AHLA PG Briefing

Connected Devices in Health Care

Health Information and Technology Practice Group • January 2019

Patrick Alston, Scott Bennett, Jiayan Chen, Bethany A. Corbin, Terrence J. Dee, Jody Erdfarb, Stephen C. Grothouse, Maria Hilsmier, Elizabeth F. Hodge, Ty Kayam, Gerard M. Nussbaum, Timothy C. Wright

AHLA

1620 Eye Street, NW
6th Floor
Washington, DC 20006-4010
www.healthlawyers.org
info@healthlawyers.org

Printed in the U.S.A.

This publication is designed to provide accurate and authoritative information with respect to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering legal or other professional services. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.
–From a declaration of the American Bar Association.

TABLE OF CONTENTS

EDITORS

- Scott Bennett – Coppersmith Brockelman PLC
- Elizabeth F. Hodge – Akerman LLP
- Gerard M. Nussbaum – Zarach Associates LLC

AUTHORS

- Patrick Alston – Premier, Inc.
- Jiayan Chen – McDermott Will & Emery LLP
- Bethany A. Corbin – Wiley Rein LLP
- Terrence J. Dee – McDermott Will & Emery LLP
- Jody Erdfarb – Wiggin and Dana LLP
- Stephen C. Grothouse – Hall Render Killian Heath & Lyman PC
- Maria Hilsmier – Premier, Inc.
- Ty Kayam – Surescripts
- Gerard M. Nussbaum – Zarach Associates LLC
- Timothy C. Wright – Goodwin

FOREWORD

You now hold in your hands or have on your screen a truly timely PG Briefing. As discussed in significantly more detail herein, connected devices are one of the more significant technological advances in health care. Unlike some other major technology changes sweeping health care, connected devices are here and in use today across the health care delivery continuum. Connected devices are also part of the fabric of everyday life for many folks, and these consumer connected devices have significant health care-related aspects.

As is the case with any new technology, there are significant legal implications for the use of connected devices in health care, how the data may be used and handled, and implications for risk, liability, and how health care is delivered. This PG Briefing delves into the many ways in which health care providers and suppliers should approach connected medical devices and aims to assist the health care attorney gain a solid grounding in the issues and implications associated with the use of connected devices in health care. We have sought to balance the needs of the general health care attorney, who will find cogent explanations of complex topics, with those of the experienced technology attorney, who will find valuable insights of relevance.

A publication of this depth and breadth is only possible with a first-rate team of co-editors and contributors. I thank them all for their willingness to share their knowledge with their colleagues in the Health Information and Technology Practice Group. Special thanks and admiration go to Elizabeth Hodge and Scott Bennett. It is a pleasure to work with two such dedicated individuals in bringing this publication to you.

Our hope is that this PG Briefing helps you better understand a rapidly changing area of technology, provides you with the basis for advising your clients, and serves as a springboard for contributing to the use of connected devices in health care.

Gerard M. Nussbaum
Vice Chair of Publications, Health Information and Technology Practice Group,
American Health Lawyers Association

I. INTRODUCTION: USES OF CONNECTED DEVICES IN HEALTH CARE

A. Connected Devices Are Not New

Health care has long used connectivity in a variety of contexts. However, these uses have often been for specific purposes and operated as standalone islands of connectivity. For example, telemetry, which is used for wireless patient monitoring over the ISM-band,[1] fed to a central station on the nursing unit in the past. These systems were often proprietary and did not interoperate well with products from other vendors, and the information was not usually distributed further or integrated into the medical record.

Health care, like most other industries, has sought to adopt connectivity to bolster efficiency, enhance service delivery, and enable new capabilities. Initially these efforts addressed specific uses, while not necessarily increasing the fluidity of clinical information into the medical record. For example, infusion pumps were connected to the hospital network for purposes of providing more timely and easy updating of formulary libraries. This was a one-way connection wherein data updates were broadcast to multiple infusion pumps. Building upon this one-way capability, device manufacturers then provided the ability of selected devices to report operational parameters (e.g., device error codes or usage statistics) back to a central server to aid in management of the devices.

Additional waves of improvement in connectivity have brought many biomedical devices into full two-way connectivity with other systems on the hospital network, including the electronic health record (EHR) system. While this level of connectivity is not uniform across health care providers, the rate at which biomedical equipment is achieving two-way connectivity with the EHR and other systems continues to increase.[2]

[1] The ISM band is an unlicensed portion of the wireless spectrum set aside for industrial scientific and medical use.

[2] This section is intended to provide a flavor of the range of connected devices in use in health care. This section is not intended to be exhaustive in enumerating the full landscape or to delve too deeply into underlying technological processes.

B. Categorizing Connected Medical Devices

Health care connected devices may be loosely categorized by use and function. Medical devices are those used for monitoring and treatment of illness. The majority of these devices are regulated by the U.S. Food and Drug Administration (FDA).[3] Connected medical devices include:

- **Biomedical equipment** (e.g., vital signs monitors, infusion pumps, ventilators, smart beds), which are often found in hospital inpatient and hospital outpatient departments, skilled nursing facilities, and ambulatory surgery centers. These devices have had limited proprietary connectivity capabilities for some time.[4]
- **Implanted devices** (e.g., pacemakers, aortic pressure monitors, spinal stimulation, insulin monitor/pumps[5]), which often use a two-stage connectivity approach wherein the device itself communicates over a lower power wireless signal to a base station, with the base station feeding the data back to the provider.[6]
- **Home health equipment** shares many characteristics with biomedical equipment. Home health equipment (e.g., vital signs monitors, infusion pumps, smart beds) are intended to replicate much of the inpatient monitoring and care functionality in the patient's home, thus supporting the earlier discharge of patients. These systems, often used in conjunction with home health services, may be delivered as a turnkey package and include a wireless Ethernet access point with communication of device data over cellular, phone lines, or the internet to the home health agency.
- **Adjunctive devices** are a relatively new category and are medical devices that support therapeutic interventions, collect/record data, or provide dosage

[3] Please refer to Section III(C) for further discussion of FDA regulation of connected devices.

[4] Often, these legacy connectivity capacities were to central monitoring stations at the nursing station and nurse call/alarm systems over wireless and wired connections.

[5] The insulin monitor may be implanted with the pump remaining external, or both parts may be primarily external. Older devices were primarily external (i.e., not implanted).

[6] The base station often makes use of a reader that is placed against the patient's skin proximate to the location of the implanted device for purposes of obtaining readings, reprogramming, and, in some cases, charging the device. The base station, often located in the patient's home, may communicate to the manufacturer's cloud infrastructure or to the health system over public telephone lines, cellular networks, or through the patient's home Wi-Fi network.

guidance. For example, an adjunctive device may be attached to an asthma inhaler, recording not only date and time of inhaler usage, but also location via Global Positioning Satellite (GPS). These devices may have either onboard cellular communications capabilities or rely upon the patient's cell phone to communicate data back to the provider.[7] In the case of this asthma inhaler example, the patient's location may be combined with data on temperature, pollutant and particulate matter, and other environmental data, as well as the patient's pulse, blood pressure, and oxygen levels to gain a picture of asthma triggers and reactions.

- **Consumer medical devices** come in several variations:
  - Some of this technology, such as personal health devices (e.g., blood pressure cuffs, scales, toothbrushes) are connected, often via Bluetooth, to a consumer's smartphone, tablet, or computer. The data may be logged via an app on the phone/tablet and may be uploaded to the cloud.[8] For individuals with serious health problems, the data from these personal devices may be shared with their care team to support the patient in managing their condition.
  - Another group of technology may be considered personal fitness devices.[9] This functionality may be incorporated in a single-purpose device (e.g., a device that tracks steps, a shirt embedded with sensors for workout monitoring) or as part of general use devices (e.g., an app on a smartphone that tracks steps, fitness trackers built into an Apple Watch). Often, the single-purpose device will communicate to an app on the user's

[7] These systems may also store the data until it is uploaded at a later time. Often the manufacturer will establish cloud-based data collection and analysis infrastructure and communicate the results to the provider.

[8] For individuals with serious health problems, the data from these personal devices may be shared with their care team to support the patient in managing their condition. This data may also be fed into the EHR, perhaps via an EHR application programming interface (API) that supports the interface of this data into the EHR. If brought into the EHR, the data may be classified or stored in an area of the electronic record that makes it clear that the data is patient reported.

[9] Another term for this category of devices is "quantified self."

smartphone that collects data (e.g., Apple Health app). Devices in this category have generally not been subject to FDA regulation.[10]

- **Environmental devices** encompass a wide array of connected devices, from IP-based security cameras and HVAC controls communicating over the hospital network, to citywide environmental condition sensors. These sensors indirectly support the processes of preventing and treating disease. To the extent they are connected to the provider's network or relied upon for data used in treatment, the provider organization should be aware of them and include them in its connected device planning and risk assessment.

The line between more traditional medical devices and consumer devices is becoming less distinct. Medical devices have benefited from advanced development in the much larger consumer devices market, which has led to advances in miniaturization, communication, storage, battery life, and user interfaces. We are also starting to see the introduction of biomedical equipment functionality in consumer devices.[11]

C. Uses for Connected Medical Devices

Biomedical devices that are connected to the main hospital network include vital signs monitors, patient beds, and infusion pumps. The data fed to and from these systems can be used, inter alia, to populate the EHR; communicate device status, location, and usage; and support updating libraries and protocols on these devices. To support more efficient processes, larger health care enterprises, ambulatory surgery centers, and specialty practices have also adopted connectivity to feed data from medical devices into the EHR. Smaller physician practices have been slower to adopt connected medical devices.

[10] Please refer to the discussion in Section III(C) regarding how the FDA has chosen to exercise regulatory discretion regarding more consumer-focused connected devices.

[11] For example, the Apple Watch Series 4 includes electrocardiogram readings and detection of atrial fibrillation, which have been granted clearance by the FDA as Class II devices. *See* https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180044.pdf and https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180042.pdf (last visited Jan. 8, 2019).

Medical devices are not the only connected devices in use in health care. Similar to many other industries, health care has adopted mobile devices, such as iPads, iPhones, tablets, and wireless phones. These mobility tools have penetrated multiple care venues from the nursing unit and the physician's office, to home health settings. These mobile devices in many cases supplement the existing computers and laptops on carts, further adding to the number of computing devices that need to be managed and maintained.

Beyond clinically-focused devices, connectivity and local computing capabilities have been added to almost every device found within the health enterprise, from copiers and printers, to display screens. They extend into building automation systems (such as heating ventilation and air-conditioning (HVAC) systems, lighting, power, and elevator control systems); asset tracking and materials management systems using smart radio frequency identification (RFID) or other wireless tracking technology and autonomous delivery robots; and security and access control systems.[12]

Technological advances have also enabled significant enhancement of mobile biomedical devices used by patients in their daily activities of living: from insulin pumps that constantly monitor and adjust the dose of insulin administered; to asthma inhalers that monitor not only when the inhaler is utilized, but also the location of use to enable integration with real-time data on weather and pollution conditions at the patient's location; and pacemakers, central spinal stimulation, and other implantable devices. These devices may also connect into the health care information ecosystem, either directly to the EHR or through cloud-based services. Devices in the field may connect directly via cellular connection or via base stations that act as an intermediary connection point between the device and the central reporting system.

Consumer devices, such as fitness trackers, mobile phones, and the full range of quantified self-monitoring tools—such as wearables and home medical equipment (e.g., scales, blood pressure cuffs)—may also be connected to and contribute data into the EHR or other health care data systems.

[12] For the sake of simplicity, this briefing will focus mainly on connected biomedical devices. The majority of the discussion in this briefing also applies to other types of connected devices.

A key element underlying this large-scale expansion of connected devices is each of these devices is another node on the network. This has often been referred to as the Internet of Things (IoT). Each device has its own Internet Protocol (IP) address that allows it to be uniquely identified on the network.[13] This unique address allows bi-directional communication. Most of these devices also have local computing power. In some cases, the local computing capacity is limited, relying on other systems on the network to process the data and send back results or commands for the next action or operation to be performed by the node device. The processing systems may be in the cloud, shared by many users, or more localized and under the control of a health care delivery organization, a vendor, or another entity with an interest in the data.

Technological advances will continue the trend towards miniaturization of devices, support for low-powered computing and connectivity, and integration between node devices. This will further drive the increase in the number of nodes on connected device networks. For example, the individual wires on a traditional twelve-lead electrocardiogram (EKG) may be easily replaced with twelve individual sensors that communicate to a central node, also worn by the patient. This central node would contain sufficient battery power and processing capacity to communicate to the main IP network. Further developments might enable each individual sensor to communicate through a mesh network directly to the data repository.[14]

D. Sharing Data with Connected Devices

There is a burgeoning population of connected medical devices. The data gathered by these devices is often valuable for treatment—whether ongoing readings from an implantable cardiac rhythm monitor, periodic readings from a handheld insulin test

[13] There are also devices that may be on other types of networks, such as Bluetooth. These networks tend to be more localized due to their low power characteristics. In the majority of instances, these local networks are themselves connected into an IP-based network through a central node. Much of the discussion relating to security and legal issues applies equally to these non-IP-based networks.

[14] In a mesh network, each node (in this case a sensor) is connected to as many other nodes as possible for communication of data. This eliminates the need for a single central node and may enhance not only fault tolerance but can result in lower power consumption.

device, or episodic data from a consumer fitness tracker. There is also a need to provide a means for accessing the patient's data that is stored in an electronic health record system from connected medical devices. For the majority of connected medical devices, the communication would be one way, from the device to the EHR, uploading data collected by a single purpose device.

Connected medical devices that both send data to and receive data from an EHR would usually do so via apps on a smartphone, perhaps using a core health app, such as the Apple iOS Health app. Such an app may both (i) communicate with other health-related apps on the phone— connecting to and gathering data from external Bluetooth-enabled connected medical devices (e.g., a scale or blood pressure cuff)—which serves as a transfer mechanism of the data to the EHR, and (ii) support the download of key elements of the patient's data from the EHR, with the patient using the app to view her EHR data.

As each device manufacturer and each EHR vendor uses its own approach for storing and managing data, it would be infeasible for every device to connect to every EHR natively. To address this challenge, a common set of standards or approach is needed. One of the most promising approaches is the use of application programing interfaces (APIs). An API is a software intermediary that allows two applications to talk to each other. An API functions like a messenger between applications. The messenger knows the specific way to ask the EHR for the list of medications stored in the EHR and how to, in turn, provide this medication list to the health application on one's smartphone—from whence the patient can view the medication list.[15]

The 2015 Edition Health Information Technology (Health IT) Certification Criteria incorporated criteria for APIs to perform specific functions relating to the sharing of selected elements of the EHR record with other applications and devices.[16] Currently,

[15] You likely use APIs every day without knowing it. For example, if you want to know the class times and instructors who are teaching vinyasa yoga tomorrow, you will access the yoga studio's web page and click on the class schedule link. An API then queries the yoga studio scheduling system and returns a list of classes and instructors to your web browser. You can further narrow the choices to just vinyasa classes, which the API then filters to show only the classes that meet your criteria.

[16] 45 C.F.R. § 170.315(g)(7)-(9).

the criteria do not force every EHR vendor to utilize the same approach for these APIs, but it does support greater use of APIs in health care.

Fast Healthcare Interoperability Resources (FHIR) is a means to further propel health care API standardization. FHIR covers much more than just retrieving select data from EHRs and will eventually provide a standards-based approach for sharing data amongst connected medical devices, EHRs, and other systems.[17]

While APIs and FHIR provide a means to reduce the complexity of data interchange between connected devices, EHRs, and other systems, the challenges relating to security (e.g., authority, access control, permission, and authentication; transmission security; tamper-resistance (integrity), auditing, and protecting availability and integrity) will still need to be addressed in any data exchange.[18] As data is brought into the EHR from connected medical devices, there are also issues of data validity, reliability, and value that directly affect the degree to which and how clinical providers will use and rely upon this data.

II. CONNECTED HEALTH CARE DEVICES: SECURITY RISKS[19]

The introduction of new technologies into the health care setting includes concerns about the security of the new technologies. Connected devices are no different.

[17] FHIR builds upon existing HL-7 standards and is being developed under the broader HL-7 standards setting governance processes. For more information on FHIR, *see* http://www.hl7.org/implement/standards/fhir/summary.html (last visited Jan. 8, 2019).

[18] The 2015 EHR certification criteria also addressed many of these security aspects through other certification criteria. *See, e.g.,* 45 C.F.R. § 315(d)(1), (9), (10).

[19] This section is intended to provide an overview to help the attorney gain an understanding of typical security risks and exposures and some of the underlying contributing factors. It is by no means exhaustive. The attorney should engage in discussions with her client's or organization's information technology, clinical engineering, and security personnel to gain greater insight into the specific risks identified and areas that may potentially be underassessed. As this is a relatively new area, the attorney may also need to support clients in identifying instances where it is appropriate to hire outside experts to support identifying and addressing security issues with connected devices.

Connected devices pose a number of security risks that should be identified and addressed to assure patient safety, information privacy, and uninterrupted operation.[20]

A. Fundamental Design Constraints Affect Connected Medical Device Security

Connected devices often are built from components that have limited processing power. This has been one of the primary barriers to building appropriate security into the new class of connected devices. This limited processing power prevents installation of malware protection software. Even on standard desktop and laptop computers, malware protection software consumes system resources (e.g., processing cycles, memory, power). Unlike standard computers, the processing chips in most biomedical equipment have significantly less capabilities. This makes most of the connected devices unable to run sophisticated security software.

Most medical equipment is also built using specific-purpose processors and memory components. This means that the components inside a given connected device were often designed and built solely for the device. This limits the commonalities across devices and makes creating a set of malware protections that could be readily adopted across all connected devices exceedingly difficult.

Security threats increase and evolve rapidly as cybercriminals develop new exploits to get around the defenses developed by the cybersecurity industry and deployed by customers. This rapid ability requires that defenses rapidly adapt in the never-ending war against the cybercriminals. As new defenses are developed, the software on standard computing systems can be updated as soon as new defenses are developed. The long development cycles for medical equipment, which may exceed five years, act as a barrier to utilizing the same approach for connected medical devices.

[20] Even security basics, such as proper password management, authentication and authorization, and appropriate monitoring need to be part of the security plan for connected devices; such security basics may form a foundation for addressing and mitigating some of the security risks of connected devices.

The medical device industry has been slow to respond to the security threat inherent in many biomedical devices. The design timeline has been a significant aspect of this slowness to respond. In addition, most new models of biomedical devices are developed based on incremental improvements over the prior model. This is beneficial because it provides continuity in terms of feature, function, and user interface for the customers and allows the manufacturer to leverage prior knowledge, experience, and safety testing (including FDA approval processes). The downside, however, is that it becomes difficult to meaningfully add incremental security in this manner. Manufacturers have tried to adapt by seeking wrap-around security, i.e., adding layers of protection around a core system that lacks significant security protection. This is sometimes referred to as "painted-on" security because the underlying product retains all of its security weaknesses. Thus, if the painted-on security is breached, the device is exposed to attack.

To be most effective, security must be designed into the device from the outset. This may require more processing power in the components utilized, careful balancing of feature and function (including security) within available power limitations (especially for those devices which rely primarily on battery power, such as implanted devices), and assuring that enhanced security does not act as an impediment to the primary device purpose—promoting the patient's health.

Redesigning a given medical device from the ground up to fully incorporate security may also substantially increase the cost of the resultant device. Significant price increases for new models of a device may also increase the overall risk of medical devices. In the current cost-conscious health care environment, funding for new equipment is limited. This has led provider organizations to try to squeeze a few more years out of existing devices. This has had the effect of retaining legacy devices in use for longer periods of time; thus, legacy devices that may have limited security protections are thereby kept in service for longer periods of time.

Vendors of medical equipment also face mixed messages from their customers. While offering models with improved, designed-in security, vendors often see greater demand for models with less security due to the lower price. In some cases, this may be due to security considerations not being fully included in the acquisition process and may point to the lack of involvement of information technology and security personnel in the acquisition process.[21]

B. Unclear Lines of Responsibility Contribute to Security Risks

Responsibility within a health system for connected device security is often not clear. Biomedical devices are often managed and maintained by a dedicated department. This department has a variety of names, with clinical engineering or biomedical engineering being among the most frequent. As such, the information technology department, where the majority of security personnel is located, does not have organizational control or involvement in these connected biomedical devices. As a result, these devices are not always tracked or monitored from a security perspective, and they often did not appear on lists of network-attached devices. This disconnect is being addressed in many health systems by either placing clinical engineering under the Chief Information Officer (CIO) or building a much more collaborative relationship between the two departments.[22] Failure to build a cross-discipline team to address connected device security is in itself a security risk.

A problem facing all types of computing platforms is the failure of the responsible individuals to apply security patches in a timely manner. Connected biomedical devices

[21] A similar effect is seen in the consumer market where the lowest purchase price is often the main selection point for devices, including home networking gear, baby monitors, and home security cameras. As a result, the market is dominated by devices with little or no security. Even when devices have security features, they are often not used. The default, out-of-the-box settings for many devices is security features turned off. Many consumers do not know that they need to activate the security features, or how to do so. Sometimes consumers leave the security features turned off because those features can slow down the device's performance. This is relevant to the provider community as these consumer devices are increasingly being used to communicate data to the provider organization, as well as being primary data collection points (see the discussion of consumer devices in Section I.B).

[22] Similar challenges are faced for other "departmental" uses of connected devices. Building automation sensors are usually fully under the management and control of the facilities department. The facilities department often has their own staff who manage these devices, or they use an outside services vendor. Security is often not a high priority concern when selecting or managing these devices. As with the clinical engineering situation, this is changing. In this context it is useful to remember that the malware in the Target attack entered the Target network through a third-party heating, ventilation and air conditioning (HVAC) maintenance vendor that had access to the Target network in order to deliver their services.

suffer similar issues. In addition, there has been a misperception that applying patches to biomedical equipment is prohibited under FDA regulations.[23] The FDA has made it clear that security patches that do not affect the underlying function or operation of the device may be applied without seeking further FDA approval.[24, 25] Even with this clarification, there remains tension between provider organizations and vendors as to who has responsibility for identifying the need for patches, when patches may be applied, and the effect of patches on support and warranties.[26]

The challenge of keeping medical devices up-to-date with the latest security patches becomes particularly significant when more complex biomedical equipment is built on top of commercial, off-the-shelf software (COTS), e.g., Microsoft Windows or UNIX. The lack of clarity as to responsibility between the information technology and clinical engineering department for patching underlying COTS may hamper timely application of patches. As well, absence of dedicated test systems, on which the necessary patches may be applied to assess whether any problems arise from the patch, often cause delays in proactively patching COTS due to the concern of patient harm or impairment of operational capabilities. Equipment vendors and provider organizations are becoming more proactive in addressing these areas, but challenges remain.

Medical devices may be assembled from constituent parts that are supplied by a multitude of suppliers. There may also be a reliance on reuse of open source code or code previously developed for early versions of a given medical device, other medical devices, or for other purposes. The vendor may not have full insight into their supply chain, including the underlying security risks inherent in the constituent parts that

[23] FDA regulation of medical devices is discussed more fully in Section III(C).

[24] FOOD AND DRUG ADMIN., *Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software,"* https://www.fda.gov/RegulatoryInformation/Guidances/ucm070634.htm (last visited Jan. 8, 2019).

[25] FOOD AND DRUG ADMIN., *Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software* (2005), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM077823.pdf (page last updated Feb. 2, 2018, last visited Jan. 8, 2019).

[26] The FDA has suggested that "[I]t is rare for health care organizations to have enough technical resources and information on the design of medical devices to independently maintain medical device software. Thus, most health care organizations need to rely on the advice of medical device manufacturers." *See* footnote 24.

comprise the final medical device, or how combining individual parts with minor security defects may contribute to a major security defect in the final product. While all FDA-approved devices must go through rigorous testing, the security testing aspects have often been given less attention than other product aspects. Even with exhaustive testing, the manufacturer is often limited to testing against the known security challenges of today. Currently it remains challenging to anticipate how cybercriminals will morph their approach in the future and include these future attack vectors in testing today.[27]

Recruiting trained and experienced security personnel remains a key challenge for health care, especially in areas that overlap both clinical engineering and information technology. This results in a substantial amount of on-the-job learning, in part, by trial and error. Thus, staff knowledge levels may act as a constraint on the ability to identify and resolve security issues that cross domains.

C. Connectivity Approaches May Contribute to Security Risks

As health systems have moved to connect biomedical devices to their Ethernet networks, they have often employed dongles that externally add network connectivity to legacy equipment. A dongle is a small device that often attaches to the biomedical equipment via a serial port—which was originally intended for equipment diagnostic use or for hard-wired connectivity to a central monitoring station or nurse call/alarm system—in order to provide network connectivity, data transfer, or even control over functions of the biomedical equipment. The dongle may simply be a means to establish connectivity over Ethernet or Bluetooth wireless networks, or it may enable additional functionality. These dongles may or may not include security protocols, support for anti-malware, or intrusion detection software. Installing patches or updates to these dongles

[27] The challenge of identifying and responding to known exploits is monumental. Microsoft and other major vendors have sponsored the concept of “Patch Tuesday” to help drive home the need to regularly patch all systems. Even a casual user of technology may have noticed the number of security updates that need to be downloaded and installed every week on their own smartphones, tablets, and personal computers.

may also require physically touching each and every dongle to update the firmware. The serial port to which the dongle attaches and the underlying biomedical equipment software and firmware was usually not designed with any substantial security as physical access to the device would be needed to use the serial port. The challenge is the dongle essentially removes this risk mitigation aspect by putting the biomedical device and its serial port on the network.

As these devices are connected to the hospital network, they become exposed to malware, intrusion, and attack. In the early stages, the exposure does not directly impact patient safety, as the connectivity is used mainly for administrative and operational uses. However, many of these connected devices are network exposure points due to weak device security and network security. As such, they often offer an entry point for attacks on other systems on the network.

When the devices on the network have the capability for some degree of onboard security, as is the case with computers running security software, the design and architecture of the network relies on these local security capabilities.[28] As connected medical devices with a very low degree of onboard security are attached to the network, the security posture of the network shifts significantly as these connected medical devices are unable to defend themselves to the same degree as a computer running security software. Thus, without redesign, the network itself can amplify the security risk of the connected medical devices to the medical devices themselves as well as other devices on the network. If the scope of network monitoring does not include connected medical devices, then the organization may be blind to malicious activity occurring on the network.

While the medical device industry is generally seeking to address security issues with connected medical devices, security risks associated with connected medical devices will likely increase over time. This reflects the general increase in security risks

[28] This is not to suggest that health care networks did not locate security capabilities at multiple points on the network.

associated with any connected device as the cybercriminals constantly develop ways to overcome new cybersecurity defenses. As such, ongoing vigilance is needed.

III. CURRENT LEGAL FRAMEWORK

Connected devices, in the health care industry or otherwise, are subject to an array of rules and regulations. This section provides an overview of the major laws, regulations, and agency guidance that impact and shape the security of and security within connected devices.

A. Health Insurance Portability and Accountability Act

Any assessment of potential security requirements for connected devices used in health care should include the Health Insurance Portability and Accountability Act (HIPAA) as one of its first checkpoints.

HIPAA may be a consideration with respect to the use of connected devices in health care in several ways. First, it may apply to the entities that develop or support the operation of a connected device, either because they are business associates or, in rarer situations, are covered entities. One example of a connected device developer that would be subject to HIPAA as a business associate is a mobile app developer engaged by a covered entity health care provider to provide an app that is downloadable by the provider's patients to support remote monitoring and care management.[29] In contrast, the developer of an app that is sold directly to consumers for use in managing a chronic illness and sharing health information collected through the app with the consumers' providers would generally not be a business associate, as

[29] *See* U.S. DEP'T OF HEALTH & HUMAN SERVS., OFFICE FOR CIVIL RIGHTS (OCR), *Health App Use Scenarios & HIPAA,* pg.3 (2016), https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf (last visited Jan. 8, 2019).

the developer is not providing the app (and creating, receiving, maintaining, or transmitting protected health information) *on behalf of* the providers.[30]

Even where HIPAA does not apply to the device manufacturer, it may nonetheless be an important consideration due to the context in which the device is used, such as where the device interacts with an electronic medical record platform or other HIPAA-regulated data system. For instance, if a developer seeks to make its consumer-facing mobile health app interoperable with major EHR platforms, customers and EHR vendors may expect the developer to implement certain security safeguards commensurate with those that a business associate would need to adopt, even if the developer is not a business associate as defined under HIPAA. While many digital health solutions are being deployed in a direct-to-consumer fashion rather than on behalf of covered entities, HIPAA will continue to be relevant as an industry benchmark and should be incorporated into contractual requirements.

The HIPAA security standards (Security Rule) are technology neutral so as not to become obsolete as risks and technologies evolve.[31] In assessing the security measures to support implementation specifications, covered entities and business associates should consider their “size, complexity, and capabilities”; their “technical infrastructure, hardware, and software security capabilities”; the security measure’s cost; and “[t]he probability and criticality of potential risks to electronic protected health information.”[32] For example, a cloud service provider that hosts data collected through a wireless insulin pump on behalf of a covered entity health care provider and that meets the definition of a business associate should consider (among other factors) the vulnerabilities of the pump’s security safeguards and risk to patients should someone exploit such vulnerabilities and gain unauthorized access to patient data.

[30] *Id.* at 2.

[31] U.S. DEP’T OF HEALTH & HUMAN SERVS., CTRS. FOR MEDICARE & MEDICAID SERVS., *HIPAA Security Series, Security 101 for Covered Entities,* pg. 8 (2007), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (last visited Jan. 8, 2019).

[32] 45 C.F.R. § 164.306(b)(2).

The HIPAA Security Rule requires covered entities and business associates to periodically conduct a security risk assessment and develop a risk management plan to mitigate risks and vulnerabilities to their electronic protected health information.[33] Any connected devices that the covered entity or business associate uses to store or transmit protected health information, or that otherwise interact with the covered entity's or business associate's data systems, should be included in the risk assessment and management plan.

Note that HIPAA also has privacy standards (Privacy Rule), as well as breach notification requirements (Breach Notification Rule), that may be applicable to connected devices.[34] The Department of Health and Humans Services, Office of Civil Rights (OCR) may impose a civil money penalty on a covered entity or business associate for failure to comply with a requirement of HIPAA.[35] Knowing violations of HIPAA are subject to criminal penalties.[36]

B. Federal Trade Commission (FTC) Security Requirements

Another key regulator in this realm is the FTC. The FTC's relevant enforcement authority stems primarily from Section 5 of the Federal Trade Commission Act (FTCA), a broadly drafted statute designed to protect consumers from "unfair or deceptive acts or practices in or affecting commerce."[37] The key limitation to the FTC's Section 5 enforcement authority is "the act or practice [must] cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[38] The FTC has issued numerous guidance documents on data security,

[33] 45 C.F.R.§ 164.308(a)(1)(ii).
[34] Please refer to Section VII(D).
[35] 45 C.F.R.§ 160.404.
[36] 42 U.S.C. § 1320d-6 (2016).
[37] 15 U.S.C. § 45(a) (2016).
[38] *Id.* § 45(n).

including for mobile health app developers[39] and in the context of the IoT.[40] The FTC's authority is important when it comes to connected devices because it covers many connected devices and their uses that are not subject to either HIPAA or the jurisdiction of the FDA (see next subsection, FDA Regulation of Medical Devices).

C. FDA Regulation of Medical Devices

The rapid evolution of digital connectivity in health care has played a leading role in the advancement of disease treatment, diagnosis, and improved outcomes. Medical devices, part of the burgeoning IoT area, are regulated by the FDA and are key contributors to the transformation of patient care. While these devices provide substantial benefits to clinicians and patients, they also present risks, particularly associated with data management and cybersecurity. The FDA evaluates evidence of medical device safety throughout the product's life cycle to ensure that only those devices with a favorable benefit-risk profile are marketed. At the same time, however, the FDA must encourage the development of technologies to address unmet needs and improve patient safety. Connected medical devices that do not have adequate controls may present cybersecurity risks that can adversely affect device functionality, disrupt the delivery of health services, and lead to patient harm.[41] When it comes to cybersecurity, the FDA is focused on risks "impacting the safety and effectiveness of the device,"[42] (e.g., data integrity and availability) rather than risks to patient privacy (e.g., confidentiality of information).

[39] *See* FED. TRADE COMM'N, *Data Security*, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Jan. 8, 2019).
[40] FED. TRADE COMM'N, *Careful Connections: Building Security* (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf (last visited Jan. 8, 2019).
[41] U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, OFFICE OF INSPECTOR GENERAL, *FDA Should Further Integrate Its Review of Cybersecurity into the Premarket Review Process for Medical Devices*, OEI-09-16-00220, Sept. 2018.
[42] FOOD AND DRUG ADMIN., *FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity*, https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf (last visited Jan. 8, 2019).

The Food, Drug, and Cosmetic Act (FDCA)[43] regulates, among other things, medical devices. A "medical device" can be a tangible device, software, or some combination thereof. Many connected devices are likely to be categorized as "medical devices," as that term is defined in the FDCA.[44] Connected devices regulated by the FDA include biomedical equipment, implanted devices, home health equipment, and sometimes, adjunctive devices. Generally, consumer products do not meet the "medical device" definition and are not regulated by the FDA, though this line is blurring as consumer devices are now including functionality that has received FDA clearance (e.g., personal health and fitness devices, such as fitness trackers).[45]

Like computer systems and networks, medical devices are vulnerable to security breaches and third-party hacking, and this vulnerability increases as these devices are connected to the internet.[46] While all connected devices come with inherent risk, the FDA permits marketing of these devices when reasonable assurances exist that the benefits to patients outweigh the risks.[47] Accordingly, connected device manufacturers are responsible for including appropriate safeguards in their devices to address patient safety risks and identify and mitigate hazards associated with their medical devices.[48]

As part of its oversight, the FDA has issued several guidance documents specifically addressing cybersecurity. While these guidance documents contain disclaimers that they are to be considered guidance, they reflect the agency's current thinking on the subject. Failure to comply with this guidance could have negative consequences, such as derailing premarket approval efforts.

[43] 21 U.S.C. § 301 *et seq.*

[44] 21 U.S.C. § 321(h).

[45] For example, the Apple Watch Series 4 received FDA Class II clearance for both the EKG and atrial fibrillation functionality; *see* note 11.

[46] FOOD & DRUG ADMIN., *Cybersecurity*, https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last visited Jan. 8, 2019).

[47] *Id.*

[48] *Id.*

i. Pre-Market Review

There are three different regulatory classifications for medical devices based on the risk to patients and health care providers.[49] Class I devices pose very little risk to patients and providers (e.g., a tongue depressor). Class II devices, which include insulin pumps and x-Ray machines, present greater risk to patients and providers. Class III devices—used to sustain or support life—pose a significant threat to patients or providers if used incorrectly, such as cardiac defibrillators.

The classification of a medical device sets the pre-market regulatory review required. There are three levels of pre-market regulatory review of medical devices: the premarket approval (PMA), 510(k) premarket notification, and general controls.[50]

In 2013, the FDA began requiring assessments of vulnerability to cyberattacks for Class II and Class III devices. The agency issued a safety communication, *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication*,[51] which recommended that "medical device manufacturers and health care facilities take steps to ensure that appropriate safeguards are in place to reduce the risk of device failure due to cyberattack."[52] Then in 2014, the FDA released guidance, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, which updated prior guidance to address the use of wireless in medical devices and emphasizing the use of authentication and encryption.[53] Recently, the FDA published a draft update to the 2014 Premarket guidance with recommendations for effective cybersecurity management to decrease the risk of patient harm by reducing device exploitability.[54]

[49] Medical Device Amendments Act of 1976, 21 U.S.C. § 360c; 42 Fed. Reg. 46028 (Sep. 13, 1977); 43 Fed. Reg. 32988 (Jul. 28, 1978); 21 C.F.R. Part 860.

[50] Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 SANTA CLARA HIGH TECH. L.J. 139, 165 (2014).

[51] U.S. GOV'T ACCOUNTABILITY OFFICE, *Cybersecurity for Medical Devices and Hospital Networks: FDA Safety Communication* (2013).

[52] FOOD & DRUG ADMIN., *Cybersecurity,* https://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm (last visited Jan. 8, 2019).

[53] FOOD & DRUG ADMIN., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (2014), https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356190.pdf (last visited Jan. 8, 2019).

[54] FOOD & DRUG ADMIN., *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff* (Oct.18, 2018),

The various FDA guidance documents emphasize several points:

- The value of conducting a risk analysis throughout the lifecycle of the device.
- Medical device security is a shared responsibility among stakeholders, including health care facilities, patients, physicians, and manufacturers of medical devices.
- Cybersecurity should be addressed during the design and development phase of a medical device. The FDA has provided a framework to guide these cybersecurity efforts.[55]
- The FDA typically does not need to review or approve any medical device changes to software made solely to strengthen cybersecurity.

ii. Quality System Regulation

The FDA has the authority to regulate the methods, facilities, and controls used in the entire lifecycle of the medical device to conform to current good manufacturing practices (GMPs). The Quality System (QS) Regulation,[56] which sets forth these GMPs, applies to all finished device manufacturers that desire to commercially distribute the medical device.[57] The purpose of the QS Regulation is to ensure that medical device manufacturers are addressing all risk, including cybersecurity risk.[58] As noted above, the FDA is concerned with cybersecurity risks related to patient safety and not confidentiality of patient information. The pre-market and post-market cybersecurity guidance documents issued by the FDA specifically target this cybersecurity risk and provide recommendations on meeting the QS Regulation.[59]

https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529 (last accessed Jan. 8, 2019). When finalized, the draft guidance will supersede the 2014 Premarket guidance.

[55] *See supra*, note 53.

[56] 21 C.F.R. Part 820.

[57] 21 C.F.R. § 820.1.

[58] *See supra*, note 42.

[59] *Id.*

iii. Post-Market Requirements

Regulation of medical devices after they enter the market occurs in three ways: adverse event reporting, post-approval studies, and post-approval reports. Of relevance to the security of connected devices is adverse event reporting.[60]

In December 2016, the FDA published the final version of its *Postmarket Management of Cybersecurity in Medical Devices*, which provided voluntary guidance and "recommendations for managing postmarket cybersecurity vulnerabilities for marketed and distributed medical devices."[61]The FDA clarified that device manufacturers should identify and address cybersecurity vulnerabilities impacting their medical device vulnerabilities as part of their postmarket management.[62] The FDA stressed that cybersecurity risks to connected devices will continually evolve and be impossible to completely mitigate through premarket controls alone. The FDA once again emphasized the shared responsibility associated with medical device cybersecurity, noting that it requires cooperation and collaboration among manufacturers, health care facilities, patients, and providers,[63] while acknowledging it has no authority over medical device users.

More recently, the 21st Century Cures Act[64] clarifies the FDA's regulatory authority over health information technology products, including mobile applications. The 21st Century Cures Act sheds light on what may be categorized as "software as a medical device" and subject to FDA oversight.[65]

[60] *See* Section VII(A).
[61] FOOD & DRUG ADMIN., *Postmarket Management of Cybersecurity in Medical Devices,* pg. 4 (Dec. 28, 2016) https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf (last visited Jan. 8, 2019).
[62] *Id.* at 4.
[63] *Id.* at 12.
[64] 21st Century Cures Act H.R.34 – 114th Congress (2015-2016), 42 U.S.C. § 1001, https://www.congress.gov/114/plaws/publ255/PLAW-114publ255.pdf (last visited Jan. 8, 2019).
[65] *See FDASIA Health IT Report: Proposed Strategy and Recommendations for a Risk-Based Framework* at 3-4, www.fda.gov (2014), https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM391521.pdf (last visited Jan. 8, 2019).

Connected devices may interface or associate with Software as a Medical Device (SaMD). Software is classified as SaMD if the software is "intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[66] For example, this would include "software that allows a smartphone to view images obtained from a magnetic resonance imaging (MRI) medical device for diagnostic purposes" or "Computer-Aided Detection (CAD) software that performs image post-processing to help detect breast cancer."[67, 68]

In April 2018, in order to accomplish the twin goals of innovation and safety, the FDA published its *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health*,[69] which sets forth five goals that the agency believes will help ensure the safety of medical devices, including driving innovation towards safer medical devices and strengthening medical device cybersecurity.

The FDA believes that developers who invest in innovation to create safer medical devices should be rewarded. Accordingly, the FDA intends to provide incentives and scientific expertise to drive the marketplace towards investing in and developing safer technologies and devices that address unmet medical needs.

As part of its efforts to keep pace with changing cybersecurity risks, the draft update to the Premarket guidance provides recommendations regarding device design, labeling, and documentation that manufacturers should consider for devices with cybersecurity risk.[70] For example, appropriate design should anticipate the need for deploying routine updates and patches as well as emergency workarounds.[71] Manufacturers should also

[66] FOOD & DRUG ADMIN., *Software as a Medical Device (SaMD),* https://www.fda.gov/MedicalDevices/DigitalHealth/SoftwareasaMedicalDevice/default.htm (last updated Nov. 19, 2018, last visited Jan. 8, 2019).

[67] Food & Drug Admin., *What are examples of Software as a Medical Device?,* https://www.fda.gov/MedicalDevices/DigitalHealth/SoftwareasaMedicalDevice/ucm587924.htm (last accessed Jan. 8, 2019).

[68] However, the smartphone is **not** a medical device.

[69] FOOD AND DRUG ADMIN., *Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health,* https://www.fda.gov/downloads/AboutFDA/CentersOffices/OfficeofMedicalProductsandTobacco/CDRH/CDRHReports/UCM604690.pdf (last visited Jan. 8, 2019).

[70] *See supra*, note 54 at pg. 4.

[71] *Id.* at p. 16.

consider labeling as a way to manage risk, including providing the FDA and health care delivery organizations with a "Cybersecurity Bill of Materials" (CBOM) which lists the commercial, open source. and off-the-shelf software and hardware components that are or could be susceptible to vulnerabilities.[72]

Further, the FDA intends to explore the development of a public-private partnership known as CyberMed Safety (Expert) Analysis Board (CYMSAB), which would serve as a resource for medical device manufacturers and the FDA. The CYMSAB would integrate patient safety issues into the assessment of device vulnerabilities, and would be responsible for adjudicating disputes, analyzing proposed mitigations, and offering consulting advice to organizations that are navigating the coordinated disclosure process. The CYMSAB would also be deployed to investigate device compromises.

D. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA)[73] was enacted in 1986 to criminalize knowingly or intentionally accessing a "protected computer" without authorization or by exceeding authorization. Among other things, the CFAA prohibits accessing a computer and obtaining information, damaging a computer or information, or threatening to damage a computer.[74]

While the term "protected computer" refers to "computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions,"[75] "computer" itself is broadly defined in the CFAA.[76] As such, any connected device that uses an electronic data processor or a computer chip would fall under this broad definition of "computer" and be under the protection of the CFAA.

[72] *Id.* at p. 20.
[73] P. L. 99-474 (1986).
[74] 18 U.S.C. §§ 1030(a)(1) - (a)(7).
[75] U.S. DEP'T OF JUSTICE, *Prosecuting Computer Crimes,* pg. 4 (2010) [hereinafter the "Prosecuting Computer Crimes Manual"], https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (last visited Jan. 8, 2019).
[76] 18 U.S.C. §§ 1030(e)(1).

Further, hospital computer networks are within the purview of the CFAA,[77] and it is a felony to cause the "modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment or care of 1 or more individuals."[78] Consequently, introducing malware or malicious code into a connected device that potentially or actually affects patient care could be prosecutable under the CFAA.

For example, in August 2018, a jury convicted an individual under the CFAA for conducting a distributed denial of service (DDoS) attack against a hospital.[79] The defendant customized malicious software that he installed on 40,000 network routers, so that he was able to control the routers from his home computer. The defendant then attacked the hospital's network by directing hostile traffic to it. The attack interrupted access to internet services hospital staff used to treat patients. It also knocked several other hospitals off the internet.[80] Although there is no indication that the particular attack involved connected health care devices, the FBI has warned about the growing risk of DDoS attacks from connected medical devices and wearables.[81]

Consequences for violating the CFAA can involve prison sentences ranging from one year to twenty years, depending on the crime committed and the United States Federal Sentencing Guidelines.[82] Although criminal in nature, the CFAA also allow for civil causes of action with remedies of compensatory damages, injunctive relief, and other equitable relief.[83]

[77] Prosecuting Computer Crimes Manual, *supra* note 75 at 45 ("This subsection [18 U.S.C. §1030(c)(4)(A)(i)(II)] provides strong protection to the computer networks of hospitals, clinics, and other medical facilities because of the importance of those systems and the sensitivity of the data that they contain.").

[78] 18 U.S.C. § 1030(c)(4)(A)(i).

[79] U.S. DEPT. OF JUSTICE, *Press Release* (Aug. 1, 2018), https://www.justice.gov/usao-ma/pr/jury-convicts-man-who-hacked-boston-childrens-hospital-and-wayside-youth-family-support (last visited Jan. 8, 2019).

[80] *Id*.

[81] FED. BUREAU OF INVESTIGATION, *Public Service Announcement*, *Common Internet of Things Devices May Expose Consumers to Cyber Exploration*, https://www.ic3.gov/media/2017/171017-1.aspx (last visited Jan. 8, 2019).

[82] 18 U.S.C. §§ 1030(a)(1) - (a)(7).

[83] 18 U.S.C. § 1030(g).

E. The Federal Anti-Tampering Act

The Federal Anti-Tampering Act[84] was signed into law in 1983 after the deaths of seven individuals in Chicago who had ingested Tylenol laced with the toxin potassium cyanide.[85] The Act criminalizes tampering or attempted tampering with or tainting "consumer products" that affect interstate or foreign commerce. Consumer products are defined to include any food, drug, device, or cosmetic, as defined in the FDCA,[86] and any article, product, or commodity produced or distributed for individual consumption or use.[87] Many connected devices could fall within this definition of "consumer product."

To violate the Act, the tampering or attempted tampering must have occurred with "reckless disregard for the risk that another person will be placed in danger of death or bodily injury and under circumstances manifesting extreme indifference to such risk."[88] Moreover, the Federal Anti-Tampering Act also criminalizes "[t]ainting of a consumer product with intent to cause serious injury to the business of any person."[89] While "tamper" and "taint" are not defined in the Act, the associated Senate Report defines tamper as to have "the limited meaning of improper interference 'as for the purpose of alteration, and to make objectionable or unauthorized changes.'"[90] The Report notes that "taint" is intended to be broader than "tamper," and means "to modify with a trace of something offensive or deleterious, or infect, contaminate, or corrupt."[91] Although whether a cyberattack constitutes tampering or tainting has yet to be litigated, an argument may be made that a cyberattack that alters or affects the functionality of a connected device could be considered tampering or tainting.

[84] 18 U.S.C. § 1365 (2012).
[85] President Ronald Reagan, Statement on Signing the Federal Anti-Tampering Act (Oct. 14, 1983); Dan Fletcher, *A Brief History of the Tylenol Poisonings*, TIME (Feb. 9, 2009), http://content.time.com/time/nation/article/0,8599,1878063,00.html (last visited Jan. 8, 2019).
[86] 21 U.S.C. § 321.
[87] 18 U.S.C. § 1365(h)(1).
[88] *Id.* § 1365(a).
[89] *Id.* § 1365(b).
[90] *State v. Harlston*, 565 S.W.2d 773, 778–79 (Mo.App.1978); S.Rep. No. 69 on S. 216, 98th Congress, 1st Sess., at 7.
[91] S.Rep. No. 69 on S. 216, 98th Congress, 1st Sess., at 7.

F. The Electronic Communications Protection Act

The Electronic Communications Protection Act (ECPA) addresses the protection of electronic communications in their storage and transfer.[92] The ECPA would be implicated for any connected device that allows for the storage or transmission of "electronic communication," which is broadly defined to include "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce."[93]

Provisions of the ECPA would apply to connected devices under Sections 2701 and 2702. Section 2701 works to safeguard the security of stored electronic communications. The ECPA makes it a federal crime to intentionally, without authorization or in excess of authorization, access a facility through which an electronic communication service is provided to obtain, alter, or prohibit authorized access to wire or electronic communication that is in electronic storage. "Electronic communication service" is defined as any service that provides users with the ability to send or receive wire or electronic communications; "electronic storage" is defined as temporary, intermediate storage incidental to transmission as well as backup storage.[94] Hacking a connected device would invariably involve accessing the storage on the connected device.

Section 2701 does not apply to an entity that is providing the electronic communication service itself.[95] Rather, Section 2702 establishes the rules for entities providing electronic communication service and remote computer service to the public. A "remote computing service" is defined as the provision to the public of computer storage or processing services by means of an electronic communications system.[96] Per the ECPA, electronic communication service providers are required to keep the content of

[92] The ECPA comprises three statutes: Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2012); Wiretap Act, 18 U.S.C. §§ 2511– 2522 (2012); Pen Register Act, 18 U.S.C. §§ 3121–3127 (2012).
[93] 18 U.S.C. § 2510(12).
[94] *Id.* §§ 2510(15), 2510(17).
[95] *Id.* § 2701(c).
[96] *Id.* § 2711.

communication confidential while it is in electronic storage by that service, and remote computer service providers are required to keep the content of any communication that is carried or maintained on that service confidential.[97] While the ECPA provides that the content of communication may not be disclosed by these providers, a record or other information pertaining to a customer of the service may be disclosed "to any person other than a governmental entity," [98] i.e., the metadata may be shared.

Violations of Section 2701 are subject to criminal penalties of up to $250,000 and/or five years imprisonment; violation of section 2702 does not carry any criminal penalties.[99] Nevertheless, the ECPA allows for a private cause of action for violation of both Sections 2701 and 2702.[100] *In re Pharmatrack* established the parameters that to succeed under this private cause of action, a plaintiff must demonstrate "that a defendant (1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication (5) using a device." [101]

G. State Cybersecurity Laws

Connected devices, by virtue of their connectivity, could be viewed by hackers or other bad actors as a means of accessing or attacking hospital networks or other computer networks. Worse yet, limited processing power, specific purpose parts, and legacy devices make security measures, such as malware protection, more difficult to implement.[102]

In September 2018, California became the first state to enact a law that mandates security features for connected devices. The California law requires any manufacturer of a device that connects "directly or indirectly" to the internet to protect the device with

[97] *Id.* § 2702(a)(1)-(2).
[98] *Id.* § 2702(c)(6).
[99] *Id.* 2701(b).
[100] *Id.* 2707.
[101] *In re Pharmatrack, Inc.*, 329 F.3d. 9, 18 (1st Cir. 2003); *see also* Barbara Fox, *Mobile Medical Apps: Where Health and Internet Privacy Law Meet*, 14 HOUS. J. HEALTH L. & POLICY 193, 216-217 (2014).
[102] *See* Section II(A).

"reasonable" security features. That law will go into effect in January 2020.[103] One notable exception to the new law is connected devices whose functionality is subject to security requirements under federal law, e.g., connected medical devices regulated by the FDA.[104]

Many states have cybersecurity laws that, while not specifically targeted at connected devices, might apply to improper conduct relating to those devices.[105] Those laws fall into several broad categories:

i. Hacking or Unauthorized Access

Hacking and unauthorized access refer to trespassing on or within a computer, information system, or network without consent, or unpermitted bypassing of the security measures of a computer, information system, or network. Almost all states have enacted some form of criminal statute addressing these matters. For example, under New York law, use of a computer, computer service, or computer network without authorization is a misdemeanor, and intentionally or knowingly committing computer trespass or accessing a computer, computer service, or computer network without authorization is a felony.[106]Many connected devices would likely fall within the statute's definition of a computer.[107]

ii. Malware

Malware is malicious code or software that disrupts service, steals sensitive information, or gains access to private computer systems (e.g. viruses, worms, and bots). Most

[103] SB-327, *available at* https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (last visited Jan. 8, 2019).
[104] *Id*. § 1798.91.06(d).
[105] *Computer Crime Statutes*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx#Ransomware (last updated Apr. 13, 2018, last visited Jan. 8, 2019).
[106] N.Y. PENAL LAW §§ 156.00, 156.50.
[107] *Id.* § 156.00(2).

states have laws that prohibit actions such as tampering, altering, damaging, or interfering with a computer or network. For example, Delaware law criminalizes the misuse of computer system information when a person "intentionally or recklessly and without authorization [a]lters, deletes, tampers with, damages, destroys or takes data intended for use by a computer system, whether residing within or external to a computer system; or [i]nterrupts or adds data to data residing within a computer system."[108] This type of statute could apply where bad actors attempt to introduce malware into a hospital computer network using a connected device or interferes with the operation of a connected medical device.

iii. Ransomware

Ransomware is a type of malware that encrypts data so that it is inaccessible to authorized users. Attackers generally require the payment of a ransom to decrypt the data or to not publish or expose the data. While some state laws pertaining to malware could also criminalize ransomware, at least four states have enacted legislation that specifically addresses ransomware: California,[109] Connecticut,[110] Texas,[111] and Wyoming.[112] Connected devices can be vulnerable to a ransomware attack and can be used to spread an attack.

iv. Spyware

Spyware is software that is secretly or surreptitiously installed into an information system that tracks or monitors activities of users. Spyware installed on connected devices could collect both data input into or transmitted from or to a connected device, as well as hamper the proper performance of the device, resulting in patient safety risks.

[108] DEL. CODE TIT. 11, § 935.
[109] CALIF. PENAL CODE § 523 (2016 S.B. 1137).
[110] 2017 H.B. 7304, Public Act 17-223.
[111] 2017 H.B. 9, Chap. 684.
[112] WYO. STAT. §§ 6-3-506, 6-3-507.

Twenty states have laws regarding spyware, and those laws are significantly different from state to state.[113]

v. Denial of Service Attacks

Denial of service (DoS) and distributed denial of services (DDoS) attacks are an emerging threat to connected devices. A DoS attack occurs by flooding a system's bandwidth to render it inoperable so that legitimate users cannot access the system. A DDoS occurs when computer systems with exploited vulnerabilities are used to attack or target another system. In October 2017, the FBI issued an alert warning that DDoS attacks of connected devices are estimated to increase from 5 billion in 2016, to as many as 50 billion by 2020.[114] Unprotected connected medical devices could be compromised and used in a DDoS attack on other systems within the health enterprise or turned outward against other targets.

Laws that might apply to DoS and DDoS crimes differ by state. Some states, such as California and Indiana, have laws that prohibit crimes against property, which could apply to DoS and DDoS attacks.[115] Other states, such as Pennsylvania and Washington, have laws regarding computer crimes that could apply to those types of attacks.[116]

H. Private Actions

Individuals who have allegedly suffered damages or losses from a breach or lapse in security of a connected device have limited options under the existing federal statutory framework, as neither HIPAA nor Section 5 of the FTCA provide for a private right of

[113] *State Spyware Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/research/telecommunications-and-information-technology/state-spyware-laws.aspx (last updated Oct. 30, 2018, last visited Jan. 8, 2019).

[114] FED. BUREAU OF INVESTIGATION, *Common Internet of Things Devices May Expose Consumers to Cyber Exploitation* (2017), https://www.ic3.gov/media/2017/171017-1.aspx (last visited Jan. 8, 2019).

[115] *See* CAL. PENAL CODE § 502; IND. CODE § 35-43-1-8.

[116] 18 PA. C.S.A. § 7612; WASH. REV. CODE § 9A.90.060.

action. Nonetheless, certain state data protection and/or consumer protection laws may allow such actions,[117] and individuals may also seek relief in courts under common law theories of liability, such as but not limited to product liability, negligence, invasion of privacy, consumer fraud, breach of fiduciary duty, breach of contract and implied contract, infliction of emotional distress, battery, and trespass to chattels.[118] While case law in this area is undeveloped, certain principles may be instructive.

First, the ability to bring a product liability claim (such as allegations of design or manufacturing defects) regarding medical devices marketed under a premarket approval (PMA) is restricted in certain respects as set forth in the U.S. Supreme Court's decision in *Riegel v. Medtronic*.[119] In the case, the Court held that the preemption clause of the Medical Device Amendments of 1976 (amending the Federal Food, Drug and Cosmetic Act) bars state common law claims that challenge the safety or efficacy of medical devices marketed under a PMA.[120]

In today's era of digital health solutions, however, *Riegel v. Medtronic*'s preemptive effect should not be overstated, as many connected devices either do not constitute medical devices currently subject to FDA regulation or are lower risk devices marketed under a 510(k) premarket notification submission to the FDA. Further, insofar as injuries from a security breach involving a Class III medical device occurred due to a manufacturing defect (i.e., not from an inherent defect in design) or other "parallel" state law claim, *Riegel v. Medtronic* likewise may not shield manufacturers and developers.[121] The *Riegel* decision also may not necessarily bar a claim based on a theory that the

[117] *E.g.,* CAL. CIV. CODE § 1798.84 (2018) (providing a private right of action for individuals injured as result of a security breach affecting personal information); MD CODE ANN., COM. LAW § 14-3508 (2018) (providing that a violation of the state's Personal Information Protection Act is an unfair or deceptive trade practice subject to the enforcement and penalty provisions of the state's consumer protection law, which includes a private right of action).

[118] *See* Wellington, *supra* note 50, at 175-182 (2014) (discussing various theories of tort liability for cyberattack injuries).

[119] 552 U.S. 312 (2008).

[120] *Id.*

[121] *Id.*

manufacturer was negligent in failing to push out patches or other security updates to a connected device in a timely manner, if failing to do so would violate the FDCA.[122]

Where product liability claims are permitted with respect to FDA-regulated medical devices, the growing body of guidance documents and other standards that the agency has issued relating to device security will likely be an important consideration. For other theories of liability such as battery and trespass to chattels, it remains to be seen how courts will translate traditional principles and inquiries—such as whether there is a physical violation of the patient or consumer in the event of a cyberattack—in the context of the evolving fact patterns surrounding the use of connected devices in health care.[123]

In data breach litigation, one focal point has been the issue of what is required in order for a plaintiff to have standing. The uncertainty lies in the injury that plaintiffs must allege—a challenging question where, as in the case of many data breaches, plaintiffs have not yet necessarily experienced identity theft or other misuse of their information following the breach. The prevailing test that the U.S. Supreme Court articulated in *Spokeo, Inc. v. Robins* focuses on whether plaintiffs have alleged a "concrete and particularized" injury, with "concrete" injury meaning one that is "de facto; that is, it must actually exist," but not one that needs to be "tangible."[124] Since *Spokeo*, however, there has been significant uncertainty as to what constitutes a sufficient allegation of a risk of possible future harm (such as identity theft) to support standing, although a breach that involves full social security numbers may be more likely to withstand legal challenge.[125]

[122] *See McClelland v. Medtronic*, 944 F. Supp. 2d 1193, 1196 (M.D. Fla. 2013) (negligence claims preempted where device went through the PMA process and no additional duty was imposed on the manufacturer to inform the plaintiff of defects to be addressed after the PMA process).

[123] *Medical Information Security Breaches and Medical Device Cybersecurity Attacks*, 158 AM.JUR. PROOF OF FACTS 3d 367 (originally published 2016, Oct. 2018 Update) ("the hospital, health facility, medical device manufacturer, or other entity may face civil liability for negligence or another theory of liability for a security breach"); *See* Wellington, *supra* note 50 at 175 ("A patient injured by a cyberattack may also have a cause of action against medical device manufacturers and hospitals for negligence.").

[124] 136 S. Ct. 1540 (2016). The *Spokeo* decision added the "concrete and particularized" factors to the previous "actual or imminent" test set forth in the Court's landmark decision in *Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).

[125] *See, e.g., In re SuperValu, Inc.,* No. 14-MD-2586 ADM/TNL (D. Minn. 2018) (granting motion to dismiss on remand from the Eighth Circuit with respect to named plaintiff who alleged a fraudulent use of his credit card after the breach, as plaintiff did not allege any out-of-pocket loss from paying or not being reimbursed for the fraudulent charge, and where the Eighth Circuit had declined to find standing for other

As cyberattacks continue to plague the health care industry, what is required in order for plaintiffs to establish standing remains subject to significant variation, including at the federal appellate level.

I. General Data Protection Regulation (GDPR)

The GDPR, which imposes extensive protections for the personal data of European Union (EU) data subjects and repeals the EU Data Protection Directive (95/46/EC) (Directive), went into effect on May 25, 2018.[126] Notably, the GDPR is not limited in scope to organizations that are established or have a means of processing in the EU. Rather, the scope of the GDPR extends to any organization that offers free or paid goods or services to data subjects in the EU, or that monitors EU data subjects' behavior taking place in the EU.[127] Thus, for example, a U.S.-based developer of a mobile medical app that is downloadable by EU residents could fall within the far-reaching scope of the GDPR. Likewise, the GDPR would also apply to the processing of data by a U.S.-based hospital that treats a patient who is located in the EU (for example, where the provider remotely monitors the patient after he returns to the EU).[128]

Although the GDPR was enacted by the EU, its enforcement could vary by country, especially since member countries may adopt their own conditions relating to

plaintiffs based on allegations of future injury arising from a substantial risk of future identity theft where the breach involved credit card numbers but not social security numbers, birth dates, or driver's license numbers); *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (finding standing for plaintiffs who alleged the theft of certain identifying information including social security numbers and credit card numbers and noting that "a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken"); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (finding no standing based on allegation of future identity theft in case of breach involving names, birth dates, last four digits of social security numbers, and physical descriptors because allegations were based on an "attenuated chain of possibilities").

[126] Commission Regulation 2016/679, art. 99, 2016 O.J. (L 119).

[127] *Id.* Art. 3.

[128] Note, however, that EU citizenship or residence of the patient is not, in and of itself, a sufficient basis for the applicability of the GDPR; rather, the trigger is that the patient is *located* in the EU when his data is collected through remote monitoring.

processing of genetic data, biometric data, and data concerning health.[129] This creates challenges for device manufacturers that conduct business on a global scale.

Regulated entities should consider whether they constitute a data "controller" or data "processor" with respect to any particular data processing activity, as regulatory obligations and attendant risk mitigation options (such as the presence of contractual privity with data subjects that provides an opportunity to establish contractual limitations on liability) will vary based on how the entity is situated with respect to the data processing. Generally, a data "controller" means any entity that, alone or jointly with others, determines the purposes and means of the processing of personal data, whereas a data "processor" means any entity that processes personal data on behalf of a controller.[130] The GDPR defines "personal data" broadly to include "any information relating to an identified or identifiable natural person," and establishes additional protections for certain data categories, including biometric data and genetic data.[131] It is critical that data controllers and data processors with respect to connected devices conduct the necessary upfront diligence to understand the pathways through which they are authorized to process personal data.

As compared to the superseded Directive, the GDPR includes more expansive and protective rights for data subjects, including, for instance, the right to erasure (i.e., the "right to be forgotten" under certain circumstances)[132] and the right to data portability (i.e., the right to obtain one's personal data provided to a controller "in a structured, commonly used and machine-readable format," and "to transmit those data to another controller . . ."). [133] Breach notification requirements are also explicit under the GDPR,[134] whereas the Directive was silent on the issue of breach notification except under certain limited circumstances.

[129] Commission Regulation 2016/679, art. 9(4).
[130] *Id.*, art. 4.
[131] *Id.*
[132] This could potentially conflict with the requirements to retain information under HIPAA and state medical records laws.
[133] Commission Regulation 2016/679, Art. 20.
[134] *See* Section VII(G).

Data protection by design and default is a critical dimension of the GDPR. Data controllers must assess up front what technical and organizational safeguards, such as encryption or pseudonymization, are necessary to comply with the GDPR.[135] Data controllers and data processors must also implement security of processing requirements that are commensurate with the risks involved.[136] The risk evaluation should consider, among other issues, the implications of any unlawful or accidental destruction, loss, alteration, disclosure, or access—a particularly important assessment in the context of connected medical devices that support more critical health care functions. Before beginning any processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons"—including the large-scale processing of health data—data controllers must also perform a privacy impact assessment that meets certain minimum standards as set forth in the GDPR.[137]

One significant issue for connected health care devices is that the GDPR generally requires obtaining express consent in order to process an individual's genetic data, biometric data, or "data concerning health."[138] Relying on consent as a basis to process personal data can pose operational challenges for the health care entity and device manufacturer if the patient later withdraws his or her consent, as the GDPR gives the patient the right to do "at any time."[139]

The GDPR includes an arsenal of various enforcement mechanisms, including the grant of extensive investigative and corrective powers to supervisory authorities.[140] Data controllers and data processors must be ready, for example, "to provide any information [the supervisory authority] required for the performance of its tasks."[141] Violations of certain provisions, such as those regarding basic principles for processing and conditions for consent, are subject to a penalty of up to 4% of a company's total worldwide annual turnover of the prior financial year or up to €20 million, whichever is

[135] Commission Regulation 2016/679, Art. 25.
[136] *Id.* Art. 32.
[137] *Id.* Art. 35.
[138] *Id.* Art. 9.
[139] *Id.* Art. 7.
[140] *Id.* Art. 58.
[141] *Id.*

higher.[142] Violations of other provisions, such as those regarding privacy by design, carry a potential penalty of up to €10 million or 2% of a company's total worldwide annual turnover of the preceding financial year, whichever is higher.[143] In addition, not-for-profit bodies, organizations, or associations may file complaints and bring legal actions on behalf of data subjects for alleged violations of the GDPR—effectively comprising a quasi-class-action pathway under the Regulation.[144] Individuals also have the right to seek compensation from data controllers and processors for any alleged damages.[145] However, determining who is liable may be a challenge, especially since many different actors may be involved with data from connected devices, such as the manufacturer of the device, the developer of an application used on the device, the health care delivery organization providing services to the EU resident, the treating physician, or a telemedicine services provider acting directly or on behalf of a health care delivery organization.

L. Gaps in Existing Laws

As illustrated above, connected devices used in health care often sit outside the scope of many key regulatory regimes. The manufacturers or developers of such solutions are typically not HIPAA covered entities, and determining whether they are business associates is a highly fact-intensive analysis that will depend in part, for example, on whether the manufacturer is storing data collected through the device on behalf of a HIPAA covered entity. Where not applicable by operation of law, the applicability of HIPAA privacy, security, and breach notification standards may depend on market pressures and the ability of health care providers and other institutional entities to contractually impose HIPAA standards for solutions that interface with their data systems. Many such solutions—particularly those that support health management functions—also fall outside the scope of the FDA's jurisdiction or oversight focus.

[142] *Id.* Art. 83.
[143] *Id.*
[144] *Id.* Art. 80.
[145] *Id.* Art. 82.

Further, rapid advances in technology and efforts to disrupt traditional notions of health care delivery are making it challenging for regulators to keep pace. The number of connected devices will increase as the “patient as consumer” paradigm continues to expand, with patients increasingly taking a more active role in their health care and seeking novel products and solutions designed to facilitate their ability to manage their treatment and monitor their wellness.

For products and solutions that do not sit neatly within the scope of HIPAA and FDA regulations, state breach and consumer protection laws, common law, and the FTC’s broad interpretation of its Section 5 enforcement authority will be particularly important, as will evolving normative and industry standards.

IV. CYBERSECURITY BEST PRACTICES FOR CONNECTED DEVICES

A. Building an Effective Cybersecurity Compliance Program

In addition to complying with the applicable legal requirements for cybersecurity,[146] health care providers and organizations can improve their cybersecurity frameworks for connected devices by drawing on general principles for effective compliance programs. The purpose of a compliance program is to establish a culture of security.[147] The U.S. Department of Health and Human Services’ Office of Inspector General (OIG) has set forth a compliance framework consisting of seven core elements:

(1) Developing standards of conduct, policies, and procedures;

(2) Designating a compliance officer or compliance committee to oversee the compliance program;

(3) Conducting training and education;

[146] For example, the HIPAA Security Rule sets out cybersecurity requirements for covered entities and business associates. *See* Subsection IV(B) below.
[147] *See* DEP’T HEALTH & HUMAN SERVS., *Top 10 Tips for Cybersecurity in Health Care*, pg. 2, https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf (last visited Jan. 8, 2019).

(4) Maintaining effective lines of communication;

(5) Undertaking internal audits and monitoring;

(6) Enforcing the compliance program through disciplinary standards; and

(7) Responding to noncompliance and implementing corrective action.[148]

When developing a cybersecurity program for connected devices, some key elements are: risk assessment; training and education; auditing and monitoring.

i. Risk Assessment

Health care organizations should develop and implement approaches for identifying and mitigating potential threats and vulnerabilities to connected devices.[149] This commonly takes the form of a risk assessment conducted on an annual basis. Risk assessments operate by identifying the most serious risks to an organization and determining whether sufficient controls are in place to mitigate those risks.[150] In this manner, a risk assessment serves to identify, measure, and prioritize compliance risks. Risk assessments allow organizations to pinpoint high-risk areas, develop responses to mitigate those risks, and conserve resources by targeting areas where patient care may be compromised or business operations may be impaired; all of which could lead to harm to patients, and financial and reputational harm to the organization. These assessments should be repeated at least on an annual basis and more frequently for high-risk areas.

[148] *See* OIG Compliance Program for Clinical Laboratories, 63 Fed. Reg. 45,076, 45,076-79 (Aug. 24, 1998).

[149] Paul Otto, *Best Practices for Managing Cybersecurity Risks Related to IoT-Connected Medical Devices*, JD SUPRA (Mar. 12, 2018), https://www.jdsupra.com/legalnews/best-practices-for-managing-23206/ (last visited Jan. 8, 2019).

[150] *See, e.g.*, HITRUST, *Healthcare Sector Cybersecurity Framework Implementation Guide,* pg. 19 (May 2016) https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf (last visited Jan. 8, 2019).

For connected medical devices, it is important that health care organizations and device manufacturers are attentive to the risks posed to data and patient safety throughout the lifecycle of the product.[151] As technology and cyber threats evolve, the risks and vulnerabilities associated with these connected devices will change. Risk assessment should be performed at every stage of a product's lifecycle, and risk management should be a corresponding requirement for any vulnerabilities identified.[152] Although an entity's perspective may depend to a large extent on whether it is a device manufacturer, health care entity or business associate subject to HIPAA, or an entity not subject to HIPAA or FDA regulations, all entities should prioritize risks based on the risk assessment and develop an annual work plan to guide compliance efforts.

For connected device manufacturers specifically, cybersecurity risk management programs should address vulnerabilities that permit any unauthorized access, modification, or denial of information stored, accessed, or transferred from a medical device both as part of the design of the connected device and throughout the device lifecycle. Components may include incorporating robust security as a foundational design element of the product,[153] monitoring cybersecurity information sources to detect current and anticipated cyber threats and risks, "[m]aintaining robust software lifecycle processes," detecting vulnerabilities and assessing their impacts, developing internal and external processes to communicate vulnerabilities, implementing a vulnerability disclosure program, and "[u]sing threat modeling to clearly define how to maintain safety and essential performance of a device by developing mitigations that protect, respond and recover from a cybersecurity risk."[154] Manufacturers may also wish to focus attention on their enterprise-wide security policies and procedures for assuring that consistent and appropriate attention is given to cybersecurity of connected devices throughout the design and lifecycle of the device and the relationship of these controls to their overall enterprise risk management posture. Manufacturers may also need to review and revise their communications approach to customers to assure that time-

[151] Otto, *supra* note 149.
[152] *Id.*
[153] Security by design is a key element in the FDA Cybersecurity Guidance, which is discussed in Section III(C).
[154] *Postmarket Management of Cybersecurity in Medical Devices*, *supra* note 61, at 13-14.

critical communications regarding cybersecurity events reach not only their traditional contact points within customer organizations, but also encompass those customer departments responsible for cybersecurity.

When health care organizations are addressing cybersecurity risks associated with connected medical devices, it is important to consider internal as well as external threats. Policies and procedures regarding internal access and use of connected medical devices are particularly important given a 2018 Verizon report that found nearly 58% of all security incidents at health care organizations involved insiders.[155]

ii. Training and Education

In addition to policies and procedures, training and education are crucial components of a strong cybersecurity program. As noted, insiders pose a significant threat to health care organizations and are responsible for a large portion of data breaches.[156] Training and education serve as an opportunity to reduce the risks associated with insider breaches and reinforce good cyber hygiene. Training and education should cover relevant cybersecurity policies and procedures, as well as industry trends and specific cybersecurity threats associated with connected medical devices.[157] During training, an organization can reinforce best practices to guard against cyberattacks, including password hygiene (such as using different passwords for different accounts and not sharing passwords). Training also can detail common examples of cyberattacks, such as phishing schemes and how to spot and avoid them. Employees should also be made aware during training that improper access to patient data could lead to disciplinary

[155] VERIZON, Protected Health Information Data Breach Report, pg. 4 (2018), http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf (last visited Jan. 8, 2019).

[156] *Id.*

[157] HIMSS, *2018 HIMSS Cybersecurity Survey*, pg. 8 (2018), http://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf at 22 (noting that security awareness training of workforce members is crucial) (last visited Jan. 8, 2019).

action.[158] Training and education should be specific to the cybersecurity risks facing the health care industry in general and the organization in particular, and it should be conducted in a frequent and ongoing manner to ensure effectiveness.[159]

iii. Proactive Monitoring

Health care organizations should adopt a proactive compliance approach that regularly tests the cybersecurity standards, policies, and procedures that are in place for connected medical devices. Such testing is an ongoing process, involving evaluating random samples, monitoring high-risk activities, and conducting trend analysis.

As part of this monitoring process, organizations may wish to conduct penetration testing on a regular basis. Penetration tests can uncover vulnerabilities in connected medical devices, such as weaknesses that may provide a malicious actor with access to or control over a system.[160] Such testing should ideally be conducted at frequent and regular intervals, as well as when major personnel and process changes occur at the organization that impact the cybersecurity program.[161]

Health care organizations should also consider implementing formalized insider threat management programs.[162]

B. Safeguards

Safeguards are a necessary component of any cybersecurity framework. The HIPAA Security Rule requires covered entities to maintain appropriate administrative, physical, and technical safeguards that ensure the confidentiality, integrity, availability, and

[158] *See* Jai Vjayan, *Insider Threat Seriously Undermining Healthcare Cybersecurity*, DARK READING (Mar. 5, 2018, 6:30 PM), https://www.darkreading.com/vulnerabilities---threats/insider-threat-seriously-undermining-healthcare-cybersecurity/d/d-id/1331191 (last visited Jan. 8, 2019).

[159] *Top 10 Tips for Cybersecurity in Health Care*, *supra* note 147, at 2.

[160] *See 2018 HIMSS Cybersecurity Survey*, *supra* note 157, at 20.

[161] *Id.* at 5, 20.

[162] *Id.*, at 20.

security of electronic personal health information (ePHI).[163] Administrative safeguards are defined to include administrative actions, policies, and procedures that manage the development and implementation of security measures designed to protect ePHI, and that manage the covered entity's workforce.[164] Physical safeguards encompass measures that protect buildings and equipment from unauthorized intrusion, destruction, or disasters.[165] Finally, technical safeguards refer to technology, policies, and procedures that are used to protect ePHI and control access to it.[166] The HIPAA Security Rule provides in-depth guidance regarding the expectations for implementing these safeguards.

C. Insurance

While prevention of a cybersecurity attack through strong compliance measures is always preferable to dealing with the aftermath of a data breach or hacking incident, it is important for health care organizations to consider risk-shifting and mitigation options that may be helpful in the event of a breach or hack.[167]

One such option is cybersecurity insurance.[168] As noted in Section VI(F), most general insurance policies do not cover losses and liabilities associated with cyberattacks, such as a breach or hack of a connected medical device.[169] Indeed, the risks associated with a cyberattack involving personal data are massive, with an average cost of $3.7 million per incident.[170] This amount does not include the cost of patient injury or death if a

[163] 45 C.F.R. §§ 164.308, 164.310, 164.312.
[164] *Id.* § 164.304.
[165] *Id.*
[166] *Id.*
[167] Lena J. Weiner, *Cybersecurity Insurance Basics for Healthcare Organizations*, HEALTH LEADERS MEDIA (June 8, 2015), http://www.healthleadersmedia.com/technology/cybersecurity-insurance-basics-healthcare-organizations (last visited Jan. 8, 2019).
[168] *See* Section VI(F) for a discussion of contract provisions and due diligence relating to vendors' insurance coverage.
[169] There have been no reported incidents of a patient death or bodily harm directly caused by a cybersecurity incident.
[170] Clemens Scott Kruse et al., *Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*, 25 TECHNOLOGY AND HEALTHCARE 1, 1, 6 (2017), https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263, at 7 (last visited Jan. 8, 2019).

connected device is compromised. Cyber incidents involving connected devices can harm patients in multiple ways, ranging from the exposure of personal information to physical harm and even death. While cybersecurity insurance can provide some protection against the financial liability associated with a breach of patient data, it is unlikely that such insurance will cover financial liability resulting from patient injury or death. Therefore, health care organizations should consult with their insurance brokers regarding the types of coverage needed to address the variety of risks posed by connected devices.

In addition to covering the costs of responding to a cyber incident, some cyber-insurance carriers also may assist with risk assessment and remediation before an incident occurs. Cyber-insurance carriers also have security and breach response vendors on call.[171] In the event of a breach, the health care organization can call its cyber-insurance carrier and receive access to a team of specialists ready to respond to the breach incident quickly.[172] Quick access to a team of specialists can result in faster breach containment and reduced liability.

Health care organizations should also review their medical malpractice policies to determine if, depending on the circumstances, they may provide coverage in the event a patient is harmed or dies as a result of a cybersecurity incident.

V. DUE DILIGENCE REGARDING CONNECTED DEVICES

Evaluating the capabilities and practices of connected device manufacturers should be a part of the health care organization's privacy, security, compliance and legal program. This includes being cognizant of regulatory and statutory requirements and industry recommendations related to cybersecurity and understanding the past, present, and future security and privacy posture of connected device manufacturers.

[171] *Id.*
[172] *Id.*

A. Security Program and Practices

As the security program of a health care organization seeks to provide for the confidentiality, integrity, and availability of the organization's data, connected devices should be included in the scope of assets that must adhere to organizational security standards. The organization's security team should evaluate the manufacturers of connected devices and how their security safeguards align with those of the health care organization.

Connected devices often present challenges to IT governance, such as:

1. While devices may have operating software, they often do not allow anti-virus software to be installed on the device, thus requiring the organization to find an alternate solution to protect against malware and ransomware attack.

2. Devices may be connected to the organization's network, but if general network access controls are weak or the network is open to a wide range of users, then, the connected medical devices may need to be connected only to a more secure portion of the organization's network where similar data is housed or access may be limited to a specific group of users and systems. This might be accomplished through, for example, network segmentation or overlaying of other security tools.

3. Security upgrades usually involve some outage in availability which needs to be accommodated if other systems or patient care rely on the connected device.

4. Updates may also require manufacturer support, which might mean that firewalls, intrusion detection, or physical security must be adjusted to support the upgrade. Such access to the connected device by a third party may bypass security controls and create potential vulnerabilities to the organization's data and network. Organizations that choose to reduce security in these instances should carefully monitor the network during this period, adopt other mitigating controls, and assure that the security environment is properly re-established at the conclusion of the event.

5. Monitoring the device functionality and device communication may be provided as a service by the manufacturer to detect problems or collect usage data from connected devices for improvement and support purposes. This may result in the manufacturer receiving more than the minimum necessary information to monitor the health of the device.

Situations like those delineated above need to be accounted for and addressed in the organization's due diligence and security program. When variations in the organization's security practices are required for the use of a connected device, the security program should perform a security audit/evaluation as well as a privacy audit/evaluation to document the variation and establish mitigations to align with the health care organization's security and privacy programs.[173]

B. Privacy Impact Assessment

As referenced above, health care organizations will want to perform certain security and privacy assessments to ensure that a medical device has the necessary security and privacy controls in place to protect the organization's confidential data (and its patients). A privacy impact assessment is recognized as a universal "systematic process for evaluating the potential effects on privacy of a project, initiative or proposed system or scheme and finding ways to mitigate or avoid any adverse effects."[174]

The precise structure and form of an organization's Privacy Impact Assessment (PIA) should reflect regulatory guidance, and be used to:

i. Identify any potential privacy/security issues;

ii. Evaluate whether the benefits of a use of data outweigh the risks;

[173] Christopher Frenz and Bev Corwin, *Secure Medical Device Deployment OWASP* (2017), https://www.owasp.org/index.php/OWASP_Secure_Medical_Device_Deployment_Standard (last visited Jan. 8, 2019).

[174] Privacy Impact Assessment, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (2018), https://iapp.org/resources/topics/privacy-impact-assessment-2/ (last visited Jan. 8, 2019).

iii. Provide a means for the compliance and legal departments to assess the project's legal, regulatory, industry and organizational standards; and,

iv. Explain the health care organization's rationale behind accepting the risk with delineated mitigations.

The purpose of the PIA is to evaluate a new use of the organization's data, whether in development, strategic arrangement, or with a third party for business opportunities.[175] The PIA process should include engagement by both internal and external stakeholders to identify risks and propose the necessary security, business, technological, legal and/or infrastructure mitigations to minimize identified risks. In order to properly vet the potential risks of an arrangement, or in this instance a medical device, a comprehensive PIA process should include the collaboration of experts in information technology, clinical engineering, security, data management, privacy and legal. The organization's PIA process should do the following:

i. Describe the arrangement, the processing operations, the related purpose, scope, duration, and interested internal and external parties;

ii. Identify the type of data associated with the arrangement, the intended use of the data and whether it will be shared, with whom, and how the data will be managed, stored, secured and destroyed if applicable;

iii. Assess the risks and rights of the individual related to the data; and

iv. Evaluate security and privacy measures that should be implemented to:

    a) Address the risks to the data or the organization; and

    b) Demonstrate compliance with applicable laws and regulations. [176]

[175] A PIA is distinct from a HIPAA security risk analysis. The PIA is an internal assessment of security risks related to data privacy, and should be done in conjunction with the introduction of any new technology or new data use. In contrast, the HIPAA Security Rule requires covered entities and business associates to periodically conduct a risk analysis, which is an "assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."

[176] See International Association of Privacy Professionals, *supra* note 174.

In order to fully evaluate the security and privacy measures as referenced in (iv) above, the organization should vet the security controls and practices of the manufacturer related to the development and maintenance of a medical device, and take into consideration the security knowledge and maturity of the device provider by:

i. Reviewing its policies and procedures; third party audit results, attestations and related security certifications;

ii. Requesting evidence from the manufacturer regarding security controls and consideration, including but not limited to, penetration test results of the medical device and related mitigations;

iii. Assessing documentation from the manufacturer regarding the auditing controls built into the device, for example, how access and activity related to the data is monitored and audited, the frequency of patching or upgrades, and the corresponding level of encryption required for the data; and,

iv. Reviewing documentation provided and discovered independently by the health care organization of the manufacturer's prior security/privacy incidents (if any). Such information can be obtained through the disclosure requests related to the PIA process, and independently discovered on the OCR breach website [177]or the FDA's website. If there is evidence of a security/privacy incident, the organization should request documentation verifying that any vulnerabilities have been mitigated, and request evidence of a risk analysis and risk management plan (as required by HIPAA).[178]

Ultimately, the PIA is designed to describe the data processing activity and to take into account the nature, context, and purposes related to the necessity and scope of the data processing. An organization will go through this assessment to help manage any resulting risks to an individual's private data (including protected health information,

[177] OCR, Breach Portal, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Jan. 8, 2019).

[178] 45 C.F.R. § 164.308(a)(1).

personally identifiable information, consumer/financial information) and the organization's confidential and proprietary data.

C. Use of the Manufacturer Disclosure Statement for Medical Device Security (MDS2) Form

The MDS2 form was developed through a collaboration of industry organizations, government agencies, and other stakeholders. This form provides a vehicle for device manufacturers to provide information about the security and privacy properties of a device to potential customers.[179] The form[180] includes information, such as the types of PHI stored on the device, and specific security capabilities. One key benefit of the form is it allows potential customers to compare security features across different devices and different manufacturers.[181]

Health systems should require medical device manufacturers to submit a MDS2 form, or a similar form, when reviewing the capabilities and security and privacy controls related to the device.

D. Known Security Vulnerabilities

Security vulnerabilities are a fact of life for many devices. Bugs in code, backdoors by manufacturers, dependencies on third- and fourth-party application programming interfaces (APIs), and defined methods of communication between software components are all vectors to exploit a connected device and thereby a health care organization’s data and environment.

[179] Axel Wirth, *Medical Device Security Update: Why the MDS2 Form was Revised*, Symantec Official Blog (Nov. 11, 2013), https://www.symantec.com/connect/blogs/medical-device-security-update-why-mds2-form-was-revised (last visited Jan. 8, 2019).

[180] National Electrical Manufacturers Association, *Manufacturer Disclosure Statement for Medical Device Security* (Oct. 7, 2013), https://www.nema.org/standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx (last visited Jan. 8, 2019).

[181] The form is *available at* http://www.himss.org/resourcelibrary/MDS2/himss.org (2018).

Known security vulnerabilities are documented in the National Vulnerability Database, an online repository of vulnerabilities maintained by the National Institute of Standards and Technology (NIST). This database is used by most commercial vulnerability scanning tools. In addition, health care organizations should implement mitigating controls when a vulnerability is identified when implementing a device or its supporting services.

Device manufacturers should have a mechanism for keeping the software or firmware patched and up to date. This may involve a manufacturer supplied patch that is manually applied by the organization, automatic updates over the internet or other networks, in-person or remote systems patching by the manufacturers, or the removal and replacement of a device or components. It is critical that health care organizations timely apply patches provided by the manufacturers.

Very little software and hardware is developed solely by the connected device manufacturer. This means that security vulnerabilities from components in the device's supply chain that comprise the hardware and dependent software can create vulnerabilities for the device and even the health care organization's overall IT environment. Manufacturers of connected devices should be able to provide a bill of materials for all licensed software or hardware used in the device so that a health care organization can determine if the underlying components have any known vulnerabilities. The bill of materials should be updated when there are significant updates or changes in licenses to the software or firmware of the hardware.

Development of a secure medical device requires that a manufacturer follow rules for secure development and/or privacy by design to deter the introduction of known vulnerabilities. When establishing that a manufacturer has developed the device/software in a secure fashion, health care organizations should determine if the following has occurred:

- *Data validation*.[182] This involves testing the parameters that are used to operate the device, in both intended and unintended ways.[183] Understanding the valid input for any device and properly handling invalid input helps defend against the majority of security weaknesses.[184] The need to obtain vendor certifications regarding data validation will be further addressed in Section VI below.

- *Verifying Third-Party Dependencies*. Very little software and hardware is developed solely by one manufacturer. A vulnerability from any component in the device's supply chain can put the security of the device at risk.

Due diligence around known security vulnerabilities, like research of past incidents and planning for continuous monitoring, should occur during the bid process and before the contract with the device manufacturer or supplier is finalized and executed.

E. Security Risk Analysis

Health care entities should perform a security analysis of a device before it is used. HIPAA requires covered entities and business associates to perform a security risk assessment, and update that assessment "in response to environmental or operational changes affecting the security of electronic protected health information."[185] Entities should evaluate the performance of the device in conjunction with existing security controls like anti-virus, identity controls, and connectivity methods.

Large health care entities with robust security programs might also consider performing a vulnerability assessment of the device that includes:

- A passive scan, which monitors the device while in use; and

[182] Data Validation, owasp.org (2013), https://www.owasp.org/index.php/Data_Validation (last accessed Jan. 8, 2019).
[183] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, *supra*, note 53.
[184] OWASP *Top 10 Privacy Risks Project*, owasp.org (2017), https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project (last visited Jan. 8, 2019).
[185] 45 C.F.R. § 164.308(a)(8).

- An active scan, where the security team attempts to hack the device through various attacks like brute force or injection, in a test environment.

An organization should also, when possible, obtain the results of a third-party test that involved taking the device apart and testing individual components.[186]

F. Ongoing Monitoring

Due diligence does not stop when the contract for purchase of the connected devices is signed.The addition of a connected device to an organization's network—whether local or remote—requires ongoing monitoring for the life of the device as part of including the connected device in the organization's existing security monitoring program. A new and different monitoring strategy may also be required. In cases where the device is remote from the organization's network, the manufacturer may supply the monitoring as a service, and this function should be considered and captured in the final executed agreement between the parties.

The monitoring of manufacturers also continues as a passive and active exercise as a part of the security program. Updates and notifications from the manufacturer and independent due diligence performed by the health care organization through the use of industry and governing agencies resources and tools (e.g., the OCR breach portal[187] and the FDA medical device recall database)[188] give an independent passive threat feed to monitor the manufacturer on an ongoing basis.

Recurring security risk assessments provide active tracking of the scope and authorization of the connected device in the health care organization. This may change the overall risk posture as device usage expands or contracts. When performing HIPAA

[186] Smaller entities, or those without sophisticated cybersecurity capabilities, may find it more expeditious to leverage industry resources and tests performed by independent testing laboratories, or tests performed under the supervision of group purchasing organizations. Purchasers may seek to require suppliers to provide the results of such testing by independent testing laboratories.

[187] OCR, Breach Portal, *supra,* note 177.

[188] FOOD AND DRUG ADMIN., *Medical Device Recalls* (2018) https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm (last visited Jan. 8, 2019).

risk assessments, health care organizations should align their manufacturer list with threat intelligence feeds from their security team to get the most current information about manufacturers with whom the organization does business. This gives the organization practical information to understand threats that it faces.

Use of annual manufacturer risk assessments, by questionnaire or audit, to reestablish the security posture of the manufacturer or product act as a touch point to understand how the device and associated services have changed since the last assessment. The health care users of connected devices should request from the manufacturers annual attestations/certifications by independent third parties of security controls that are critical to business functions or that could negatively impact patient care.

Ongoing monitoring should include a review of contracts at the time of renewal. Often the manufacturer will update end user license agreements outside of the contract cycle as new features are brought online. An organization's legal team, as well as privacy and security departments, should work together when there are changes to licenses, privacy practices, or security capabilities to be sure that the proper mitigations are taken to secure the organization's data and protect it from vulnerabilities and undue harm. These different perspectives can help to eliminate gaps in providing due diligence for manufacturers of connected devices.

VI. CONTRACT PROVISIONS FOR CONNECTED DEVICE SECURITY

As discussed above, the substantial level of security risk associated with connected devices for health care entities is not comprehensively addressed by existing law in the United States, and the government rarely holds connected device manufacturers meaningfully accountable to their downstream business-to-business customers when it comes to data security issues. Health care entity customers can be especially vulnerable, as HIPAA pins a number of expensive obligations on covered entities for the data security shortcomings of their business associates. Health care entities are largely left to manage risks with respect to their patients' safety and data on their own. Too often, health care entities capitulate to the common manufacturer refrain that "if it's behind your firewall, it’s your problem” when it comes to shouldering the information security burden for products licensed or sold for installation in health care entity systems.

This should not, and does not, have to be the case with respect to connected devices. Health care entities can enhance security through effectively contracting for the purchase of connected devices. This section identifies and briefly describes some important basic contract provisions to consider, in addition to traditional procurement terms, in order to shift and mitigate those security risks identified during the due diligence process before connected devices have been delivered and connected to a health care entity’s network.

A. Performance Warranties

Performance warranties promise that a device will conform to and perform in accordance with its specifications. While performance warranties for devices are a mainstay in general procurement contracting, depending on the device, their role with respect to connected devices can have far-reaching consequences for a health care entity’s operations. For instance, if a connected device that functions as a central node for a number of other devices connecting to the network fails, all of those dependent devices lose their connection to the network.

Generally, manufacturers of physical products such as connected devices prefer to limit performance warranty duration (often ranging from 90 days to 1 year), forcing purchasers to thereafter rely on post-warranty support on a subscription-fee basis. Manufacturers justify this on the ground that the purchase price is not sufficient to cover the maintenance of a device through long-term wear and tear. However, it is much more difficult to justify categorically limiting the duration of a performance warranty geared specifically at the computing and connectivity components of a device. Subject to exceptions for physical damage, unauthorized modification and the like, health care entities should push manufacturers to warrant the performance of these aspects throughout the useful life of the device.

Device manufacturers often insist on limiting the remedies for a breached performance warranty to repair or replacement of the device, ostensibly seeking to avoid expectation damages. However, a loosely written “sole and exclusive remedy” clause may be open to a much broader interpretation, potentially barring recovery for *any* claims arising from a device failing to perform. As noted above, failure of a device to meet the requirements of a performance warranty can yield ripple effects throughout a network, which could result in losses that may be recoverable under other legal theories. Accordingly, when agreeing to sole and exclusive remedies for warranty breach, health care entities should exercise care to narrowly tailor the remedy to the warranty breach claim itself, and not related claims.

B. Maintenance and Support

For most connected devices, a performance warranty is not sufficient to ensure continued secure functionality throughout the useful life of a device. Most contractual performance warranties are by nature relatively static—they simply provide that the device will continue to work as it did when delivered. To trigger a remedy, a breach of the warranty must first occur. Health care entities should not passively wait for a warranty breach to jeopardize the integrity of its networks before a device is supported. To close this gap, the vast majority of connected device manufacturers also include a maintenance and support service with their devices, which is much more fluid for connected devices than for isolated devices. Rather than relying on phone support or travel, vendor support personnel can often remotely access a health care entity’s network to service a connected device directly. This remote access to the network raises additional security concerns for the health care entity that should be addressed in the contract.[189]

Device connectivity also enables manufacturers to push updates and upgrades to the software installed in many connected devices and/or to external software dedicated to

[189] *See* Section VI(C).

managing devices. It is imperative in today's cybersecurity environment to "patch" such software as quickly as possible to eliminate security vulnerabilities as they are discovered. Manufacturers can also push updates to maintain a device's secure compatibility over time with new versions of those external software programs and other devices to which they are connected. Depending on the device, patches can either be pushed directly to the relevant software, or they can be made electronically available to the device owner for installation. In either case, health care entities should ensure that, consistent with the entities' change control processes,[190] contracts governing maintenance and support services include requirements for software patching and updating. Those contracts should also allow the entity to hold the manufacturer liable if it fails to provide patches or updates in a timely manner. Having set these requirements, health care entities must have a robust process to assure that installation of any patches or updates provided available by the manufacturer.

C. Security Requirements

Business associate agreements (BAAs) require vendors with access to PHI to maintain a certain level of information security, but most standard form BAAs do not typically shift risk between the parties. As a result, standard BAAs function more to ensure a Covered Entity's compliance with its HIPAA obligations than to shield it from loss and liability due to the Business Associate's insufficient security practices. Many health care entities are accordingly becoming accustomed to negotiating additional security requirements into agreements, especially those for web-based services and other hosting arrangements where their sensitive data will be stored or managed by the vendor on remote systems. Health care entities in today's cybersecurity environment should strongly consider incorporating information security requirements into the terms of *all* transactions involving connected devices. Following are some broadly applicable security

[190] "Change control" is the process used for controlling and recording any changes to a project, system, or product, including an organization's IT system. The approach involves documenting, identifying, and authorizing changes so the impact of each change is evaluated before the decision is made to implement the change.

requirements that health care entities should consider including in connected device purchase agreements, most of which can flexibly be included as vendor representations, warranties and/or covenants:

i. Bill of Materials

As discussed in Section V (due diligence), manufacturers of connected devices should be able to provide a bill of materials for all licensed software or hardware used in the device so that a health care organization can determine if the underlying components have any known vulnerabilities. The contract can require the manufacturer to update the bill of materials when there are significant updates or changes in licenses to the software or firmware of the device.

ii. Security Analysis and Vulnerabilities

The contract should include, perhaps as an exhibit, the results of any security or vulnerability assessment of the device performed by the manufacturer, as well as a timeline for the manufacturer to mitigate any risks identified through the analysis. As noted above, the contract should also require the manufacturer to address, through updates or upgrades, future published vulnerabilities.

iii. Data Validation

As explained in Section V, data validation involves testing the parameters that are used to operate the device in both intended and unintended ways. This is an integral part of software validation during design that should extend into each invocation or use of the device. The contract should include an attestation by the manufacturer regarding the data validation it has performed for the device.

iv. Security Program

Information security is not a concern only for those vendors providing cloud and other hosted services, as alluded to throughout this briefing; it should also be a paramount consideration for manufacturers of connected devices. Health care entities should thus expect connected device manufacturers to have integrated programs in place built around security policies and procedures for the design, manufacture, provisioning, and support of such devices. This expectation should be reflected in the corresponding purchase agreement.

Specifically, health care entities should consider incorporating a requirement that connected device manufacturers maintain and consistently observe a written security policy containing some or all of the following elements:

(1) a general requirement that it provide for effective administrative, physical, and technical safeguards to protect health care entity data from unauthorized disclosure, destruction, alteration, damage, loss and misuse;

(2) limiting access to such data to personnel who have a need to know or otherwise access it to enable provisioning and support of the connected device;

(3) securing networks, facilities, and computing equipment and environments used to support or develop updates for the connected device, including implementing authentication and access controls and the use and review of audit logs;

(4) securing transmission, storage, and disposal of health care entity information obtained through support of the connected device, including encrypting such data when stored on any media or transmitted over public or wireless networks;

(5) conducting risk and vulnerability assessments and periodic penetration testing of connected device versions, and promptly implementing corrective actions in response to any issues identified as a result;

(6) implementing appropriate personnel security and integrity procedures and practices, including conducting background checks; and

(7) providing appropriate privacy and information security training to employees.

v. Development Lifecycle

The security program requirements discussed above primarily focus on a connected device manufacturer's operational security posture. Equally, if not more, important is that a device manufacturer integrate information security and privacy considerations into the connected device design process. Many influential organizations in the fields of device design and security, notably including the FTC, have embraced the concepts of "Security by Design" (SbD) and "Privacy by Design" (PbD) as best practices for the design and development of connected devices.[191] These frameworks essentially require devices to be built from the ground up with security and privacy in mind.

As established in the *Maintenance and Support* discussion above, connected devices are often subject to continuous design and development, and they may be replaced by new versions during the life of a purchasing agreement between the manufacturer and the health care entity. Consequently, health care entities should consider including contractual representations and warranties that manufacturers have and will continue to incorporate SbD and PbD into their device development processes.

vi. Malicious Code

The introduction of malicious code – which is a catchall term encapsulating viruses and other malware, spyware, and even ransomware – remains a primary means by which

[191] FED. TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers (2012)*, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Jan. 8, 2019).

cyber criminals infiltrate devices and networks. An example is where, due to the vendor’s lax security program, a third party is able to introduce malicious code into the connected device.

Device vendors will often seek to narrow the scope of their liability for the effects of malicious code introduced via the connected devices or support services they provide, or to limit the remedies available to device purchasers for the harm they incur as a result. Malware introduced due to the manufacturer’s negligence may harm not only the manufacturer’s device, but also the health care entity’s other network-based systems. Health care entities should strive to incorporate strict vendor liability for the harms they suffer due to the introduction of malicious code as a result of the vendor’s negligence or intentional conduct, including reimbursement for any costs associated with restoring or recreating all systems or data that are lost or damaged.

vi. Remote Access

Manufacturers will often access health care entity networks and computer systems via remote connection in order to provide support and updates for connected devices. This could present a particularly significant risk to health care entities if not properly managed. Specifically, the health care entity is opening up its defensive systems to the flow of data to and from a relatively unknown external source that is manned by relatively unknown external personnel.

The contract should give the health care entity the authority to dictate the means and scope of the vendor’s access to its network, systems, and connected devices. The best practice is to require the vendor’s strict adherence to the health care entity’s remote access policy, which should reflect the entity’s information systems team’s standard remote access controls.

For health care entities without a remote access policy or preferred tools, vendor contracts should require that vendors use remote access tools employing industry standard security protocols. Contracts should also require vendors to ensure that all personnel having access to any part of the entity's network and systems:

(i) are assigned a separate login ID and use only the assigned IDs when logging on;

(ii) log off immediately upon completion of each session of access;

(iii) do not allow access to other individuals;

(iv) keep strictly confidential the log-in IDs and all other information that enables access; and

(v) have their access terminated promptly upon termination of their employment or their reassignment away from providing services to the health care entity.

Contracts should require vendors to maintain and periodically review audit trails of their workforce members' access to the health care entity's systems. Health care entities should also use audit trails to ensure that vendor personnel stay within the bounds of their permitted access.

vii. Data Rights

Vendor personnel in many cases will collect data from connected devices for support purposes, and then will maintain a copy of such data in the vendor's systems. Moreover, many manufacturers see value in the data collected by the connected devices they make and often look to secure contractual rights to collect and use that data for their own purposes to the extent permitted by law. Just as BAAs do not typically shift liability for risk, they are also usually silent on ownership and use rights for data provided to vendors by health care entities beyond those set forth under HIPAA[192] and similar restrictions for personally identifiable information. Health care entities will instead

[192] 45 C.F.R. § 164.502(a)(5) (listing prohibited uses of PHI).

need to include additional contract terms to establish ownership and use rights with respect to the data provided to and generated by connected devices.

Contracts should specify what data the manufacturer may receive from the device. For example, vendors generally would not need PHI or other individually identifiable information, so the contract might limit the vendor to de-identified information. The contract should specify the ownership of data obtained from the device, such as the health care entity's ownership of any PHI.

Contracts should include terms and conditions that define how the manufacturer may use data, such as:

- Limiting use of the data to specifically authorized purposes;
- Requiring the manufacturer to comply with privacy and security standards, laws, and regulations;
- Prohibiting any offshore transfer of the data;
- Giving the health care customer the right to audit the manufacturer's records relevant to the data;
- Limiting the time period that the manufacturer may retain data, and governing destruction and/or disposal of the data; and
- If the manufacturer will maintain data from the device for the entity's use, the contract should also include provisions:
    - Requiring data integrity and availability; and
    - Establishing remedies if a connected device or vendor loses, corrupts, or inappropriately destroys data. This might include the entity's costs for recreating or reconstructing the data.

viii. Security Breach Procedures

Costs incurred due to a security breach of health care data are currently estimated to average $380 per individual record.[193] Considering that an average of 16,060 patients' and other individuals' identifiable records are affected in a single security breach,[194] and the relative inevitability of an entity suffering a breach,[195] the potentially debilitating liability amounts should be among the foremost concerns for every health care entity.

Any agreement for the purchase or support of connected devices that presents an opportunity for vendor or third-party personnel to access PHI or other personally identifiable information should include provisions delineating the parties' responsibilities in the event of a security breach. The events triggering the provision should be defined, such as the unauthorized disclosure of certain data by a vendor or confirmed compromise of vendor's safeguards for such data. To the extent a security incident is attributable to a vendor (for example, connected device design flaws, mistakes made during maintenance and support, bad actors employed by vendor's subcontractors), the agreement should obligate the vendor to a set of responsive actions such as:

- immediately investigating and remediating the incident;
- cooperating with and making information regarding the breach available to the health care entity; and
- involving the health care entity with disclosing the incident to authorities and/or the public.

The contract also should require the vendor to cover or reimburse the health care entity for costs associated with:

[193] Ponemon Institute, *Cost of a Data Breach Study* (2018), https://www.ibm.com/security/data-breach/ (last visited Jan. 8, 2019).

[194] Bitglass, *Healthcare Breach Report 2018* (2018), https://pages.bitglass.com/HealthcareBreachReport2018.html (requires user login).

[195] *See*, e.g., Jennifer Burnett, Council of State Governments E-Newsletter, *Not If, But When* (July/Aug. 2017), https://www.csg.org/pubs/capitolideas/enews/cs17_1.aspx (last visited Jan. 8, 2019).

- providing legally required notifications to affected individuals and regulatory bodies;
- providing identity theft monitoring to affected individuals;
- defending against any lawsuits; and
- any other reasonable response and mitigation activities.

D. Indemnification

If unsuccessful at negotiating an explicit vendor obligation to cover the costs associated with a security incident attributable to the vendor, an option is to negotiate relatively broad vendor defense and indemnity obligations. Defense and indemnification for third-party claims and the health care entity’s related costs and losses that arise from acts, omissions, and/or breaches of the vendor’s contractual obligations can achieve the same result. Even language simply requiring defense and indemnification for third-party claims and the health care entity’s related costs and losses arising from a vendor’s negligent acts and omissions will be effective if the health care entity can establish that the vendor breached a duty of care to safeguard the health care entity’s data.

Connected device manufacturers are hesitant to agree to assume full responsibility to defend and indemnify in situations where the health care entity and/or a third party contributed to the loss. To address this concern—and based on the circumstances (including restrictions on indemnity under applicable state law)—the indemnification provision could be limited so that the vendor must defend and indemnify only to the extent that its negligence or intentional conduct contributed to the loss.

When drafting an indemnification provision relating to a connected device, health care entities should keep in mind that the potential harms go beyond data breaches. Indemnification provisions should also address the risks to patient health and safety that can be created by connected devices.

E. Limitation of Liability

The effectiveness of any of the contractual provisions discussed above will be severely hampered if subject to a vendor-favorable, restrictive limitation of liability provision. Ideally, all vendor obligations and liabilities with respect to the health care entity's data (and patient safety) should be carved out from any limitations on the vendor's total potential liability amounts, as well as any disclaimer of vendor liability for specific types of damages (for example, indirect, incidental, or punitive damages).

However, an unqualified carve-out of this breadth is typically difficult to secure from a vendor. Vendors are often more receptive to moving liability for obligations related to information security and data rights under a heightened "super-cap" wholly separate from the standard liability limitation and not subject to any damages exclusions. A super-cap on vendor liability can often range from ten to twenty times the health care entity's spend under the agreement. Specialized super-caps can make vendors' information security obligations more meaningful, while allowing vendors to retain the ability to quantify contractual risk against expected revenue.

F. Insurance

While negotiating favorable liability limitations in connected device purchase agreements is of paramount importance, they are beneficial only to the extent that the vendor is sufficiently capitalized or insured to cover its liabilities.

Most traditional commercial general liability (CGL) insurance policies include express exclusions for product failures resulting from technological components.[196] Accordingly, a vendor CGL policy is not likely to cover most vendor liabilities arising with respect to connected device security.

[196] *See* Michael K. Stewart*, Insurance for Technology Businesses: Are You Covered?,* http://www.fh2.com/resources/insurance-for-technology-businesses-are-you-covered/ (last visited Jan. 8, 2019).

In order to ensure that vendors have insurance coverage for such liabilities, health care entities should consider incorporating requirements in connected device purchase agreements that require the vendor to maintain cyber coverage. These types of policies have a variety of different names, including "cyber risk," "information security," "technology errors and omissions," "privacy," "media liability," "cyber extortion," and "privacy and network security." These coverages are available both as CGL riders and as standalone policies."[197] Relevant coverage might also be available under other types of policies, such as professional liability insurance or third-party fidelity bond.

Health care entities should accordingly take care to review vendor insurance policies, and even include express contractual requirements, for the following coverages:

> (i) third party financial loss (including, where appropriate, loss due to patient harm) due to the error, omission, or negligence of any vendor personnel;
>
> (ii) blanket employee dishonesty and computer fraud; and
>
> (iii) third party and contractual liability for coverage of defense and indemnification for cybersecurity and privacy incidents, including investigation, notification, discovery, and monitoring costs, regulatory coverage, class action administrative costs, judgments and settlements, as well as cyber threat response costs.

Health care entities can standardize required vendor minimum coverage amounts or can negotiate them on a case-by-case basis by pegging them to liability cap amounts and/or the financial risk associated with the number of individually identifiable records being processed in connection with the relevant connected devices.

[197] Raptis, Steve, *Analyzing Cyber Risk Coverage*, RISK & INSURANCE (March 2015), http://riskandinsurance.com/analyzing-cyber-risk-coverage/ (last visited Jan. 8, 2019).

VII. REPORTING ADVERSE EVENTS AND BREACHES

An adverse event or data breach that involves a connected device can trigger reporting obligations under federal, state, and international law. This section addresses the reporting requirements under FDA regulations, FTC regulations, HIPAA, state breach laws, and the GDPR.

A. FDA's Medical Device Reporting Regulations

The Medical Device Reporting (MDR) regulation[198] mandates that certain device-related adverse events and product problems involving medical devices be reported to the FDA. These requirements are applicable only to manufacturers, importers, and device user facilities involved with medical devices regulated by the FDA.[199] The MDR regulations specify categories of individuals and entities that are exempt from the reporting requirements, and also include a process for manufacturers, importers, and device user facilities to request an exemption or variance.[200]

i. Manufacturers

Manufacturers[201] are required to report to the FDA no later than thirty (30) calendar days after the day they become aware of information that reasonably suggests a device may have caused or contributed to a death or serious injury.[202] Manufacturers also must report to the FDA no later than thirty (30) calendar days after the day they become aware of information that reasonably suggests a device has malfunctioned and that this device or a similar device that they market would be likely to cause or contribute to a death or serious injury if the malfunction were to recur.[203]

[198] 21 C.F.R., Part 803.
[199] *Id.* § 803.1.
[200] *Id.* § 803.19(a)(1)-(3).
[201] *See* definition of "manufacturer" at 21 C.F.R. § 803.3(l).
[202] *Id.* § 803.50(a)(1).
[203] *Id.* § 803.50(a)(2).

In two limited cases, a five (5) day reporting timeframe applies to a manufacturer. First, a manufacturer must submit a report to the FDA no later than five (5) working days after the day it becomes aware of an MDR reportable event that necessitates remedial action to prevent an unreasonable risk of substantial harm to the public health. Second, the FDA may request a five (5) day report for all subsequent events of the same nature that involves substantially similar devices for the time period specified in the written request.[204]

The MDR dictates specific requirements for the content and method of submission of reports.[205] Manufacturers are required to conduct an investigation of each event and evaluate the cause of the event.[206] MDR reporting is not triggered for data breach. Foreign manufacturers whose devices are distributed in the United States are required to designate a U.S. agent to be responsible for medical device reporting and to inform the FDA by letter of the name and address of the designated U.S. agent.[207]

ii. Importers

Importers[208] are required to submit a report to the FDA and to the manufacturer as soon as practicable, but no later than 30 calendar days after the day they receive or otherwise become aware of information from any source—including user facilities, individuals, or medical or scientific literature, whether published or unpublished—that reasonably suggests one of their marketed devices may have caused or contributed to a death or serious injury.[209]

Furthermore, importers must submit a report to the manufacturer as soon as practicable, but no later than 30 calendar days after the day they receive or otherwise

[204] *Id.* § 803.53(a)-(b).
[205] *Id*. §§ 803.50(b)(1)(i)-(iii), 803.56, 803.11(a). Form FDA 3500A is available on the Internet at https://www.fda.gov/downloads/AboutFDA/ReportsManualsForms/Forms/UCM048334.pdf (last visited Jan. 8, 2019).
[206] 21 C.F.R. § 803.50(b)(3).
[207] *Id.* § 803.58(a).
[208] *See id.* § 803.3(j) (defining "importer").
[209] *Id*. § 803.40(a).

become aware of information from any source – including user facilities, individuals, or from their own research, testing, evaluation, servicing, or maintenance of one of their devices – that reasonably suggests one of their devices has malfunctioned and that this device or a similar device they market would be likely to cause or contribute to a death or serious injury if the malfunction were to recur.[210]

iii. Device User Facilities

Device user facilities[211] must report a suspected medical device-related death to both the FDA and the manufacturer. These reports must be made as soon as practicable, but no more than 10 work days after the day the facility became aware of information, from any source, that reasonably suggests a device has or may have caused or contributed to the death of a patient of the facility.[212]

Also, device user facilities must report a medical device-related serious injury to the manufacturer or to the FDA if the medical device manufacturer is unknown. This report must be made no later than 10 work days after the day the facility became aware of information, from any source, that reasonably suggests a device has or may have caused or contributed to a serious injury to a patient of the facility.[213]

Lastly, device user facilities must submit annual reports on Form FDA 3419, including information all of reports made that year.[214] If no medical device reports to manufacturers or to the FDA were made during the time period, no annual report is required.[215]

[210] *Id*. § 803.40(b).
[211] *See id*. § 803.3(d) (defining "device user facility").
[212] *Id*. § 803.30(a)(1).
[213] *Id*. § 803.30(a)(2).
[214] *Id*. § 803.33(a)-(b).
[215] *Id*. § 803.33(d).

B. FDA's MedWatch Program

The FDA encourages health care professionals, patients, caregivers and consumers to submit voluntary reports of significant adverse events or product problems with medical products to the FDA's Safety Information and Adverse Event Reporting Program, known as MedWatch, or through the MedWatcher mobile app.[216]

According to the FDA, the MedWatch form can be used to report adverse events that are observed or suspected for human medical products, including medical devices.[217] The form allows the reporting of several different categories of issues, including "Product Problem (e.g., defects/malfunctions)."[218] Although it appears that the form was designed with adverse events that cause physical harm to patients in mind, the FDA has made it clear that MedWatch can be used to report cybersecurity issues.[219]

C. FTC Breach Reporting Requirements

The FTC has issued a breach notification regulation (FTC Breach Notification Rule).[220] The Rule applies to: (i) vendors of personal health records (i.e., non-HIPAA covered entities and non-HIPAA business associates that offer or maintain a personal health record), (ii) "PHR related entities" (i.e., entities that offer products or services through websites of vendors of personal health records (including HIPAA covered entities), or that access information in or send information to a personal health record), and (iii) "third party service providers" (i.e., entities that offer services involving the use of

[216] *See* FOOD & DRUG ADMIN., *MedWatcher Mobile App*, https://www.fda.gov/MedicalDevices/Safety/ReportaProblem/ucm385880.htm (last visited Jan. 8, 2019); FOOD & DRUG ADMIN., *MedWatch: The FDA Safety Information and Adverse Event Reporting Program*, https://www.fda.gov/Safety/MedWatch/default.htm (last visited Jan. 8, 2019).

[217] FOOD & DRUG ADMIN., *MedWatch Online Voluntary Reporting Form*, https://www.fda.gov/downloads/aboutfda/reportsmanualsforms/forms/ucm163919.pdf (last visited Jan. 8, 2019).

[218] *Id.*, p. 2 of the form.

[219] FOOD & DRUG ADMIN., *Cybersecurity*, https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm (last updated Oct. 31, 2018, last visited Jan. 8, 2019) (stating "We look for and encourage reports of cybersecurity issues through our surveillance of devices already on the market." and including a link to the page that explains both mandatory and voluntary medical device reporting).

[220] 16 C.F.R. §§ 318.1 to 318.9.

unsecured individually identifiable health information to a vendor of personal health records or PHR related entity).[221]

An example of a PHR vendor is an online service (not subject to HIPAA) that allows consumers to store and organize medical information from many sources in one online location. A PHR-related entity would include a business that has an application that helps consumers manage their medications or lets them upload readings from a blood pressure cuff or pedometer into a PHR. Examples of third-party service providers include companies that provide billing, data storage, or debt collection services to a PHR vendor.[222]

The FTC Breach Notification Rule requires notice to individuals and the FTC in the event of an unauthorized acquisition of unsecured identifiable health information contained in a PHR.[223] In certain instances, notice to the media or through the vendor's or PHR-related entity's website is required.[224] The Rule also requires a third-party service provider that discovers a breach to notify the vendor of personal health records or PHR-related entity to which it provides services.[225]

As a growing number of connected devices used in the health care context are not subject to HIPAA (think Fitbit and Apple Watch), the FTC's security and breach notification requirements could become an increasingly important means of addressing data privacy and security concerns with connected devices. The FTC has used its authority under Section 5(a) of the FTC Act,[226] which bars unfair and deceptive acts and practices in or affecting commerce, to bring enforcement actions against companies that

[221] *Id.* §§ 318.1 and 318.2.

[222] FED. TRADE COMMISSION, *Complying with the FTC's Health Breach Notification Rule* (last updated March 2018), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule (last visited Jan. 8, 2019).

[223] 16 C.F.R. §§ 318.2 and 318.3(a).

[224] *Id.* § 318.5.

[225] *Id.* § 318.3(b).

[226] 15 U.S.C. § 45.

the FTC believes have failed to live up to their promises to secure consumers' personal information.[227]

D. HIPAA Breach Notification Rule

Both covered entities and business associates have notification obligations in the event of a HIPAA breach.[228] Not all HIPAA violations are HIPAA breaches. HIPAA specifically defines a breach as "the acquisition, access use, or disclosure of protected health information in a manner not permitted under [the Privacy Rule] which compromises the security or privacy of the protected health information."[229] Although the language in this definition seems to indicate flexibility in determining when a HIPAA violation "compromises the security or privacy of health information," the regulation does not provide much latitude in making that determination.[230] The regulation states that an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach unless the covered entity or business associate demonstrates there is a low probability the PHI has been compromised based on a risk assessment that considers specific factors.[231]

Relevant to connected devices, in 2016 the OCR issued guidance on the issue of whether a ransomware attack constitutes a reportable breach under HIPAA.[232] In that guidance document, the OCR stated that when electronic PHI is encrypted by a ransomware attack, "a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a 'disclosure' not permitted under the HIPAA

[227] FED. TRADE COMMISSION, *Privacy and Security Enforcement webpage*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited Jan. 8, 2019).
[228] *See* Section III(A) for a discussion of the applicability of HIPAA to connected devices.
[229] 45 C.F.R. § 164.402(1).
[230] *Id*.
[231] 45 C.F.R. § 164.402 (subsection 2 under definition of "Breach").
[232] OCR, *Fact Sheet: Ransomware and HIPAA*, https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf?language=es (last visited Jan. 8, 2019).

Privacy Rule."[233] That is a presumptive breach that requires notifications, "[u]nless the covered entity or business associate can demonstrate that there is a '. . . low probability that the PHI has been compromised . . . .'"[234]

E. Reports to Department of Homeland Security's US-CERT

The United States Computer Emergency Readiness Team (US-CERT) was originally created in order to provide a centralized hub of coordination and information sharing between federal organizations regarding cyber breaches. US-CERT offers secure web forms for users to report incidents and submit malware artifacts for analysis.[235] Connected device users experiencing cyber breaches should consider reporting to this federal agency but are not required to do so.[236]

F. State Breach Notification Statutes

Currently, all 50 states – as well as the District of Columbia, Guam, Puerto Rico, and the Virgin Islands – have laws that require reporting of certain data breaches involving personally identifiable information (PII).[237] The state laws, however, vary from each other in their requirements and procedures. In addition, some state laws exempt organizations subject to federal regulation, such as covered entities or business associates under HIPAA, or financial institutions subject to the Gramm-Leach-Bliley Act.[238]

[233] *Id.* at 5-6.
[234] *Id.* at 6.
[235] *See* https://www.us-cert.gov/about-us (last visited Jan. 8, 2019).
[236] US-CERT, *Report Incidents, Phishing, Malware, or Vulnerabilities*, https://www.us-cert.gov/report (last visited Jan. 8, 2019).
[237] For the citations to all state breach reporting laws that were in effect as of March 29, 2018, *see* NAT'L CONF. OF STATE LEGISLATURES, *Security Breach Notification Laws* (Sept. 29, 2018), www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Jan. 8, 2019); *see also* Jonathan M. Joseph, AHLA, *Data Breach Notification Laws: A Fifty State Survey* (American Health Lawyers Association 2d ed.).
[238] *See, e.g.*, ARK. CODE § 4-110-106; WIS. STAT. § 134.98(3m).

Most states require notification to only their affected residents, but some states require notice to *all* affected people.[239]

Most states put the burden of notifying affected individuals on the person or entity that owns or leases the data. A person or entity that is simply maintaining the data is generally required only to notify the owner.[240] However, with connected devices, there could be situations where it is unclear who owns the data – the device manufacturer or the health care organization using the device. This highlights the importance, as mentioned in Section V(C)(vii) above, of addressing in contracts relating to connected devices ownership of data and allocation of responsibilities in the event of breach.

Some states require reporting to state regulators (generally, the state's attorney general or insurance commissioner), or the three credit reporting agencies if the breach exceeds a certain size.[241]

States generally require notifications of breaches involving a person's name in combination with any of the following: social security number; driver's license or state ID card number; or credit card number, debit card number, or financial account number in combination with any password, security code, or access code that would allow access to the account.[242] Some states require notification for breaches of other types of information, including biometric data, taxpayer ID numbers, birth certificates, and medical information.

There are limits on when incidents must be reported. Nearly every state has an encryption/redaction safe harbor; if the requirements of the safe harbor are met, no breach notifications need to be made.[243] Some states have harm thresholds for reporting, which generally provide that reporting is not required if the breached entity

[239] *See, e.g.*, HAW. REV. STAT. § 487N-2(a); N.H. REV. STAT. § 359-C:20(I)(a); N.C. GEN. STAT § 75-65(a); TEX. BUS. & COM. CODE § 521.053(b).

[240] *See, e.g.*, UTAH CODE § 13-44-202(3)(b).

[241] *See, e.g.*, FLA. STAT. § 501.171(3) & (5).

[242] *See, e.g.,* DEL. CODE tit. 6, § 12B-101(4).

[243] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (d)(1)(A).

determines there is no reasonable likelihood of harm to consumers or misuse of personal information.[244]

Many states require that incidents must be reported "in the most expedient time possible and without unreasonable delay . . ."[245] This standard affords the entity reasonable time to quickly investigate the incident to determine what happened so the entity can inform the individuals after having been made aware of the scope and manner of the breach. Some states have imposed specific time limits, such as 30 days.[246] A current trend among states is shortening the time period for notifications. States generally allow a breached entity to delay notifications at the request of law enforcement.[247]

G. GDPR Breach Notification

The GDPR imposes new breach notification obligations on both data *controllers* and data *processors*.[248]

As discussed in Section III(I) above, the GDPR applies to any organization that offers free or paid goods or services to data subjects in the EU, or that monitors EU data subjects' behavior taking place in the EU.[249] For example, the GDPR would apply to the processing of data by a U.S.-based hospital that treats a patient who is located in the EU (for example, the provider remotely monitors the patient after he returns to the EU).[250] However, the GDPR generally would not apply to data that hospitals collect regarding EU subjects while the subjects are located in the United States.

[244] *See, e.g.*, MICH. COMP. LAWS § 445.72(1); KAN. STAT. § 50-7a01(a).
[245] *See, e.g.*, GA. CODE § 10-1-912(a).
[246] *See, e.g.*, FLA. STAT. § 501.171(4)(d).
[247] *See, e.g.*, CONN. GEN STAT. § 36a-701b(d).
[248] A data "controller" is any entity that determines the purposes and means of the processing of personal data. A data "processor" is any entity that processes personal data on behalf of a controller. Commission Regulation 2016/679, art. 4.
[249] *Id.* Art. 3.
[250] Note, however, that EU citizenship or residence of the patient is not, in and of itself, a sufficient basis for the applicability of the GDPR; rather, the trigger is that the patient is *located* in the EU when his data is collected through remote monitoring.

Breach notification under the GDPR is triggered by any "personal data breach," meaning a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored, or otherwise processed.[251] In order to prevent "notification fatigue," the GDPR sets a higher standard for notification to individuals. Controllers are required to notify individuals of a personal data breach only if it is likely to result in a high risk to the rights and freedoms of the individuals.

Under the GDPR, a loss of availability of personal data can constitute a breach, such as when there has been significant disruption to the normal service of an organization (e.g., a power failure or denial of service attack that renders personal data unavailable, either permanently, or temporarily).[252] According to guidance issued by the Article 29 Data Protection Working Party, one example of a situation that would likely require breach notification is when a hospital's "critical medical data about patients are unavailable, even temporarily," because that could lead to cancelled surgical procedures and risks to patients' health.[253]

The GDPR also requires breach notification for some situations involving the loss or destruction of personal data, even if that information is not exposed to a third party. Here are two examples of data loss that, according to the Article 29 Data Protection Working Party, might constitute a reportable breach:

1. "[A] device containing a copy of a controller's customer database has been lost or stolen."

2. "[T]he only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession."[254]

[251] General Data Protection Act, Art. 4.

[252] *Id.* Art. 33; *see also* Article 29 Data Protection Working Party, *Guidelines on Personal data breach notification under Regulation 2016/679* (Oct. 3, 2017), https://iapp.org/media/pdf/resource_center/WP29-Breach-notification_02-2018.pdf (last visited Jan. 8, 2019).

[253] Article 29 Data Protection Working Party, *supra* note 252.

[254] *Id.*

Although the guidance issued by the Article 29 Data Protection Working Party does not address connected devices, these two examples suggest that if personal data contained on a connected device is deleted, and there is no backup copy of that data, the GDPR might require breach notification.

A data processor must notify the controller of the personal data breach without undue delay after becoming aware of it.[255] In turn, the controller must then evaluate whether it is obligated to notify the supervisory authority and the affected individuals. The controller must notify the supervisory authority of a breach when the controller has concluded that the breach is likely to result in a risk to the rights and freedoms of the data subjects. The notification must occur without undue delay and, where feasible, not later than seventy-two (72) hours after becoming aware of the breach.[256] The GDPR dictates specific content that must be included in breach notifications from the controller to the supervisory authority.[257]

The controller must notify affected individuals without undue delay, as soon as reasonably feasible and in close cooperation with the supervisory authority.[258] The notification from the controller to the individuals must also be written in "clear and plain language" and include recommendations for the individual to mitigate potential adverse effects.

The GDPR specifies that no notification to individuals is required if: (1) the controller implemented appropriate technical and organizational protection measures and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorized to access it, such as (state of the art) encryption, and (2) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to is no longer likely to materialize (i.e., the controller may have

[255] General Data Protection Act, Art. 33.
[256] *Id*.
[257] *Id*.
[258] *Id*.

immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it).[259]

Furthermore, in cases when notifying individuals would involve disproportionate effort, the controller may instead issue a public communication whereby the data subjects are informed in an equally effective manner.[260]

In navigating the requirements for breach notification under GDPR, Table 1—which applied broadly to breaches under GDPR—may be helpful in assessing a duty to report or act on a potential breach.[261] Another tool for assessing the need to report breaches is available in a flowchart published by the Article 29 Working Party.[262]

Table 1: Assessing Duty to Report or Act Under GDPR

	Controller to Supervisory Authority	**Controller to Individuals**	**Processor to Controller**
What?	Personal data breach, where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons	When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, but exceptions apply	Personal data breach

[259] General Data Protection Act, Article 33-34; *see* INFORMATION COMMISSIONER'S OFFICE, *Personal Data Breaches*, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ (last visited Jan. 8, 2019).

[260] *Id.*

[261] The editors would like to thank Jodi Erdfarb of Wiggin and Dana LLP for creating and sharing this chart.

[262] Article 29 Data Protection Working Party, *Guidelines on Personal Data Breach Notification under Regulation 2016/679* (adopted on Oct. 3, 2017, and last revised and adopted on Feb. 6, 2018), *available at* http://ec.europa.eu/newsroom/document.cfm?doc_id=47741 (last visited Jan. 8, 2019). This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy.

When?	Without undue delay and, where feasible, not later than 72 hours after having become aware of it	Without undue delay, as soon as reasonably feasible, and in close cooperation with the supervisory authority	Without undue delay after becoming aware of a personal data breach
Content?	1. Describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; 2. Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; 3. Describe the likely consequences of the	1. Include content required in notices from controllers to the supervisory authority; 2. Must be written in clear and plain language; and 3. Must include recommendations for the individual concerned to mitigate potential adverse effects.	

	personal data breach; and 4. Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.		

VIII. Conclusion

The increasing presence of connected devices in health care presents opportunities for improving patient health and treatment, as well as challenges that health care attorneys will play a role in addressing. Those challenges include:

- Security risks with security devices, caused by fundamental design constraints, unclear lines of responsibility within entities that use connected devices, and connectivity approaches (see Section II).
- The multiple sources of federal, state, and international law that govern connected devices in health care, depending on the type of device and user. The relevant laws include HIPAA, FTC security requirements, FDA regulations for medical devices, federal laws relating to the security of electronic information and systems, state cybersecurity laws, and the GDPR of the European Union (see Section III).
- The various legal requirements for reporting adverse events and breaches relating to connected devices (see Section VII).

This briefing suggests a number of different ways for health care organizations and their attorneys to manage the challenges and risks associated with connected devices, including:

- Cybersecurity best practices for connected devices (see Section IV).
- Due diligence regarding connected devices (see Section V).
- Contract provisions relating to the security of connected devices (see Section VI).

The technology of connected devices will not stand still. It will continue to change and evolve. Health care delivery organizations, manufacturers, suppliers, vendors, and the attorneys who represent them need to stay informed about those developments so that they can manage the associated changes in the risks and legal challenges associated with connected devices.