AHLA

Journal of Health & Life Sciences Law

VOLUME 12, NUMBER 3 | JUNE 2019

FEATURED ARTICLES

PRACITCE RESOURCES

OFFICIAL JOURNAL OF AMERICAN HEALTH LAWYERS ASSOCIATION

Practice Resource

Securing Connected Devices in Health Care: Taking Proactive Action

Gerard M. Nussbaum, Elizabeth Hodge, and Scott Bennett[1]

ABSTRACT: Connected devices (e.g., an infusion pump that receives drip instructions from a server and communicates with the EHR, or a continuous glucose monitor that sends data about one's glucose levels to an Android, iPhone, or Apple Watch) are one of the more significant technological advances in health care. There are significant legal implications for their use in health care: data privacy, use and security, patient safety, risk, and liability concerns. As health care becomes more reliant on connected devices, the risks of patient harm, loss of data privacy, and crippling cyber-attack all grow. Failure to identify, allocate, and mitigate the risks can result in patient harm, loss or disclosure of protected health information, serious interruption in the delivery of treatment, significant financial exposure, and loss of patient, employee, and community trust in the provider organization. Understanding and mitigating the risks requires careful assessment and planning. This Practice Resource provides background on the risks and legal requirements for acquiring and using connected devices in health care and suggestions for reducing those risks.

Gerard M. Nussbaum, Elizabeth Hodge & Scott Bennet, *Securing Connected Devices in Health Care*, J. Health & Life Sci. L., June 2019, at 84. © American Health Lawyers Association, www.healthlawyers.org/journal. All rights reserved.

1 This article is based, in part, on the book: Patrick Alston et al., *Innovative Tech: A Health Care Bundle* (Scott Bennett ed. et al., Am. Health Lawyers Ass'n, 2019), https://www.healthlawyers.org/Members/PracticeGroups/HIT/memberbriefings/Documents/HIT_Briefing_Connected_Devices_January2019.pdf. The book explores many of the topics discussed in this Practice Resource in greater depth. The authors would like to thank the other contributors to that book: Patrick Alston, Jiayan Chen, Bethany A. Corbin, Terrence J. Dee, Jody Erdfarb, Stephen C. Grothouse, Maria M. Hilsmier, and Timothy Wright.

Securing Connected Devices in Health Care

ARTICLE CONTENTS

INTRODUCTION

In order to improve patient care and safety, provide for more timely care interventions, and achieve operational efficiencies, health care organizations (HCOs) are increasingly connecting medical devices throughout the enterprise. This allows data to flow bidirectionally between the devices and core information systems, such as the electronic health record. Biomedical devices that are connected to the main hospital network can 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 electronic health record system (EHR); communicate device status, location, and usage; and support updating libraries and protocols on these devices.

Wide Range of Connected Devices

Connected devices are not limited to medical equipment. They span the range from tablet and handheld devices, office equipment, and building controls to security systems, real-time locator services, and asset tracking solutions. These devices are connected by wireless modalities (e.g., WiFi, Bluetooth, RFID, and proprietary means). This manifestation of the Internet of Things (IoT) also encompasses connecting into devices outside the four walls of the hospital or ambulatory treatment facilities, including implanted, home health, wearable, and general consumer technologies; as well as general use data sources (e.g., environmental sensors, traffic monitors).

Connected medical devices, whether worn by patients or implanted, increasingly communicate with the EHR. This communication may be accomplished via apps on a smartphone, such as the Apple iOS Health app, which leverage application programming interfaces (APIs). An API is a software intermediary that functions like a messenger between applications.[2] The EHR certification standards incorporated criteria for APIs, which may enhance this type of communication.[3] 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

2 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.

3 45 C.F.R. § 170.315(g)(7)-(9) (2019).

and will eventually provide a standards-based approach for sharing data amongst connected medical devices, EHRs, and other systems.[4]

The line between more traditional medical devices (which are often subject to Food and Drug Administration regulation) and consumer devices (which are usually not) 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.[5]

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) will still need to be addressed in any data exchange.[6] 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.

Connected Devices Security Risks

Connected devices pose a number of security risks that should be identified and addressed to assure patient safety, information privacy, and uninterrupted operation.[7]

4 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 Summary*, FHIR, http://www.hl7.org/implement/standards/fhir/summary.html (last visited Apr. 19, 2019).

5 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* Letter from Angela C. Krueger, Deputy Dir., Eng'g & Sci. Review, Office of Device Evaluation, Ctr. for Devices & Radiological Health, to Donna-Bea Tillman, Senior Consultant, Biologics Consulting Grp., Inc. (Sept. 11, 2018), https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180044.pdf and Letter from Angela C. Krueger, Deputy Dir., Eng'g & Sci. Review, Office of Device Evaluation, Ctr. for Devices & Radiological Health, to Donna-Bea Tillman, Senior Consultant, Biologics Consulting Grp., Inc. (Sept. 11, 2018), https://www.accessdata.fda.gov/cdrh_docs/pdf18/DEN180042.pdf.

6 The 2015 EHR certification criteria also addressed many of these security aspects through other certification criteria. *See, e.g.*, 45 C.F.R. § 170.315(d)(1), (9), (10).

7 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.

Devices are Difficult to Secure

Connected devices often are built from specific-purpose processors and memory components that have limited processing power, which limits the ability to implement robust security, including using malware protection.

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 is able to be updated as soon as new defenses are developed. The long development and approval cycles for medical equipment, which may exceed five years, act as a barrier to utilizing the same approach for connected medical devices. 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 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. Thus, legacy devices with limited security protections are kept in service for longer periods of time.

Unclear Lines of Responsibility Contribute to Security Risks

Responsibility within a health system for connected device security is often not clear. Biomedical devices are managed and maintained by a dedicated department (clinical engineering), which is not part of the information technology department, where the majority of security personnel is located. This gap means that medical devices are not

always tracked or monitored from a security perspective, and do 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.[8] 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, including medical devices, is the failure of responsible individuals to apply security patches in a timely manner. There has been a misperception that applying patches to biomedical equipment is prohibited under FDA regulations.[9] Security patches that do not affect the underlying function or operation of the device may be applied without seeking further FDA approval.[10, 11] 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.[12]

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 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 based on concerns about potential harm to patients or the organization's operational capabilities. Equipment vendors and provider organizations are becoming more proactive in addressing these areas, but challenges remain.

---

8 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 Corporation attack entered the Target network through a third-party heating, ventilation, and air conditioning maintenance vendor that had access to the Target network in order to deliver its services.

9 FDA regulation of medical devices is discussed more fully in this article at Current Legal Framework, The U.S. Food & Drug Administration (FDA) Regulations of Medical Devices, pg. 94.

10 *Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software,"* FDA, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/information-healthcare-organizations-about-fdas-guidance-industry-cybersecurity-networked-medical (last updated June 28, 2018).

11 *Id.*

12 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 id.*

Medical devices may be assembled from constituent parts that are supplied by a multitude of suppliers, which can mask inherited security risks in the constituent parts that comprise the final medical device. 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. It's challenging to anticipate how cybercriminals will morph their approach in the future and include these future attack vectors in testing today.[13]

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.

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 (small hardware devices that plug into the biomedical equipment's serial port or maintenance access port) that externally add network connectivity to legacy equipment to provide network connectivity, data transfer, or even control over functions of the biomedical equipment. These dongles usually do not include security protections and are difficult or impossible to patch. This results in putting unprotected devices on the network, and thus accessible to cyberattack, both on the device as well as a launching point for attacking other network attached systems. 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, 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

13 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.

does not include connected medical devices, then the organization may be blind to malicious activity occurring on the network.

Potential Patient Harm

A significant risk factor with connected medical devices is the potential for patient harm. While there have not been any reported patient deaths directly linked to attacks on connected medical devices, there are a number of ways in which compromised connected devices could harm patients.[14] These risks from intentional cyberattack are in addition to the risks to patients from the increasing complexity of software and firmware associated with medical devices, which are more appropriately classified as potential product defects.

The degree of harm caused by a cyberattack on a connected medical device will be heavily influenced by the ability of caregivers to identify that the device has been attacked, and to intervene to prevent or mitigate patient harm. For example, if a cyberattack were to interfere with the functioning of a ventilator alarm, a deterioration in the patient's condition might not be noticed in a timely manner, leading to hypoxic brain injury or death due to inadequate ventilation. This interference could be accomplished by rendering the alarm function inoperative, disabling the monitoring device entirely, or by degrading the performance of the device so that the alarm is sufficiently delayed as to lead to irreversible patient harm before a caregiver can respond.

If a cybercriminal were to take control of a connected infusion pump, he or she could speed up or slow down the infusion rate, potentially leading to patient harm. Similar risks would be present if a cybercriminal gained access to an implantable device such as a pacemaker or insulin pump, or a connected base station. As the FDA noted in a safety alert regarding the need to update firmware in a pacemaker, "Many medical devices . . . contain configurable embedded computer systems that can be vulnerable to cybersecurity intrusions and exploits."[15] In 2013, the potential risks from connected pacemakers came to the public's attention through media reports that former Vice President Dick Cheney had the wireless functionality of his pacemaker

14 The intent of this section is to provide examples to assist the reader in understanding the potential magnitude of patient harm that could result from connected medical devices. It is not intended to address all of the potential methods of attack on a connected medical device, or to delve into the technical details of a potential attack.

15 *Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication*, FDA (2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (last updated Oct. 18, 2017).

disabled, out of concern that the device could be hacked in an assassination attempt.[16] Other attacks could be used to compromise data on the device itself, such as drug libraries on an infusion pump or stored treatment protocols.

Researchers, including some who have attempted to hack their own medical devices, have shown the potential for cyberattacks on connected devices.[17] In many cases, these demonstration attacks required some level of physical proximity to gain access to the device (though proximity for a wireless attack could be from a substantial distance away from the device). However, as the general success of phishing messages has shown, it is not difficult to recruit the unwitting assistance of technology users to aid in a cyberattack. Also, a patient or another person with physical access to the device could seek to alter the device for his or her own purposes, such as reprograming a patient-controlled pain pump which could cause addiction or even respiratory arrest and death.[18]

Attacks on connected medical devices may also be used to infiltrate and compromise other systems on the network, such as the EHR. Access to the EHR could enable a cybercriminal to alter data to cause patient harm, for example by changing allergy information or altering medication records. In these examples, the connected medical device would be merely serving as a gateway for the cybercriminal to gain access to other systems.

Connected devices may be a pathway by which ransomware is able to infiltrate a provider's network, as was seen in the 2017 attack that brought down the U.K National Health Services (NHS), as well as hospitals in the U.S. NHS patients scheduled for heart surgery had their operations cancelled, clinicians' lack of access to records raised the potential that medication allergies would not be noticed, and recent test results were unavailable.[19] Loss of key medical devices and information systems during an active surgical procedure due to ransomware, other malware, or deliberate impairment or inoperability could have grave consequences for the patient.

16 Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, N.Y. Times, Oct. 21, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.97187ca0ee8e.

17 Ms. Smith, *Hacking Pacemakers, Insulin Pumps and Patients' Vital Signs in Real Time*, CSO (Aug. 12, 2018), https://www.csoonline.com/article/3296633/hacking-pacemakers-insulin-pumps-and-patients-vital-signs-in-real-time.html.

18 Arezu Sarvestan, *Hospital Patient Hacks His Own Morphine Pump*, Mass Device, Aug. 15, 2014, https://www.massdevice.com/hospital-patient-hacks-his-own-morphine-pump-massdevicecom-call/.

19 Henry Bodkin et al., *Government Under Pressure After NHS Crippled in Global Cyber Attack as Weekend of Chaos Looms,* The Telegraph, May 13, 2017, https://www.telegraph.co.uk/news/2017/05/12/nhs-hit-major-cyber-attack-hackers-demanding-ransom/.

Looking more broadly, attacks on facilities' connected devices could result in loss of key power, environmental, and support systems. For example, interference with connected devices in utility systems could cause loss of power and inability of the backup systems to come online. This could significantly affect patient care, especially among high acuity patients, those undergoing a procedure, or those needing transportation to receive appropriate care. While not caused by a cyberattack, the challenges posed to the health care system by Hurricane Katrina in 2005 illustrate the kind of worst-case scenario that could result from an attack on power and other utility systems.

Even when a cyberattack leads to patient harm, the cause of the injury may not be obvious to those responding and thus may not be attributed to a cyberattack. This could lead to a failure to engage in the necessary forensic analysis as part of the post-event, root-cause analysis, resulting in underappreciation of the dangers posed by unsecure connected devices, as well as a failure to take necessary remedial actions to prevent reoccurrence.

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 patchwork of major laws and regulations pertaining to cybersecurity of connected devices.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA), and particularly its security standards (Security Rule), may apply to the use of connected devices in health care in several ways. Entities that develop or support the operation of a connected device may be subject to HIPAA because they are covered entities or business associates. For example, 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 might be subject to HIPAA.[20] The Department of Health and Humans Services, Office for 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.[21]

20 *See* Health App Use Scenarios & HIPAA 3 (2016), https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf.

21 45 C.F.R.§ 160.404 (2019).

Even where HIPAA does not apply to the device manufacturer, it may nonetheless be an important consideration based upon how the device is used, such as where the device interacts with an electronic medical record platform or other HIPAA-regulated data system.

U.S. Food & Drug Administration (FDA) Regulation of Medical Devices

The Food, Drug, and Cosmetic Act (FDCA)[22] regulates "medical devices," which can be tangible devices, software, or some combination thereof. Connected devices regulated by the FDA include biomedical equipment, implanted devices, home health equipment, and sometimes, adjunctive devices. Generally, consumer products are not a "medical device" 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).[23]

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. Connected medical devices lacking adequate controls may present cybersecurity risks that can adversely affect device functionality, disrupt the delivery of health services, and lead to patient harm.[24] Unlike OCR, the FDA focuses on cybersecurity risks "impacting the safety and effectiveness of the device," [25] rather than risks to patient privacy.

Federal Trade Commission (FTC) Security Requirements

The FTC's enforcement authority stems primarily from Section 5 of the Federal Trade Commission Act (FTCA), a statute designed to protect consumers from "unfair or deceptive acts or practices in or affecting commerce . . . ."[26] The FTC's Section 5 enforcement authority is limited to an act or practice which "[must] cause[] or [be]

22 Federal Food, Drug, and Cosmetic Act, 21 U.S.C. §§ 301–399i (2019).

23 *E.g.,* the Apple Watch Series 4 received FDA Class II clearance for both the EKG and atrial fibrillation functionality; *see* n. 5.

24 Suzanne Martin, Deputy Inspector Gen. for Evaluation & Inspections, U.S. Dep't of Health & Human Servs., Office of Inspector Gen., FDA Should Further Integrate Its Review of Cybersecurity into the Premarket Review Process for Medical Devices (2018), https://oig.hhs.gov/oei/reports/oei-09-16-00220.pdf.

25 FDA, FDA Fact Sheet: The FDA's Role in Medical Device Cybersecurity, https://www.fda.gov/downloads/medicaldevices/digitalhealth/ucm544684.pdf.

26 15 U.S.C. § 45(a).

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."[27] The FTC may view security flaws as an unfair or deceptive trade practice. The FTC has issued numerous guidance documents on data security, including for mobile health app developers[28] and in the context of the IoT.[29] The FTC's authority is important because it covers many connected devices and their uses that are not subject to either HIPAA or under the jurisdiction of the FDA.

State Cybersecurity Laws

Many states have cybersecurity and/or data breach laws that, while not specifically targeted at connected devices, might apply to those devices.[30] These laws typically apply to any entity that acquires, maintains, or uses personal information. State laws may also require that covered entities take reasonable measures to protect and secure personal information that is in electronic form and, importantly, may provide a private right of action for individuals that HIPAA, the FTC Act and FDA regulations do not.[31] Biometric privacy laws may also become an issue for connected devices.

In what may be a sign of the future, in September 2018, California became the first state to enact a law that mandates security features for connected devices. Effective in January 2020, the California law requires any manufacturer of a device that connects "directly or indirectly" to the internet to protect the device with "reasonable" security features.[32]

General Data Protection Regulation (GDPR)

The GDPR imposes extensive protections for the personal data of European Union (EU) data subjects.[33] 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'

27 *Id.* § 45(n).
28 *See Data Security*, FTC, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Apr. 20, 2019).
29 FTC, Careful Connections: Building Security in the Internet of Things (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.
30 *Computer Crime Statutes: Laws Addressing Ransomware and Computer Extortion*, NCSL, http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (last updated Jan. 31, 2019).
31 *See, e.g.*, Fla. Stat. § 501.171.
32 S.B. 327 (Ca. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327.
33 Commission Regulation 2016/679, art. 99, 2016 O.J. (L 119).

behavior taking place in the EU.[34] Thus, a U.S.-based developer of a mobile medical app that is downloadable by EU residents could be subject to the GDPR. Likewise, the GDPR would also apply to a U.S.-based hospital that remotely monitors a patient after he returns to the EU.[35]

Although the GDPR was enacted by the EU, its enforcement could vary by country since member countries may adopt their own conditions relating to processing of genetic data, biometric data, and data concerning health,[36] thereby creating challenges for device manufacturers that conduct business globally.

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 existing federal laws, as neither HIPAA nor the FTCA provide for a private right of action. Nonetheless, certain state data protection and/or consumer protection laws may authorize such actions,[37] and individuals may also seek relief in courts under common law theories of liability, such as 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.[38] Connected device manufacturers and HCOs using these devices should closely monitor the case law regarding private rights of action as this area is evolving and can vary by jurisdiction.

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

34 *Id.* art. 3.

35 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.

36 Commission Regulation 2016/679, art. 9(4).

37 *E.g.,* Cal. Civ. Code § 1798.84 (2019) (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 (2019) (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).

38 *See* Katherine Booth Wellington, *Cyberattacks on Medical Devices and Hospital Networks: Legal Gaps and Regulatory Solutions*, 30 Santa Clara High Tech. L.J. 139, 175–82 (2014), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1578&context=chtlj (discussing various theories of tort liability for cyberattack injuries).

typically not HIPAA-covered entities; determining whether they are business associates is a highly fact-intensive analysis. Many solutions that interface with a health care provider's data systems—particularly those that support health management functions—also fall outside the FDA's jurisdiction or oversight focus. For products and solutions that do not fit 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.

CYBERSECURITY BEST PRACTICES FOR CONNECTED DEVICES

Building an Effective Cybersecurity Compliance Program

In addition to complying with the applicable legal requirements for cybersecurity,[39] health care providers and organizations can improve their cybersecurity frameworks for connected devices by drawing on general principles for effective compliance programs. 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;
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.[40]

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

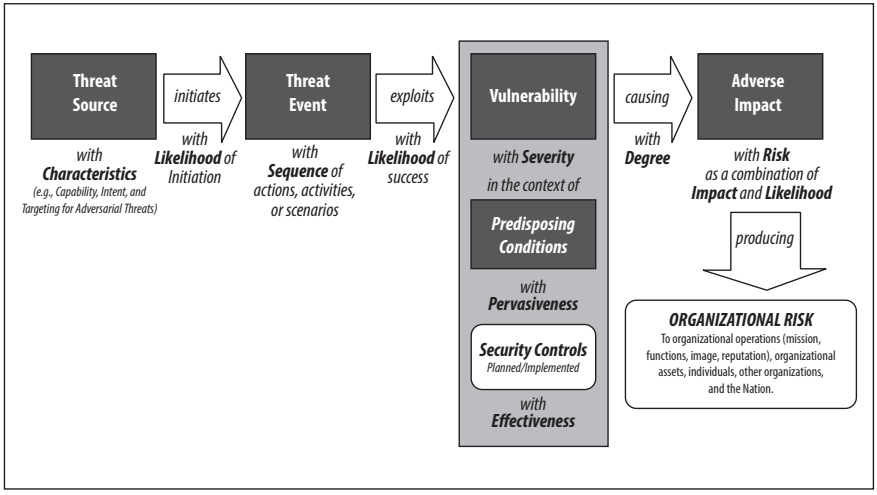
39 For example, the HIPAA Security Rule sets out cybersecurity requirements for covered entities and business associates.

40 *See* Publication of OIG Compliance Program for Clinical Laboratories, 63 Fed. Reg. 45076, 45076–79 (Aug. 24, 1998).

Risk Assessment

HCOs should develop and implement approaches for identifying and mitigating potential threats and vulnerabilities to connected devices.[41] 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.[42] 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. Figure 1 provides an overview of the risk assessment process.

Figure 1: Risk Assessment Process



41 Paul Otto, Hogan Lovells, *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/.

42 *See, e.g.*, HITRUST, Healthcare Sector Cybersecurity Framework Implementation Guide 19 (2016), https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

For connected medical devices, it is important that HCOs and device manufacturers are attentive to the risks posed to data and patient safety throughout the lifecycle of the product.[43] 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.[44] Although an entity's perspective may depend to a large extent on whether it is a device manufacturer, HCO or business associate, 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.

Connected device manufacturers' 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,[45] 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."[46] 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-critical communications regarding cybersecurity events reach not only their traditional contact points within customer organizations, but also encompass those customer departments responsible for cybersecurity.

43 Otto.
44 *Id.*
45 Security by design is a key element in the FDA Cybersecurity Guidance.
46 FDA, Postmarket Management of Cybersecurity in Medical Devices, at 13–14 (Dec. 28, 2016).

HCOs addressing connected medical device cybersecurity risks should consider internal as well as external threats. Connected device risk should be part of the overall organization cybersecurity risk assessment.

Training and Education

Training and education are crucial components of a strong cybersecurity program. Insiders, either through malicious action or error, are responsible for a large portion of data breaches.[47] Training and education should cover relevant cybersecurity policies and procedures, as well as industry trends and specific cybersecurity threats associated with connected medical devices.[48] 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). Employees should also be made aware during training that improper access to patient data could lead to disciplinary action.[49] 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.[50]

Proactive Monitoring

HCOs 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.[51] Such testing should ideally be conducted at frequent and regular intervals, as well as when major personnel and process changes occur at the

47 Verizon, Protected Health Information Data Breach Report 4 (2018), http://www.verizonenterprise.com/resources/protected_health_information_data_breach_report_en_xg.pdf.

48 HIMSS N. Am., 2018 HIMSS Cybersecurity Survey, at 22 http://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf (noting that security awareness training of workforce members is crucial).

49 *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).

50 Dep't Health & Human Servs., Top 10 Tips for Cybersecurity in Health Care, at 2, https://www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf (last visited Jan. 8, 2019).

51 *See* 2018 HIMSS Cybersecurity Survey, at 20.

organization that impact the cybersecurity program.[52] HCOs should also consider implementing formalized insider threat management programs.[53]

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 security of electronic personal health information (ePHI).[54] 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.[55] Physical safeguards encompass measures that protect buildings and equipment from unauthorized intrusion, destruction, or disasters.[56] Finally, technical safeguards refer to technology, policies, and procedures that are used to protect ePHI and control access to it.[57] The HIPAA Security Rule provides in-depth guidance regarding the expectations for implementing these safeguards.

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 HCOs to consider risk-shifting and mitigation options that may be helpful in the event of a breach or hack.[58] A cyberattack involving personal data is massive, has an average cost of $3.7 million per incident,[59] excluding the cost of patient injury or death if a connected device is compromised.

One such option is cybersecurity insurance. Most general insurance policies do not cover losses and liabilities associated with cyberattacks, such as a breach or hack

52 *Id.* at 5, 20.
53 *See id.*, at 20.
54 45 C.F.R. §§ 164.308, .310, .312 (2019).
55 *Id.* § 164.304.
56 *Id.*
57 *Id.*
58 Lena J. Weiner, *Cybersecurity Insurance Basics for Healthcare Organizations*, HealthLeaders (June 8, 2015), http://www.healthleadersmedia.com/technology/cybersecurity-insurance-basics-healthcare-organizations.
59 Clemens Scott Kruse et al., *Cybersecurity in Healthcare: A Systematic Review of Modern Threats and Trends*, 25 Tech. & Health Care 1, 1, 6 , 7 (2017), https://content.iospress.com/download/technology-and-health-care/thc1263?id=technology-and-health-care%2Fthc1263.

of a connected medical device.[60] 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 cyber-insurance will cover financial liability resulting from patient injury or death. Therefore, HCOs 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.[61] In the event of a breach, the HCO can call its cyber-insurance carrier and receive access to a team of specialists ready to respond to the breach incident quickly.[62] Quick access to a team of specialists can result in faster breach containment and reduced liability.

HCOs 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 cybersecurity incident.

Due Diligence

Evaluating the capabilities and practices of connected device manufacturers should be a part of the HCO'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.

Privacy Impact Assessment

As an adjunct to the security risk assessment, a privacy impact assessment (PIA) may be useful to ensure that each connected device has the necessary security and privacy controls in place to protect the confidential data held by the organization. The PIA focuses on whether the appropriate security, business, technological, legal and/or infrastructure mitigations are in place to minimize identified risks to data privacy. In

60 There have been no reported incidents of a patient death or bodily harm directly caused by a cybersecurity incident.
61 *Id.*
62 *Id.*

order to properly vet the potential risks of a connected device, the PIA process should include the collaboration of experts in information technology, clinical engineering, security, data management, privacy and legal; as well as vetting the security controls and practices of the manufacturer related to the development and maintenance of a medical device, and the security knowledge and maturity of the device provider.

Known Security Vulnerabilities

Security vulnerabilities are a fact of life for many devices. Bugs in code, "backdoors" left by manufacturers, dependencies on third- and fourth-party application programming interfaces, and defined methods of communication between software components are all vectors that may be exploited. Organizations should implement mitigating controls when a vulnerability is identified.

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 HCO, 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 HCOs timely apply patches provided by the manufacturers.

Since very little software and hardware is developed solely by the connected device manufacturer, 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 HCO's overall IT environment. Manufacturers of connected devices should be able to provide a bill of materials for all software or hardware used in the device so that an HCO 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 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 whether a manufacturer has developed the device/software in a secure fashion, HCOs should determine if the following has occurred:

- *Data validation*.[63] This involves testing the parameters that are used to operate the device, in both intended and unintended ways.[64] Understanding the valid input for any device and properly handling invalid input helps defend against the majority of security weaknesses.[65]
- *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.

Security Risk Analysis

HCOs 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."[66] Entities should evaluate the performance of the device in conjunction with existing security controls like segregated networks, access controls, intrusion detection and connectivity methods.

Large HCOs 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
- 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.[67]

---

63 *Data Validation*, OWASP, https://www.owasp.org/index.php/Data_Validation (last modified Dec. 1, 2013).

64 FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff (2018), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.

65 *OWASP Top 10 Privacy Risks Project*, OWASP, https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project (last modified Mar. 4, 2019).

66 45 C.F.R. § 164.308(a)(8) (2019).

67 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.

Ongoing Monitoring

Due diligence does not stop when the contract for purchase 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 be required. The manufacturer may supply the monitoring as a service, and the security aspects of this service should be clearly documented in the final acquisition and services agreement.

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 HCO through the use of industry and governing agencies resources and tools (e.g., the OCR breach portal[68] and the FDA medical device recall database)[69] 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 HCO. This may change the overall risk posture as device usage expands or contracts. When performing HIPAA risk assessments, HCOs 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 each manufacturer 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 also 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

68 *Breach Portal*, OCR, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited Apr. 21, 2019).
69 *Medical Device Recalls*, FDA, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm (last updated Apr. 20, 2019).

changes to licenses, privacy practices, or security capabilities to be sure that the risk assessment and 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.

CONTRACTING FOR CONNECTED DEVICES

As discussed above, the substantial level of security risk associated with connected devices for HCOs 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. HCO 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. While many digital health solutions are being deployed in a direct-to-consumer fashion rather than on behalf of covered entities, HIPAA continues to be relevant as an industry benchmark and should be incorporated into contractual requirements.

HCOs are largely left to manage risks with respect to their patients' safety and data on their own. Too often, HCOs 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 HCO systems.

This should not, and does not, have to be the case with respect to connected devices. HCOs can enhance security through effectively contracting for connected devices. This includes basic contract provisions to shift and mitigate security risks identified during the due diligence process as part of the procurement process.

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 HCO's operation. 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, HCOs 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. 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, HCOs should exercise care to narrowly tailor the remedy to the warranty breach claim itself, and not related claims.

Maintenance and Support

For most connected devices, a performance warranty is insufficient 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. HCOs 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 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 HCO's network to service a connected device directly. This remote access to the network raises additional security concerns for the HCO that should be addressed in the contract.

Device connectivity may enable manufacturers to push software and firmware updates and upgrades to connected devices and/or to external systems dedicated to 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 device, or they can be made electronically available to the device owner for installation. In either case, HCOs should ensure that, consistent with the entities' change control processes,[70] 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 or if the updates lead to harm or diminished device functionality. Having set these requirements, HCOs must have a robust process to assure that installation of any patches or updates provided are available by the manufacturer.

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

Bill of Materials

Manufacturers of connected devices should be able to provide a bill of materials for all software or hardware used in the device so that an HCO 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 the software or firmware of the device.

70 "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.

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.

Data Validation

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.

Security Program

Information security is not a concern only for those vendors providing cloud and other hosted services; it should also be a paramount consideration for manufacturers of connected devices. HCOs 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, HCOs should consider incorporating a requirement that connected device manufacturers maintain and consistently observe written security policies containing some or all of the following elements:

1. a general requirement that it provide for effective administrative, physical, and technical safeguards to protect HCO 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 HCO 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.

Development Lifecycle

The security program requirements discussed above primarily focus on a connected device manufacturer's operational security posture. A device manufacturer should also 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.[71] These frameworks essentially require devices to be built from the ground up with security and privacy in mind.

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 HCO. Consequently, HCOs should consider including contractual representations and warranties that manufacturers have, and will continue, to incorporate SbD and PbD into their device development processes.

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 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.

71 FTC, 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.

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 HCO's other network-based systems. HCOs 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.

Remote Access

Manufacturers will often access HCO networks and computer systems via remote connection in order to provide support and updates for connected devices; this results in the HCO opening up its defensive systems to external systems that may not be fully controlled or managed according to the HCO's security requirements. This could present a particularly significant risk to HCOs if not properly managed.

The contract should give the HCO 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 HCO's remote access policy, which should reflect the entity's information systems team's standard remote access controls.

For HCOs 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:

1. are assigned a separate login ID and use only the assigned IDs when logging on;
2. log off immediately upon completion of each session of access;
3. do not allow access to other individuals;
4. keep strictly confidential the log-in IDs and all other information that enables access; and
5. have their access terminated promptly upon termination of their employment or their reassignment away from providing services to the HCO.

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

Data Rights

Vendor personnel in many cases will collect data from connected devices for support purposes; maintaining a copy on the vendor's systems. Manufacturers see value in the data from connected devices and often look to secure contractual rights to collect and use that data for their own purposes. 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 HCOs beyond those set forth under HIPAA[72] and similar restrictions for personally identifiable information. HCOs will instead 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 HCO's ownership of any PHI and its operational data, with a limited use license granted to the manufacturer.

Terms of this use data license may include:

- Limiting use of the data to specifically authorized purposes;
- Requiring compliance 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;
- 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.

72 45 C.F.R. § 164.502(a)(5) (listing prohibited uses of PHI).

Security Breach Procedures

Costs incurred due to a security breach of health care data are currently estimated to average $380 per individual record.[73] Considering that an average of 16,060 patients' and other individuals' identifiable records are affected in a single security breach,[74] and the relative inevitability of an entity suffering a breach,[75] the potentially debilitating liability amounts should be among the foremost concerns for every HCO.

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 HCO; and
- involving the HCO in disclosures to authorities and/or the public.

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

- 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.

73 Ponemon Inst., The Fourth Annual Study Cost of a Data Breach Study (2019), https://www.ibm.com/security/data-breach/.

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

75 *See, e.g.*, Jennifer Burnett, *Not If, But When,* Council of State Governments E-Newsletter, July/Aug. 2017, https://www.csg.org/pubs/capitolideas/enews/cs17_1.aspx.

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 HCO's related costs and losses that arise from acts, omissions, and/or breaches of the vendor's contractual obligations can achieve a similar result. Even language simply requiring defense and indemnification for third-party claims and the HCO'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 HCO's data or patient safety.

Connected device manufacturers are hesitant to agree to assume full responsibility to defend and indemnify in situations where the HCO 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, HCOs 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.

Limitation of Liability

The effectiveness of any contractual provision 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 HCO'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 HCO's spend under the agreement. Specialized super-caps can make vendors' infor-

mation security obligations more meaningful, while allowing vendors to retain the ability to quantify contractual risk against expected revenue.

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.[76] Accordingly, a vendor CGL policy is not likely to cover most vendor liabilities arising with respect to connected device security.

In order to ensure that vendors have insurance coverage for such liabilities, HCOs 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.[77] Relevant coverage might also be available under other types of policies, such as professional liability insurance or third-party fidelity bond.

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

1. third party financial loss (including, where appropriate, loss due to patient harm) due to the error, omission, or negligence of any vendor personnel;
2. blanket employee dishonesty and computer fraud; and
3. 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.

76 *See* Michael K. Stewart, *Insurance for Technology Businesses: Are You Covered?*, Friend, Hudak & Harris LLP, http://www.fh2.com/resources/insurance-for-technology-businesses-are-you-covered/ (last visited Apr. 25, 2019).

77 Steve Raptis, *Analyzing Cyber Risk Coverage*, Risk & Ins., Mar. 13, 2015, http://riskandinsurance.com/analyzing-cyber-risk-coverage/.

When considering the variety of insurance coverage and indemnities required of a vendor, the HCO will need to assess the types of incidents that may occur and the corresponding type of cybersecurity incident and fallout for each type of incident. For example, an incident where the weaknesses in the vendor's product permitted a malicious actor to access PHI would need to address all of the aspects associated with a breach under HIPAA and other privacy laws, including direct and indirect costs. If the malicious actor altered data or impaired the operation of the device or connected systems, the vendor indemnifications would need to cover the business interruption and recovery costs, as well as the actual or potential harm to patients or HCO staff. Other intangible costs, such as loss of reputation may also be appropriate to include among the indemnifications requested by the HCO when negotiating an agreement with a vendor. Untangling responsibility for such adverse incidents is difficult; the recommendation therefore is—in addition to assuring that the HCO is appropriately protected through contractual indemnifications and the vendor has sufficient applicable insurance coverage to make good on the vendor's contractual commitment—the HCO should also assure that it has appropriate insurance coverage for these types of incidents in the event responsibility for the adverse outcomes of a cybersecurity incident is shared between the vendor and the HCO.

HCOs 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.

THE NEVER-ENDING BATTLE FOR SAFE USE OF CONNECTED DEVICES

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 associated with any connected device as cybercriminals constantly develop ways to overcome new cybersecurity defenses. As such, ongoing vigilance is needed. Organizations can mitigate the risks associated with connected devices by understanding the legal framework and the nature of the risks, undertaking necessary due diligence and countermeasures, and assuring that responsibility is appropriately allocated through contracts. Attorneys advising health care provider and vendor organizations need to keep pace with the changes occurring to support their ability to counsel their employers and clients. J

PROVIDER-VENDOR CONTRACTS: A CHECKLIST OF TERMS

1. Patching
   a. Clearly identify who has responsibility for identifying the need for patches, when and how the vendor will provide patches.
   b. Specify who has the responsibility for installing patches.
   c. Address the effect of patches on support and warranties.
   d. Provide that the manufacturer is liable if it fails to provide patches or updates in a timely manner.
2. Business Associate Agreement
   a. Evaluate all vendors of connected devices to ascertain if they are BAs.
   b. Maintain a central inventory of all BAAs.
   c. Periodically review each vendor to determine if BA status has changed, and confirm there is a current BAA in place.
3. Use uniform privacy and security requirements, based on HIPAA and industry best practices, for all vendors (whether BA or non-BA).
4. Require vendor to provide information about vulnerabilities and cybersecurity events. Specify the threshold for reporting, the timeframe, and the specific department(s) or people within the provider organization who must be notified.
5. Require vendor to disclose known vulnerabilities and past security incidents as part of the acquisition process, and reference these representations in the agreement.
6. Require the vendor to provide a bill of materials for all licensed software or hardware used in the device, and update the bill annually or when there are significant changes in licenses to the software or firmware.
7. Require the manufacturer to provide annual attestations/certifications by independent third parties for critical security controls.

Provider-Vendor Contracts: A Checklist of Terms *continued*

8. Include provisions that address:
    a. Performance warranties
    b. Maintenance and support, including safeguards if manufacturer will have remote access to the provider's network
    c. The manufacturer's obligation to address currently known and later discovered security vulnerabilities
    d. The data validation the manufacturer has performed for the device
    e. The manufacturer's obligation to maintain and consistently observe a written security program
    f. The manufacturer's obligation to incorporate Security by Design and Privacy by Design into the development of the connected device
    g. Indemnification, specifically addressing patient injury and breaches of the provider's data
    h. Ownership and use rights with respect to the data provided to and generated by the connected device
    i. The parties' responsibilities in the event of a security incident or breach
    j. The manufacturer's obligation to have adequate insurance

PROVIDER-VENDOR CONTRACTS: SAMPLE PROVISIONS

Indemnification

Manufacturer/Vendor will indemnify, defend, and hold harmless Health Care Provider and its directors, officers, employees, agents, affiliates, and subsidiaries from and against that portion of any and all actions, claims, lawsuits, liabilities, demands, causes of action, costs, expenses, and damages (including reasonable attorney's fees) arising from or relating to the Connected Device. Manufacturer/Vendor's obligations under this section survive the expiration or termination of this agreement.

Limit on "sole and exclusive remedy" provision

[The "sole and exclusive remedy" provision] applies only to claims of breach of an express warranty by Manufacturer/Vendor. That provision does not apply to, or limit in any way, any other rights or remedies of Health Care Provider or liability of Manufacturer/Vendor arising from or relating to the Connected Device or this agreement.

Carve outs for limitations on liability

[The provision(s) limiting liability] do/does not apply to, or limit in any way, any rights or remedies of Health Care Provider or liability of Manufacturer/Vendor arising from or relating to (1) an injury to a patient of Health Care Provider, or (2) any acquisition, access, use, or disclosure of Health Care Provider's patient or other information that violates any federal or state law or Manufacturer/Vendor's obligations under this agreement.

Author Profiles

GERARD M. NUSSBAUM With over 30 years of health care and industry experience, Gerard is a trusted advisor to the executive teams of major health care providers and digital health firms. He focuses on the intersection of information technology, strategy, operations, finance, and legal/regulatory matters to help guide clients in addressing a wide variety of challenges. Gerard has deep experience in information technology strategic planning, regulatory compliance programs, merger and acquisition planning and execution; and interim management. Gerard is a regular author and speaker at leading industry events. Gerard has provided leadership and expertise to academic medical centers, health systems, community hospitals, and digital health firm clients in many areas. Contact him via email at gerard@zarachassociates.com.

ELIZABETH HODGE is Of Counsel at Akerman LLP in West Palm Beach, FL. She concentrates her practice on compliance and regulatory issues affecting health care providers, payers, and employer-sponsored health plans. She has significant experience with HIPAA and the HITECH Act and assists covered entities and business associates in complying with these laws through the development of policies and procedures, workforce training, analysis and notification of breaches, and assisting with government audits and investigations. She also counsels her clients on regulatory issues, including state and federal fraud and abuse laws. Contact her via email at elizabeth.hodge@akerman.com.

SCOTT BENNETT is a Partner at Coppersmith Brockelman PLC in Phoenix, AZ. Scott advises hospitals and other health care providers regarding compliance with the Stark Law, Anti-Kickback Statute, and other fraud and abuse laws; represents providers in connection with internal investigations and litigation including cases under the False Claims Act; and counsels clients regarding information security and data breaches. He is a Certified Information Privacy Professional/United States (CIPP/US) through the International Association of Privacy Professionals. Contact him via email at sbennett@cblawyers.com.