of the stock and profit from the stock decline through short selling. Section VI of this report addresses the litigation in greater detail.

[23] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm.

[24] https://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2017/ucm552687.htm.

action (CAPA) procedures when evaluating the Muddy Waters report and that the company "did not confirm all required corrective and preventive actions were completed, including a full root cause investigation and the identification of actions to correct and prevent recurrence of potential cybersecurity vulnerabilities" and "did not confirm that verification or validation activities for the corrective actions had been completed, to ensure the corrective actions were effective and did not adversely affect the finished device."[25]

In August 2017, the MDM recalled 465,000 pacemakers in a continued effort to mitigate the risk. At the same time, FDA issued another Safety Communication about an approved firmware update to reduce the risk of patient harm through third party access to the pacemaker.[26] "Firmware" is a specific type of software embedded in the hardware of the pacemaker itself. FDA recommended that patients and healthcare providers "discuss the risks and benefits of the cybersecurity vulnerabilities and the associated firmware update designed to address such vulnerabilities at their next regularly scheduled visit."[27] The update would require an in-person visit with a health care provider and FDA warned of a very low risk of an update malfunction during the process. FDA advised that healthcare providers determine if an update is appropriate for the given patient based on the potential benefits and risks. An additional recall and accompanying Safety Communication were issued on April 11, 2018, to announce a firmware update to address similar vulnerabilities in different implantable cardiac devices.[28]

These events, including the Warning Letter and the multiple recalls and Safety Communications, demonstrate the need to perform a thorough assessment of each reported vulnerability; to create and follow policies and procedures related to vulnerability intake, risk assessment, and coordinated disclosure; to consider other devices that may also be subject to the reported vulnerability (known as conducting a variant analysis); and to coordinate closely with FDA when the vulnerability may raise a significant safety risk.

V. Role of an ISAO

ISAOs are an important resource for MDMs. ISAOs are self-organized groups that have been established to gather, analyze, and disseminate cyber threat information among communities of interest that may include participants from multiple sectors. In addition to companies in a given sector, ISAO membership can include constituents such as legal, accounting, and consulting firms that support cross-sector clients.[29] FDA encourages the use of medical device ISAOs to share information on cybersecurity threats and vulnerabilities "that may affect the safety, effectiveness, integrity, and security of the medical devices and the surrounding Health IT infrastructure."[30] In addition to collecting and disseminating vulnerability information, ISAOs may offer other benefits such as the sharing of best practices among MDMs.

---

[25] *Id.*

[26] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm.

[27] *Id.*

[28] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm.

[29] Two of the Debevoise attorneys who worked on this report, Luke Dembosky and Jeremy Feigelson, also served as co-chairs of the ISAO Standards Organization's Governance Working Group.

[30] Postmarket Cybersecurity Guidance at 7.

In the Postmarket Cybersecurity Guidance addressed above, FDA strongly encourages industry collaboration to address cybersecurity vulnerabilities. Indeed, sharing risk information and intelligence is deemed to be "critical to the adoption of a proactive, rather than reactive, postmarket approach."[31]

FDA considers participation in an ISAO "a critical component of [an MDM's] comprehensive proactive approach to management of postmarket cybersecurity threats and vulnerabilities and a significant step towards assuring the ongoing safety and effectiveness of marketed medical devices."[32] It is anticipated that additional medical device ISAOs will be announced in the near future, as current options are limited.[33]

VI. Other Legal and Commercial Considerations Supporting the Need for Effective Cybersecurity Practices

For MDMs, developing cybersecurity portals and taking other steps to address and remediate cybersecurity vulnerabilities is not only important from an operational perspective, but also can minimize the legal and commercial risks that may arise as a result of the identification of significant cybersecurity vulnerabilities or, worse yet, actual cyber attacks.

This section of the report addresses select areas of potential legal liability that may arise from the failure to become aware of, and/or the failure to appropriately address, potential cybersecurity vulnerabilities. While the theories of liability addressed below may be raised by private plaintiffs, government regulators, and/ or prosecutors, whether those theories are successful will depend on a variety of factors including the specific circumstances of the case and case law in the applicable jurisdiction.

A. Product Liability

If a medical device cybersecurity vulnerability allegedly causes bodily harm, the victim may bring product liability claims against the MDM (and potentially other entities in the medical device ecosystem). Depending on the circumstances, plaintiffs would likely pursue one or more of three types of product liability claims: negligence, strict liability, and/or breach of warranty. A plaintiff's claims could be based on the design or operation of the device, failure to provide appropriate warnings about the risk of a cybersecurity vulnerability, or failure to appropriately monitor for the existence of vulnerabilities and appropriately address them once identified.

Negligence

A negligence claim can be made where a manufacturer fails to exercise a duty of care in the design or manufacture of the product. In the case of a cybersecurity vulnerability, a plaintiff may also argue that the manufacturer has an obligation to implement post-sale processes to monitor for potential

[31] Postmarket Cybersecurity Guidance at 7.

[32] *Id.* at 8.

[33] In October 2016, the FDA entered into a Memorandum of Understanding (MOU) with the National Health Information Sharing and Analysis Center (NH-ISAC) and the Medical Device Innovation, Safety, and Security Consortium (MDISS). The NH-ISAC serves as the central hub for threat and vulnerability information sharing across the healthcare and public health sector of critical infrastructure. The NH-ISAC-MDISS collaborative ISAO is currently the only medical device ISAO established via an MOU with FDA.

cybersecurity vulnerabilities and develop countermeasures for any vulnerabilities that had been identified. One of the key questions in the negligence analysis is whether the manufacturer acted reasonably. What counts as "reasonable" may evolve over time (depending on the circumstances), and may be influenced by what standards emerge in the relevant industry. A plaintiff might argue, for example, that an error in a device's computer code left it dangerously vulnerable to a cyber attack, that an MDM should have taken steps to avert a foreseeable attack by a hacker, or that a MDM knew of a cybersecurity risk and failed to provide appropriate warnings about that risk. As CVD policies and practices become more widespread in the device industry, some courts may conclude that these practices are (depending on the circumstances) necessary for the exercise of reasonable care.

Strict Liability

In general, a strict liability claim can be brought against an MDM if a device is "unreasonably dangerous" without regard to whether the MDM acted negligently. Unreasonable danger is generally defined as being more dangerous than what an ordinary consumer would expect.[34] A plaintiff may argue that a device was unreasonably dangerous if it were particularly susceptible to a cybersecurity vulnerability that could affect the operation of the device in ways that could endanger the life or health of a patient (e.g., an implantable cardioverter defibrillator that was vulnerable to a cyber attack that caused it to deliver large shocks at the inappropriate time). A plaintiff may also argue that a device was unreasonably dangerous if it were not accompanied by appropriate warnings regarding the risk of a cybersecurity vulnerability.

Breach of Warranty

Breach of warranty claims may be brought where a manufacturer fails to adhere to product warranties (as broadly defined).[35] Such warranties can be express, for example, where a manufacturer advertises that its device is "secure." Plaintiffs may also argue that a product has an "implied" warranty that it is, for example, "fit for a particular purpose." The issue of warranties may become increasingly significant to the extent that MDMs face commercial pressure to make assurances regarding cybersecurity.

Product Liability Defenses

MDMs are likely to have a variety of avenues to defend against product liability claims arising out of a cybersecurity vulnerability. As an initial matter, preemption may limit liability in certain circumstances. The Medical Device Amendments of 1976[36] preempts any state law that places different or additional requirements on devices subject to federal regulation (typically limited to Class III medical devices approved by FDA via the premarket approval, or PMA, process). If a claim is preempted, it must be dismissed. For example, claims have been preempted when premised on a manufacturer making a

[34] *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 402A (AM. LAW. INST. 1965); RESTATEMENT (THIRD) OF TORTS § 2(b) cmt. g (Am. Law. Inst. 1998).

[35] The Federal Trade Commission regulates "consumer product" warranties via the Magnuson-Moss Warranty Act (MMWA). Although most medical devices posing cybersecurity vulnerabilities do not come within the "consumer product" definition, the MMWA may provide helpful guidance when formulating clear and effective product warranties.

[36] 21 U.S.C. § 360c *et seq*. (2016).

misstatement to the FDA, or where the plaintiff claimed that the device failed to satisfy standards that were not required by federal law.[37]

Preemption does not completely foreclose product liability with respect to medical devices. Preemption will not apply, for example, where state law claims are premised on a manufacturer failing to manufacture devices in accordance with FDA standards (e.g., "manufacturing defect"),[38] or where a device is not subject to device-specific federal regulations.[39] In addition, preemption does not apply to Class I or Class II devices that are either exempt from FDA premarket review or solely subject to 510(k) clearance by FDA.

MDMs may also have defenses that are unique to harm resulting from a cybersecurity vulnerability. Unlike the typical product liability case where a product failure is alleged to be the result of an error by the manufacturer, here the resulting harm may be caused by intervening, intentional criminal conduct by a nefarious and sophisticated third party. MDMs may be able to argue, depending on the circumstances, that they could not and should not be held responsible for failure to prevent such harm. The success of this argument likely will depend largely on the circumstances regarding the vulnerability at issue. For example, this argument may be more persuasive in the case of a new or "zero day" vulnerability (one for which there was not yet a known digital "signature" allowing it to be readily detected), versus situations involving a known vulnerability that the MDM failed to test for and address. Many additional defenses may also be available but are beyond the scope of this report.

B. Securities Fraud Claims Against Publicly Traded Companies

In February 2018, the SEC issued detailed guidance regarding cybersecurity-related disclosure obligations for publicly-traded companies.[40]

As noted in the SEC's guidance, cybersecurity vulnerabilities may have a significant financial impact on MDMs. This may range from the cost of developing and implementing emergency countermeasures to the erosion of market share due to reputational damage. For publicly traded MDMs, these developments could have a negative impact on the company's stock price. While these cybersecurity risks exist with respect to any networked product, the risk for MDMs is magnified because a device failure caused by a cybersecurity vulnerability could result in bodily harm.

The SEC emphasized the importance of disclosure regarding a company's assessment of material cybersecurity risks: "It is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyber-attack."[41] In assessing disclosure obligations, companies should consider "the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of

[37] *See, e.g., Buckman Co. v. Plaintiffs' Legal Committee*, 531 U.S. 341 (2001); *Riegel v. Medtronic, Inc.*, 552 U.S. 312 (2008).

[38] *Bass v. Stryker Corp.*, 669 F.3d 501 (5th Cir. 2012).

[39] *Redd v. DePuy Orthopaedics*, 48 F.Supp.3d 1261 (E.D. Mo. 2014).

[40] Comm'n Statement and Guidance on Public Co. Cybersecurity Disclosures, 83 FR 8166 (Feb. 26, 2018), https://www.sec.gov/rules/interp/2018/33-10459.pdf.

[41] *Id*. at 8167.

the incident on company compliance."[42] The SEC further made clear that boilerplate disclosure statements in the company's periodic filings are no longer sufficient, meaning that actual cyber events the company has encountered may not be presented as hypothetical risks.[43] The SEC recognized, however, that any disclosure need not be at a level of detail that would compromise a company's cybersecurity efforts by providing a roadmap to cyber attackers who seek to exploit the vulnerabilities.[44]

The SEC also stated that a company should establish "disclosure controls and procedures that provide an appropriate method of discerning the impact that [cybersecurity risks] may have on the company and its business."[45] Moreover, "the development of effective disclosure controls and procedures is best achieved when a company's directors, officers, and other persons responsible for developing and overseeing such controls and procedures are informed about the cybersecurity risks and incidents that the company has faced or is likely to face."[46]

The SEC has taken enforcement actions against companies arising from inadequate cybersecurity. For example, in April 2018, a technology company paid a $35 million penalty because it allegedly misled investors by failing to disclose—for two years—the existence of a data breach that affected 500 million customers.[47] The SEC also faulted the company for failing to have controls and procedures in place to assess its cybersecurity disclosure obligations.[48]

The establishment of a cybersecurity portal and implementation of a CVD policy should be integrated with the disclosure controls addressed by the SEC. An MDM that performs a thorough assessment of cybersecurity threats will be far better positioned to make accurate disclosures to the public regarding applicable risks.

In light of SEC cybersecurity guidance and enforcement actions, SEC-regulated MDMs thus should regularly assess their actual material cyber risks and update their disclosures accordingly; ensure that information about potentially material vulnerabilities and incidents are immediately relayed to appropriate corporate officials to assess materiality; and conduct investigations of reported vulnerabilities so that any required disclosures can be made in a timely manner.

The SEC cybersecurity guidance document contains a warning against insider trading on the basis of cybersecurity matters that constitute material non-public information.[49] As part of an assessment of the materiality of cybersecurity vulnerabilities and incidents, MDMs should consider whether a temporary trading freeze is warranted for those in possession of such information. Failure to avoid trading on this basis may result both in SEC enforcement and criminal prosecution.

---

[42] *Id*.

[43] *Id.* at 8169.

[44] *Id*.

[45] *Id*. at 8167.

[46] *Id.*

[47] Altaba, Inc., Exchange Act Release No. 83096, 2018 WL 1919547 (Apr. 24, 2018).

[48] *Id*. at *5.

[49] Guidance on Public Co. Cybersecurity Disclosures, *supra* note 40 at 8171-72.

C. Federal Criminal Enforcement

DOJ has launched a number of criminal investigations when product manufacturers (including FDA-regulated companies) were alleged to have sold products that caused significant bodily harm.[50]

DOJ may investigate an MDM based upon a cybersecurity vulnerability, particularly one that causes patient injury or death, and may bring a criminal action against an MDM or its executives on the theory that a serious cybersecurity vulnerability rendered its devices misbranded or adulterated (as those terms are defined by the FDCA). DOJ may argue that a company or its responsible corporate officers committed a strict liability misdemeanor simply by selling a misbranded or adulterated device.[51] If DOJ believes that a company knowingly sold a misbranded or adulterated device, it could seek a felony conviction under the FDCA.

Alternatively, DOJ may bring a criminal action under the federal mail or wire fraud statutes. In prior investigations involving companies regulated by the FDA and other product manufacturers, DOJ has carefully examined representations made by the product manufacturer to either corporate customers or the ultimate purchasers. DOJ analyzed whether there were discrepancies between the company's representations and its internal knowledge and practices. DOJ has taken the position that companies can be charged with mail or wire fraud if a company knowingly deceived a customer or purchaser regarding the characteristics of the product it was selling. DOJ has made this argument in situations where a company represented that its drug was an effective treatment for a certain disease, when in fact the clinical trial had failed.[52] DOJ may similarly attempt to argue that an MDM committed fraud by touting the safety of its device at a time when it knew about a significant vulnerability but did not adopt appropriate countermeasures.

It therefore is imperative that a device company carefully scrutinize its statements to customers and the public regarding cybersecurity risks. Manufacturers of networked devices in particular may seek to avoid making unqualified representations about their devices being invulnerable to cybersecurity attacks or employing state-of-the-art practices to minimize vulnerabilities.

D. Privacy and Data Breaches

Cyber attackers may target medical devices to, among other things, steal PHI either directly from medical devices that store such data or use devices as a vector to access a provider's entire network of patient data. PHI is an attractive target for cyber attackers because it typically commands a greater black-market price than financial data. MDMs may be subject to various types of enforcement and other civil actions if device vulnerabilities result in patient data being compromised.

---

[50] *See, e.g.*, Press Release, U.S. Dep't. of Justice, Former Peanut Company President Receives Largest Criminal Sentence in Food Safety Case (Sept. 21, 2015); Press Release, U.S. Dep't. of Justice, Manhattan U.S. Attorney Announces Criminal Charges Against General Motors and Deferred Prosecution Agreement With $900 Million Forfeiture (Sept. 17, 2015); Press Release, U.S. Dep't. of Justice, New Jersey Medical Device Manufacturer Admits Selling Contaminated Ultrasound Gel (July 6, 2016).

[51] *See United States v. Park*, 421 U.S. 658 (1975); *United States v. Dotterweich*, 320 U.S. 277 (1943).

[52] Press Release, U.S. Dep't of Justice, Former InterMune CEO Sentenced for False & Misleading Statements Related to Pulmonary Fibrosis Drug's Clinical Tests (Apr. 14, 2011).

HIPAA Enforcement

Data breaches that result in personal health data being stolen may result in the Department of Health and Human Services (HHS) bringing an action under HIPAA, which requires entities to protect against "any reasonably anticipated impermissible uses and disclosures."[53]

Covered entities and business associates under HIPAA face significant liability should they fail to properly secure PHI. For example, in June 2018, a hospital whose inadequate privacy measures resulted in a series of breaches involving more than 33,000 patient records was ordered to pay more than $4 million.[54] A major healthcare provider was fined $2.3 million after it experienced a breach in which more than two million patient records were compromised. In the resolution agreement between the entity and HHS, HHS found that the entity "failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level."[55]

State Attorney General Enforcement

State attorneys general have vigorously enforced state consumer protection laws and other state laws related to privacy and cybersecurity. In Massachusetts, the Attorney General reached a settlement with a medical center after the PHI of nearly 4,000 patients was lost on a stolen laptop.[56] The New Jersey Attorney General's office reached a settlement with a health network after the records of more than 1,650 patients were compromised as a result of a subcontractor accidentally removing password protections while accessing a file sharing site.[57] While both cases were examples of human error and not malicious intrusions, they demonstrate that state officials may pursue claims against MDMs should vulnerable medical devices lead to data breaches.

FTC Enforcement

The FTC is closely monitoring the privacy and cybersecurity practices of healthcare companies.[58] The FTC is authorized to bring enforcement actions against unfair and deceptive acts and practices[59] and has been proactive in its use of those powers in response to privacy and cybersecurity matters.

An FTC official recently reiterated the FTC's position that a "failure to have taken reasonable security measures . . . can constitute an unfair practice under the FTC Act."[60] What is reasonable "will depend on

[53] 45 C.F.R. § 164.306(a) (2017).

[54] *See* Univ. of Tex. MD Anderson Cancer Center, DAB *CR5111* at 9 (2018) ("Respondent failed to comply with regulatory requirements because it failed to adopt an effective mechanism to protect its ePHI.").

[55] 21st Century Oncology, Inc., Resolution Agreement (2017), *available at* https://www.hhs.gov/sites/default/files/21co-ra_cap.pdf.

[56] Press Release, Mass. Office of Att'y Gen., Beth Israel Deaconess Medical Center to Pay $100,000 Over Data Breach Allegations (Nov. 21, 2014).

[57] Press Release, N.J. Office of Att'y Gen., Virtua Medical Group Agrees to Pay Nearly $418,000, Tighten Data Security to Settle Allegations of Privacy Lapses Concerning Medical Treatment Files of Patients (Apr. 4, 2018).

[58] Thomas Pahl, *Cybersecurity & the Healthcare Industry: The FTC's Tools for Tackling New Threats* (Mar. 29, 2017).

[59] 15 U.S.C. § 45(a)(1),(2).

[60] Pahl, Cybersecurity & the Healthcare Industry, *supra* note 58, at 3.

a number of factors, including the size and complexity of a company's operations, the amount and sensitivity of data it collects, and the availability of low-cost tools to mitigate threats."[61] To avoid FTC enforcement actions premised upon "deception" rather than "unfairness," MDMs should not "misrepresent the level of security [they] provide," which could constitute a deceptive practice.[62] MDMs should also "protect against well-known, foreseeable threats" to forestall the chance of FTC enforcement.[63]

The FTC has brought several enforcement actions against manufacturers of networked devices related to cybersecurity issues. One such action involved a manufacturer of networked baby monitoring cameras that advertised that its products were "secure."[64] The FTC argued that the company engaged in unfair and deceptive practices because there was a software problem that allowed anyone with the camera's Internet address to view or listen to the camera's feed. The FTC criticized the manufacturer for "fail[ing] to implement a process to actively monitor security vulnerability reports . . . thereby delaying the opportunity to correct discovered vulnerabilities or respond to incidents."[65] The FTC and the manufacturer ultimately reached a settlement, pursuant to which the company was required to establish a comprehensive cybersecurity program and to have it audited by a third party every two years.[66] Based upon a recent decision by the 11th Circuit, the FTC may need to pursue detailed data security requirements in FTC orders as ambiguous requirements may be deemed unenforceable.[67]

There have been some indications that, in practical terms, the FTC may defer to FDA on cybersecurity matters affecting medical devices (particularly for matters premised on "unfairness" rather than "deception"). It remains the case that the FTC appears to have the legal authority to pursue such matters, so its views on cybersecurity are appropriately taken into account by MDMs. Further assessment of the FTC's legal authority over data breaches and cybersecurity vulnerabilities is beyond the scope of this report.

E. Class Actions Based on Economic Losses

MDMs may also face the risk of class action lawsuits brought by purchasers of medical devices (including patients and HDOs) who claim they have suffered economic losses either because of reports that the devices they purchased are subject to cybersecurity vulnerabilities or because of actual cybersecurity exploits. Such plaintiffs would allege that the vulnerabilities caused the value of their devices to decrease.

Plaintiffs may seek to use the following class action complaints as templates in litigation against MDMs.

---

[61] *Id*. at 3.

[62] *Id.* at 7.

[63] *Id.*

[64] TRENDnet, Inc., 122 F.T.C. 2090 (2014).

[65] *Id*. at 4.

[66] Press Release, F.T.C., FTC Approves Final Order Settling Charges Against TRENDnet, Inc. (2014).

[67] *LabMD, Inc. v. F.T.C.*, 891 F.3d 1286 (11th Cir. 2018).

Complaint Arising Out of the Muddy Waters Allegations

Thus far, there has been one high-profile example of litigation resulting from a medical device's reported cybersecurity vulnerability. In August 2016, a class of purchasers sued an MDM based upon purported vulnerabilities associated with its medical devices. This complaint was brought the day after Muddy Waters, a short seller, published a report detailing vulnerabilities it claimed were present in the MDM's pacemakers and other implantable medical devices.

The plaintiffs' core allegation was that the devices they purchased were worth less than what they paid as a result of the cybersecurity vulnerabilities.[68] The complaint relied heavily on alleged representations made by the MDM, including that the device transmitted data securely; that remote monitoring would not affect the device's performance; that the device was protected with industry-standard safety protocols; and that the MDM used the first medical device network to have received an ISO 27001 certification, "a stringent worldwide information security standard."[69]

The plaintiffs alleged that these representations were false and that the devices "lacked even the most basic security defenses . . . that are used by other cardiac device manufacturers," as demonstrated by the Muddy Waters report that alleged at least three ways to infiltrate the devices.[70] The plaintiffs ultimately declined to pursue this litigation and the matter was voluntarily dismissed not long after it was filed.

Complaints Arising Out of Reported Cybersecurity Vulnerabilities

Lawsuits filed against the automobile industry provide instructive examples of the type of lawsuits that may be filed against MDMs as a result of a device cybersecurity vulnerability. Several lawsuits were filed after the publication of a 2015 WIRED article outlining cybersecurity risks in vehicles.[71] In one case, plaintiffs sued the manufacturer of an "infotainment" system that was installed in some vehicles.[72] Vulnerabilities in the system, plaintiffs alleged, could result in hackers compromising critical and non-critical vehicle systems. Although the court has dismissed the plaintiffs' fraud claims, it has permitted the plaintiff to proceed with claims that the vehicles were defective and certified a class with regard to some of the plaintiffs' claims.[73] As of this writing, the case is ongoing. The plaintiffs' success in certifying a class may encourage other plaintiff counsel to consider bringing class actions against manufacturers of networked products based on alleged cybersecurity vulnerabilities.

[68] Complaint, *Ross v. St. Jude Medical*, 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016).

[69] *Id.* at 22.

[70] *Id*.

[71] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me In It*, WIRED (July 21, 2015, 6:00 AM), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[72] *Flynn v. FCA US LLC,* No. 15-cv-0855-MJR-DGW, 2018 WL 3303267 (S.D. Ill. July 5, 2018).

[73] *Id*. at *5.

F. Class Actions Based on Compromised Patient Data

MDMs are also at risk of class action lawsuits if cybersecurity vulnerabilities result in hackers gaining access to patient data that is stored on devices or if hackers can use devices as a vector to gain access to patient data stored on hospital networks.

High profile cybersecurity breaches outside the MDM context have resulted in class action lawsuits filed by customers who alleged harm because their data were compromised. Such actions have typically been based on a variety of theories, including unfair business practices (the failure to employ proper cybersecurity being an improper practice), deceptive business practices (the company deceived its customers by promoting its cybersecurity practices when they in fact were inadequate) or common law negligence, strict liability, or breach of warranty (the company owed a duty to the consumer to maintain proper cybersecurity and breached that duty, breached a warranty, or otherwise sold a defective device).

One of the key challenges confronted by plaintiffs who file suit after a security breach is establishing that they were harmed by the company's conduct. In cases where plaintiffs cannot provide concrete evidence of actual or imminent harm, the cases may be dismissed for lack of standing.[74] In some cases, courts have found that allegations that plaintiffs were injured by identity theft, or that they were forced to spend time safeguarding their finances, were too speculative to establish standing.[75] Plaintiffs in post-breach litigation have successfully established standing in cases where the companies violated contractual promises that they made[76]; violated federal laws such as the Fair Credit Reporting Act[77]; and where there was a substantial risk of harm because a breach allegedly exposed valuable data.[78]

In some cases, plaintiffs who successfully established standing have negotiated large, class-wide settlements. For example, a class action alleging that a health insurer's improper practices resulted in the PHI of approximately 80 million people being compromised was settled for $115 million.[79] In another case, a dating website for married individuals settled a class action for $11.2 million after a cybersecurity breach revealed the names of subscribers to the website.[80] That company also reached a $1.66 million settlement with the FTC.[81]

---

[74] *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)) (emphasis removed).

[75] *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017); *Whalen v. Michaels Stores, Inc.*, 689 F.Appx. 89 (2nd Cir. 2017).

[76] *Kuhns v. Scottrade, Inc.*, 868 F.3d 711 (8th Cir. 2017).

[77] *In re Horizon Healthcare Services Inc. Data Breach Litigation,* 846 F.3d 625 (3d Cir. 2017).

[78] *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

[79] *In re Anthem Data Breach Litigation*, 162 F.Supp.3d (N.D. Cal. 2016); Brendan Pierson, *Anthem to pay record $115 mln to settle U.S. lawsuits over data breach*, REUTERS (Jun. 23, 2017 6:38 pm), https://www.reuters.com/article/anthem-cyber-settlement/anthem-to-pay-record-115-mln-to-settle-u-s-lawsuits-over-data-breach-idUSL1N1JK1WV.

[80] Jonathan Stempel, *Ashley Madison parent in $11.2 million settlement over data breach*, REUTERS (July 14, 2017 5:29pm), https://www.reuters.com/article/us-ashleymadison-settlement-idUSKBN19Z2F0.

[81] *Id*.

G. Risk of Ransomware and Other Disruptive Attacks

Disruptive cyber attacks are on the rise, with ransomware and similar cyber extortion schemes being the most notable variant. A company would face a uniquely challenging situation if it was subject to a ransomware attack in which a hacker infiltrated the software of life-saving devices and threatened to disable them or alter their performance if a ransom were not paid. In typical cyber extortion cases, the attacker is able to provide proof of the potential data they are threatening to release if they are not paid or, in the case of ransomware, it is readily apparent to the victim company that they are truly at risk of damage because they have already been locked out of their files. In a situation in which an attacker claims to be able to issue a command to alter or disrupt operation of medical devices, the company would certainly hesitate to ask for proof of this capability unless it is clear that doing so will not involve risk to a patient or the healthcare delivery system.

These complications make the use of a CVD policy all the more important to try to identify vulnerabilities before an attacker does and to fix them in a timely manner. Although beyond the scope of this report, MDMs may also benefit from drills designed to practice addressing these and other high-risk scenarios.

H. The Potential Risk of Litigation Should Not Dissuade MDMs From Disclosing Vulnerabilities

Some MDMs may be concerned that the disclosure of potential vulnerabilities may invite lawsuits that are similar to those described above. As a general rule, disclosure is preferable for a variety of reasons:

- The disclosure of vulnerabilities to FDA and other regulators may be required (see Section IV of this report).
- Failure to disclose a vulnerability could itself be actionable.
- A significant vulnerability is likely to be publicly disclosed at some point by a third party, so it is preferable to self-disclose while concurrently providing mitigation advice.
- The risk of litigation can often be reduced, if not eliminated, by the timely development and implementation of a plan to remediate the vulnerability.
- In many cases, class actions may be dismissed because the plaintiffs will be unable to establish that the existence of a potential vulnerability has caused them to suffer actual or imminent harm.
- As MDMs increasingly adopt CVD policies and the disclosure of cybersecurity vulnerabilities becomes more common, any negative perception associated with vulnerability disclosure should be lessened as such disclosures are likely to be seen as part of a responsible continuous quality improvement and risk management system.

For all of the reasons discussed above, in ordinary circumstances the negative repercussions that flow from failure to disclose a cybersecurity vulnerability typically outweigh any risks of litigation arising out of the disclosure of the existence of a potential vulnerability. Of course, not all situations are the same and therefore should be assessed on a case-by-case basis.

I. Commercial Benefits to Developing Effective Cybersecurity Practices

For MDMs, the implementation of a cybersecurity portal and development of a CVD policy may not only reduce the risk of litigation, but it may also have important commercial benefits.

MDMs that can convince the marketplace that they have implemented effective cybersecurity practices are likely (all things equal) to have a competitive advantage in the marketplace over those MDMs that do little to address cybersecurity vulnerabilities. MDMs may be able to use periodic disclosures of vulnerabilities as a selling point to highlight their attentiveness to cybersecurity issues.

When a company is proactive about addressing security vulnerabilities, the chances that it will receive public criticism from FDA or legitimate security researchers should be diminished. The more diligent and collaborative the approach of MDMs in addressing these issues proactively, the more confidence they will inspire on the part of consumers, investors, regulators, lawmakers and other stakeholders.

VII. Developing an Internet-Based Portal for Receiving Medical Device Vulnerability Reports

Cybersecurity threats are constantly shifting and evolving. Having a reliable and trusted platform to collect information from security researchers, users, and other members of the public regarding potential threats to postmarket devices is thus a critical element in cybersecurity risk management. An Internet-based portal can be a powerful way of crowdsourcing vulnerability information.

In designing a vulnerability portal, MDMs should take the following into consideration:

- ***Accessibility.*** Vulnerability portals rely on voluntary reporting. Portals that are difficult to use may discourage those efforts or lead potential submitters to turn to the government or the public instead. Generally, an MDM should have a webpage dedicated to its portal.

- ***Security.*** Vulnerability portals by definition involve the collection of sensitive information. In addition, web portals may serve as potential gateways into an MDM's supporting systems. These portals thus make attractive targets for cybercriminals and need to be secured accordingly. While specific technical recommendations are outside the scope of this report, the list of issues to address should include:

    - *User authentication protocols and access logs:* Hackers will probe for weaknesses related to password complexity, password recovery and reset, account lockout features, and other fundamental technical aspects of the site. More conservative security choices include a closed registration process in which users are required to pre-register and verify their identity to create an account, as well as use of complex password requirements and multi-factor authentication. The company should also monitor and preserve access logs and employ current anti-virus and malware protections. As with all public digital interfaces, security considerations must be balanced with usability and troubleshooting activities.

    - *Encrypted channels for communications:* All communications with a vulnerability reporter should occur over an encrypted channel, whether through the portal itself or otherwise, and this practice should continue even after the initial report has been made. The use of ubiquitous technologies such as secure file shares with virtual private network (VPN) services and/or multi-factor authentication to access them (and at a

minimum, use of hypertext transfer protocol secure or "https" for communications to and from the site) makes this relatively easy and inexpensive.

- *Robust data security for submitted information, including protocols for internal access:* There are multiple threat vectors to consider when providing public interfaces to private data. MDMs should operate in expectation of a breach and implement protective technologies to identify and prevent a successful attacker from gaining further access to the underlying stored data (or into any other company systems). In addition, the company should consider limiting internal access to the data received by adhering to the principle of least-privilege, or "role-based" access, to ensure that sensitive information is not disseminated throughout the organization unnecessarily.

- *Network security, including appropriate architecture and maintenance of anti-virus protection:* MDMs should anticipate that malicious files may be uploaded to the portal (avoiding anti-virus detection), and therefore segmentation from the rest of the network is essential. Because cybersecurity is never a one-off, static endeavor, the company should continuously monitor access to the portal (as well as the data submitted) and should periodically run penetration testing and vulnerability scans to identify potential weaknesses.

- ***Incentives.*** While not commonly used by MDMs, companies in other industries provide incentives for individuals who submit an actionable vulnerability. This may include monetary rewards (a "bug bounty") or public recognition. These strategies should be carefully evaluated prior to implementation, however, given their potential for incentivizing testing and disclosures by individuals with motivations other than patient safety. MDMs may consider consulting with both internal and external stakeholders before deciding whether the benefits of such incentives outweigh the risks.

The content on the portal webpage should be clear and thorough, and should include the following information and disclaimers:

- ***Scope of the CVD process.*** Portal webpages should communicate to the public which devices are included in the MDM's vulnerability reporting process.

- ***Guidelines for submitter conduct.*** Providing clear expectations for conduct by potential submitters and communicating which devices are included in the vulnerability reporting process will help ensure that no adverse events result from third-party testing. MDMs should caution individuals not to test devices that are actively in use or to take any steps that could potentially jeopardize patient safety. MDMs may also indicate that testing leading to unauthorized access to PHI is out of scope.

- ***How to submit information through secure channels.*** Many MDMs that currently offer a vulnerability reporting portal request that submissions be made through encrypted email. The portal webpage thus should include the MDM's PGP key, which submitters can use to encrypt their email in a way that can be decrypted by the MDM.

- ***What information to submit and not submit.*** MDMs need to specify the types of information required for them to respond appropriately to a submitted vulnerability, including:

- A high-level description of the vulnerability;
- The exact specifications for the device, such as version, model, and serial numbers;
- The computers, network connectivity, and firmware configurations in use when the vulnerability was discovered;
- A detailed description of the vulnerability, including a description of the exploit code, proof of concept, and sample packet capture as applicable;
- When and where the vulnerability was discovered;
- Known or suspected threats relating to the vulnerability;
- Whether the vulnerability is known to other parties or has been reported to government agencies; and
- The contact information for the security researcher, if they wish to share it.

As mentioned above, MDMs should actively discourage submitting any information that contains personally identifiable or protected health information.

- ***How the MDM may use information provided by submitters.*** It should be transparent to submitters how the information they submit will be used and what that means for them:
  - The information submitted is non-proprietary and non-confidential;
  - The MDM may use the information in any way it deems appropriate; and
  - Submitting information through the portal does not create any rights for the submitter nor any obligations for the MDM.

- ***What the submitter can expect once a vulnerability is reported.*** MDMs should also provide:
  - A description of the structures and processes the MDM will follow in order to ensure appropriate analysis and action in response to the reported vulnerability.
  - An estimated timeline for the analysis and any necessary response to vulnerabilities identified through the portal; and
  - Any expected communication between the MDM and the submitter, including how the submitter may be updated on the investigation's progress.

Below is an anonymized chart comparing the information provided on the portal webpages of a number of MDMs:

	Scope of its coordinated disclosure process	Guidelines for submitter conduct	How to send vulnerability notifications through secure channels	What information to submit	How the MDM may use information provided by submitters	What the submitter can expect once a vulnerability is reported
Company A	X	X	X	X	X	X
Company B				X		X
Company C		X	X	X	X	X
Company D	X	X	X	X		X
Company E	X	X	X	X	X	X
Company F		X	X	X	X	X
Company G		X	X	X	X	X
Company H		X	X	X		X
Company I	X	X	X	X	X	X

	Scope of its coordinated disclosure process	Guidelines for submitter conduct	How to send vulnerability notifications through secure channels	What information to submit	How the MDM may use information provided by submitters	What the submitter can expect once a vulnerability is reported
Company J	X	X	X	X	X	X
Company K				X		X
Company L				X		X
Company M		X			X	
Company N	X	X	X	X	X	X
Company O				X		
Company P	X	X	X	X		X
Company Q		X	X	X		X

VIII. Best Practices from Interviews

We interviewed FDA officials, MDMs, representatives of a medical device trade association, and security researchers to identify best practices for the implementation of a CVD policy. Although the interviewees have different perspectives regarding product security and coordinated disclosure, and the MDMs' approaches and policies differ in certain ways, we discovered many common attributes associated with a successful CVD policy. Best practices gleaned from our stakeholder interviews are identified below.

A. A Corporate Culture that Recognizes the Importance of Product Security.

MDM interviewees that have successfully implemented CVD policies emphasized the importance of strong support from the C-Suite and across functions, including legal, regulatory, quality, public relations, and marketing. Some product security teams have used highly visible security incidents, such as the Wannacry and NotPetya ransomware attacks in 2017, to create a sense of urgency around cybersecurity and to promote cross-functional buy-in at their organizations.

Establishing in-house training and regular communications with employees regarding product security has also been useful in maintaining awareness, educating employees about current product security efforts, and encouraging the prompt reporting of any issues that arise. In-house training can also ensure that MDM employees are aware of procedures in a crisis situation. When issues arise, the product security team may need to play a central role, and ongoing outreach within the organization, before any incident occurs, can ensure that the product security team's authority will be accepted. These lines of communication can be strengthened if the product security team proactively positions itself during day-to-day operations as a resource for other functions.

B. A Properly Structured and Supported Product Security Team.

Product security teams are often centralized within the corporate structure rather than distributed across business units. A centralized structure bolsters communication, coordination, and the maintenance of institutional knowledge and helps prevent the duplication of security efforts across the organization. This allows vulnerabilities to be assessed and knowledge to be shared at an enterprise level rather than limited to specific business units, thus increasing the efficiency of the disclosure and remediation process. Many MDM interviewees reported that it is helpful to establish a direct reporting

channel from product security to the C-Suite, as well as regularly scheduled updates to the board of directors. In addition, it may be optimal to maintain a separate budget for product security apart from individual business units, providing independence and fewer budgetary constraints.

Many MDM interviewees report that it is helpful for the product security team to be distinct from the information security team and operationally adjacent to the R&D team, to facilitate "security by design" (i.e., building cybersecurity into the design process).

MDMs may also ensure coordination between the product security and quality teams by leveraging the organizational infrastructure already in place for FDA compliance. In certain circumstances, such as when patient safety is at risk, the quality team may need to lead or co-lead the remediation and disclosure efforts. The quality team may also provide the product security team with important insight by monitoring customer feedback regarding adverse events and security-related incidents.

C. A Premium on Strong Customer Relationships and a Reputation for Prioritizing Patient Safety.

It is important to maintain open lines of communication with customers regarding product security. If an MDM regularly communicates with customers about product security and demonstrates the priority it places on patient safety, notifications regarding cybersecurity vulnerabilities may be less alarming to the customer as they may be seen in a larger context. MDMs may consider providing routine updates on the company's cybersecurity efforts as further evidence that attention to these issues is ongoing. In certain situations, it may also be beneficial to inform customers about vulnerabilities prior to broader public disclosures. When product updates or patches are released, MDMs may need to educate customers on the need to download patches and update devices.

D. A Thorough, Well-Documented Assessment of Each Cybersecurity Vulnerability Reported to the MDM.

It is important to formally assess each vulnerability not only for patient safety and legal reasons, but also to maintain credibility with the healthcare and security research communities and government agencies, including FDA. Upon learning of a vulnerability, an MDM should have a process for efficiently validating the vulnerability and performing a risk assessment. The MDM should also have a process for escalating significant issues to senior management and/or the board where appropriate, as well as to other relevant departments within the company (e.g., the legal department or public relations).

Product engineers or other technical experts should lead the validation, risk evaluation, and remediation efforts. The MDM may use its existing safety risk assessment process and may consider involving a healthcare professional familiar with the device to provide context to properly assess the patient safety risk. The assessment process should include a plan for escalating high-impact vulnerabilities within the company. If a vulnerability may impact patient safety, the quality team should be notified and FDA compliance processes should be followed similar to the process for any other quality issue impacting patient safety.

MDMs should always operate with the assumption that following the disclosure of a significant vulnerability, the entire CVD process, including the risk assessment, may be closely examined and challenged by regulators, plaintiffs' lawyers, security researchers, the media, customers, and others.

After the MDM conducts the risk assessment, it should develop a remediation strategy according to protocols outlined in the CVD policy. The MDM should also assess whether the vulnerability could impact any other devices in its portfolio. The remediation plan should be fully tested prior to release, particularly if patient safety will be at risk should the device stop functioning.

E. A Clear Policy and Procedure for Proactively Disclosing Vulnerabilities.

A CVD policy may require disclosure in certain circumstances or may allow a case-by-case assessment based on the specific situation. In certain situations, an MDM may be required by law to disclose to certain parties, such as the FDA. Some MDM interviewees reported adopting a policy of disclosing all confirmed cybersecurity vulnerabilities to customers, the public (through DHS NCCIC, which releases ICS-CERT reports on Tuesdays and Thursdays), and/or FDA. A clear policy on disclosure, established in advance, may reduce the time an MDM needs to address a vulnerability because the decision-making process has been streamlined.

Interviewees reported that both FDA and DHS NCCIC can be invaluable partners when considering the appropriate risk assessment, disclosure, and mitigation related to a particular vulnerability, even if regulations do not always require disclosure to the government in a particular case. Interviewees reported positive experiences when interacting with both agencies and advise close coordination with the agencies early in the CVD process, particularly when a vulnerability may impact patient health. MDMs may also find it helpful to consult with FDA and/or DHS to determine whether a vulnerability should be publicly disclosed.

FDA strongly encourages public disclosure through DHS NCCIC (and/or an ISAO) regardless of the level of risk presented by the vulnerability.[82] MDMs often choose to disclose vulnerabilities through DHS NCCIC for a variety of reasons, including security researcher expectations, FDA's encouragement of the process, and the collaborative nature of the DHS NCCIC disclosure process. As a general rule, DHS will not issue an advisory without manufacturer input and consent as long as the manufacturer cooperates with the agency. DHS cautions manufacturers that if they are unresponsive or do not establish a reasonable timeframe for remediation, the agency may issue an advisory 45 days after the manufacturer is notified of the vulnerability regardless of the existence or availability of patches or workarounds.[83] Interviewees told us that it may be beneficial for an MDM to proactively draft a proposed DHS NCCIC disclosure. DHS often shares the draft disclosure with FDA and the security researcher (if applicable) prior to public release, and FDA may provide comments. In addition to public disclosure through a DHS ICS-CERT Advisory, MDMs may consider posting an advisory on the company website or, in certain high impact cases, issuing a press release. As noted, MDMs may choose to notify customers before issuing a public notice.

[82] As addressed in Section IV above, FDA requires uncontrolled risks to be reported under Part 806, but, in the Postmarket Cybersecurity Guidance, FDA indicated that it does not intend to enforce reporting requirements for a specific vulnerability if, among other things, the MDM actively participates in an ISAO. FDA has indicated that, at least for now, DHS NCCIC can function as a proxy for an ISAO. Accordingly, as long as an MDM reports a vulnerability to NCCIC, and the vulnerability is publicized, FDA will treat the disclosure pursuant to the Postmarket Cybersecurity Guidance as if it were directed to an ISAO. FDA encourages disclosure of controlled risks through DHS NCCIC as well.

[83] DHS NCCIC Vulnerability Disclosure Policy, https://NCCIC.us-cert.gov/NCCIC-Vulnerability-Disclosure-Policy.

Interviewees (including FDA) emphasized the importance of considering whether a disclosure would result in increased risk or create unnecessary alarm for patients. It may be helpful to consult with healthcare professionals to fully evaluate patient impact.

MDMs should have a remediation plan in place prior to public disclosure, which may include solutions to remove a cybersecurity vulnerability from a medical device or compensating controls that mitigate the risk. A remediation plan, even an interim countermeasure that reduces risk while more comprehensive long-term solutions are being further evaluated, is critical if public disclosure could otherwise expose patients to harm, whether due to the patient's emotional duress or third-party exploitation of the publicized vulnerability.

If disclosure raises any patient safety concerns, the MDM should discuss the concerns with FDA. FDA may play a role in coordinating between stakeholders (e.g., the MDM, DHS NCCIC, security researchers) to determine the appropriate timetable for public disclosure to ensure patient safety is not compromised by premature release of vulnerability information without a remediation plan in place. In addition, MDMs should draft public disclosures with the minimum amount of information necessary for mitigation to avoid inadvertently providing an attacker with information needed to take advantage of a vulnerability.

MDMs also should consider international cybersecurity disclosure-related rules and regulations. Different regulatory regimes and disclosure obligations may exist abroad and could impact decision-making for disclosure in the United States.

F. Treating Security Researchers as Partners Rather than Adversaries.

We interviewed leading security researchers who regularly report cybersecurity vulnerabilities to MDMs. They provided the following advice:

- Seek common ground with security researchers and focus on shared concerns over product security and patient safety. Treat researchers with respect and do not alienate or discredit them. Remember that researchers can always choose to circumvent the company's coordinated disclosure process and instead report directly to DHS, FDA, and/or the public if they are dissatisfied with the MDM's response to a reported vulnerability.

- Provide regular updates to the security researcher on the progress of the coordinated disclosure process. Assign a product security employee with technical expertise, not an employee from the legal or public relations teams, to communicate with the security researcher. A product security employee will be able to "speak the same language" as the researcher and can effectively communicate that the company is taking the issue seriously. Security researchers obviously do not appreciate receiving a cease-and-desist letter or other communication from the legal department as a first response.

- When validating the reported vulnerability, consider asking the researcher to demonstrate the vulnerability.

- Never offer the researcher money in exchange for silence.

- Consider openly and actively collaborating with security researchers outside of the coordinated disclosure process to demonstrate the company's ongoing commitment to cybersecurity.

Despite the importance of leading with a technical response rather than a legal one, it is critical to recall that there are no legal protections, such as attorney-client privilege, when communicating with security researchers and that any information shared with researchers may be discoverable in a lawsuit. For this reason, MDMs should carefully consider the content of all communications with researchers.

IX. General Cybersecurity Risk Management Principles

Risk management is the process of identifying, assessing and controlling threats that may result in the loss of life, the loss of capital and earnings, or a damaged reputation. Risks can stem from a wide variety of sources, including financial loss, legal and regulatory expectations, criminality and malfeasance, as well as accidents and mistakes. Developing strategies to manage risks stemming from information and data systems have become a top priority for digitized companies.

The ISO standard 27001:2013:6.1.2 provides the general framework for an information risk management strategy, which includes the following five elements:

1) Identification of the risks that could cause the loss of confidentiality, integrity and/or availability of information
2) Identification of risk owners and a comprehensive risk accountability model
3) Definition of the criteria for assessing risk tolerance including consequential outcomes
4) Identification of how risk will be calculated
5) Defining the criteria for how risks will be assumed and acceptable methodology for mitigation

MDMs should consult other ISO standards as well, such as the 14971:2007 "Risk Management Process" and 13485:2016 "Medical Devices – Quality Management" that provide additional guidance. Further guidance specific to medical devices is also available from other organizations. The National Institute of Standards and Technology (NIST), for example, publishes guidance such as its Special Publication 1800-8, "Securing Wireless Infusion Pumps."

As is true in other products and industries, the available guidance forms an incomplete picture of how best to secure any specific medical device, corporate network, or data-sharing process. It is thus necessary to seek guidance from multiple sources and balance the combined expectations against risks and the organization's stated risk tolerance. Even so, MDMs will find that there are key areas that have yet to be definitively addressed by guidance, such as effectively analyzing the large mass of data generated by digital medical devices and incorporating that analysis into risk decision-making.

X. General Cybersecurity Operational Considerations

CVD policies are part of an MDM's larger cybersecurity approach. As such, it is helpful for CVD policies to be informed by aims and vocabularies frequently used in the cybersecurity arena. The most widely accepted cybersecurity framework for organizations in the United States is the NIST Cybersecurity Framework (NIST CSF). The NIST CSF was originally developed to apply to the 16 critical infrastructure sectors defined by Presidential Policy Directive (PPD) 21. (Healthcare is one of those sectors.) The NIST CSF arguably presents the most pragmatic approach to identifying and standardizing areas of cybersecurity risk and provides an ideal foundation with which to integrate other contributing control

frameworks, such as standards (whether general or industry specific) associated with ISO and other organizations and regulatory bodies.

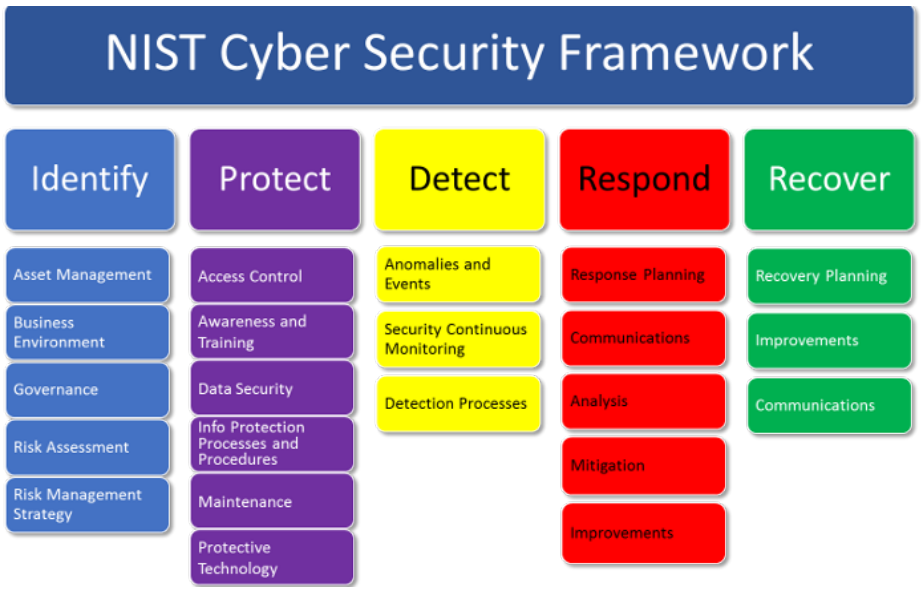

Illustration 1 – The National Institute of Stands & Technology Cybersecurity Framework

NIST CSF identifies 22 categories of concern that align under the five core functions. In the detailed model, the 22 categories shown are further divided into 98 subcategories.

MDMs developing CVD policies will find that several of the NIST CSF categories contribute specific expectations for activities that are an integral part of the CVD process. For example, some MDMs we interviewed described the challenge of coordinating responses across functions in large organizations. When fully implemented, the NIST CSF encourages control framework mapping and alignment exercises that compel various functional teams that may not have otherwise interacted to work together toward common cybersecurity goals. The NIST CSF thus could arguably serve as a natural interface between device security and traditional IT security, resulting in a more holistic approach to cybersecurity within an organization.

Another key benefit to the NIST CSF is that it facilitates metrics that can be repeated and authenticated and can serve as the foundation for streamlining future audits with state and federal agencies. These quantifiable metrics are also helpful when seeking cybersecurity event insurance and defending the reasonableness of "in-place" protections should a cybersecurity event occur.

In addition to the NIST CSF, MDM's may also find "The CERT® Guide to Coordinated Vulnerability Disclosure," published by Carnegie Mellon University, to be a useful resource. The guide covers the principles of CVD, roles in the CVD process, phases of CVD, process variations and operational issues.

XI. Conclusion

The adoption and effective implementation of strong CVD policies by MDMs supports public health and safety, and concurrently provides MDMs with a number of legal and non-legal benefits as documented in this report. Among other things, CVD policies advance patient safety, demonstrate good corporate

citizenship, and improve communication among internal and external stakeholders. CVD policies may also reduce legal exposure by ensuring that an MDM has adequate processes for receiving information about potential vulnerabilities and taking appropriate action in response.

The growing adoption of CVD policies, including the use of online portals, is evidence of a maturing medical device industry that increasingly recognizes the benefits of transparency and cybersecurity risk mitigation. Collaboration among stakeholders in the medical device ecosystem is essential as the industry faces a growing range of cyber threats.