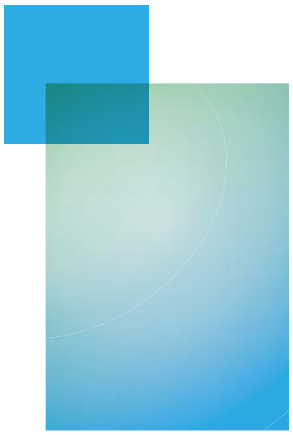
CYBER RISKS FROM MEDICAL DEVICES AND INSURANCE IMPLICATIONS

AXIS

Vulnerabilities threaten not only the risk of exposure to personal information stored in devices and networks, but pose serious risks to patient safety if the devices are disabled or otherwise altered.



Introduction

While cyber security is a hot topic in every area of business including insurance, medical devices[1] generally are not the first thing that come to mind when assessing immediate or long term cyber risks. Surely there have been a number of high profile lawsuits against hospitals and medical providers involving liability for unintentional access to/disclosure of PII and PHI from patient files and medical records. Yes, hospitals have been in the news for security breaches — everyone recalls that nefarious hackers held hospital hard drives hostage worldwide with the WannaCry and SamSam ransomware attacks within the last two years. But cyber risks from personal medical devices are just TV stuff, right? (Remember the 2012 season finale of *Homeland,* where the fictional United States Vice President was assassinated by terrorists who hacked his wireless pacemaker using the serial number and reprogrammed it?) Frighteningly, the answer in 2019 is likely no.

Personal medical devices (like pacemakers and implantable defibrillators), other wireless technologies (like insulin pumps), institutional/networked medical devices and other mobile health technologies (including infusion pumps, patient monitors, ventilators, imaging modalities and other life-sustaining or life-supporting devices), and even seemingly benign devices like hearing aids (which can now be controlled via smartphones), pose numerous, significant cyber risks from being hacked, to malware, to unauthorized access. The vulnerabilities threaten not only the traditional risk of exposure to personal information stored in these devices/networks, but pose serious risks to patient safety if the devices are disabled, infected with malware, rendered inaccessible or otherwise altered. These risks, in turn, raise a number of novel liability questions and potential coverage questions under numerous kinds of insurance policies, including GL, products liability, cyber and professional liability, and potentially D&O.

Table of Contents

I. The Risks

a. Personal Medical Devices

Between 2015 and 2018, the FDA issued six product safety communications (the cyber equivalent of voluntary product recalls) addressing cyber security vulnerabilities in personal medical devices.

Independent research discovered a security flaw in that would allow an unauthorized user to access and control the infusion system remotely through a hospital's network.

- On May 15, 2015, the FDA issued a safety communication warning that an independent researcher had found that the Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems (computerized infusion pumps designed for the continuous delivery of anesthetic or therapeutic drugs that can be programmed remotely through a healthcare facility's Ethernet or wireless network) contained a security vulnerability including software codes through which an unauthorized user could exploit the devices to interfere with the pump's functioning and, with malicious intent, remotely modify the dosage delivered to lead to under- or over-infusion of critical therapies. The FDA instructed healthcare facilities to reduce the risk of unauthorized access by implementing recommendations issued by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) of the U.S. Department of Homeland Security, risk mitigation strategies set forth in a letter issued by Hospira and by following "good cybersecurity hygiene practices" set forth in the FDA's "Cybersecurity for Medical Devices and Hospital Networks" Safety Communication dated June 2013.[2]
- On July 31, 2015, the FDA issued another Safety Communication warning that an independent researcher had discovered a security flaw in Hospira's Symbiq infusion system that would allow an unauthorized user to access and control the system remotely through a hospital's network. Unlike the prior LifeCare PCA communication, the FDA advised healthcare providers to discontinue use of the Symbiq devices because of the cyber vulnerability (the first time the FDA had ever done so). Although the FDA did not require that the devices be withdrawn from the market (it was still in use by, and being sold by, third parties), Hospira had already discontinued manufacture of the product for unrelated reasons. Hospira eventually devised a software update to close the access port to the pump along with other cybersecurity protections.[3]
- On January 9, 2017, the FDA issued a Safety Communication regarding the St. Jude Medical's Merlin@home Transmitter, which uses a monitor to wirelessly connect to a patient's implanted cardiac device, read data stored on the device, and transmit the data back to the patient's physician via the Merlin.net Patient Care Network, to reduce the number of in-office visits a patient needs. Specifically, the FDA warned that a vulnerability in the Merlin Transmitter would allow an unauthorized user (someone other than the patient's physician) to remotely access the cardiac device and modify the programming commands, which could lead to either rapid battery depletion or

administration of inappropriate pacing or shocks. St. Jude's devised a software patch to correct the vulnerability that would be automatically downloaded to each transmitter. Each patient was advised to leave their device plugged in and turned on to receive the patch automatically, and to continue routine in-office medical follow-ups.[4]

- On August 29, 2017, the FDA issued a safety communication regarding vulnerabilities in Abbott's (formerly St. Jude Medical) Accent, Anthem, Accent MRI, Accent ST, Assurity and Allure implantable cardiac resynchronization therapy pacemakers (CRT-P) devices, which are used to correct slow or irregular heart rhythms. These vulnerabilities would allow potential unauthorized Abbott created a firmware update to correct the problem, which affected more than 465,000 devices.[5]
- On April 17, 2018, the FDA issued a safety communication involving Abbott (formerly St. Jude Medical) Current, Promote, Fortify, Fortify Assura, Quadra Assura, Quadra Assura MP, Unify, Unify Assura, Unify Quadra, Promote Quadra and Ellipse implantable cardiac defibrillator (ICD) and cardiac resynchronization therapy defibrillator (CRT-D) devices for vulnerabilities that could lead to unauthorized access causing premature battery depletion and/or administration of inappropriate pacing/ shocks. The manufacturer issued Firmware updates to separately address the battery depletion issue and the cybersecurity vulnerability in the ICD and RT-D devices.[6]
- On October 11, 2018, the FDA issued a safety communication regarding vulnerabilities associated with the internet connection between the Medtronic CareLink 2090 and CareLink Encore 29901 Programmers, which are used to download software from the Medtronic Software Distribution Network (SDN) to Medtronic's implantable pacemakers and defibrillators during implantation and regular follow-up visits. Medtronic issued a software update (voluntary recall) to correct the problem.[7]

As recently as October 31, 2018, the FDA acknowledged that it is not aware of any patient injuries or deaths associated with these incidents, nor is it aware that any specific devices or systems in clinical use have been purposely targeted (to the contrary, the vulnerabilities that were the subject of these communications were discovered by "white hat" hackers working with the medical community). Nor are we aware at the time of publication of any individual lawsuits arising out of these incidents. However, the FDA expressly acknowledged the real risk that "these vulnerabilities could allow unauthorized users to remotely access, control and issue commands to compromised devices, potentially leading to severe patient harm." The FDA instructed that "healthcare facilities can reduce the risk of unauthorized access by implementing recommendations in the safety communications."[8]

b. Institutional Devices

While the risk of harm to an individual from a malicious hack into a personal medical device is chilling (indeed, the stuff of compelling TV drama), individual devices can be "repaired" relatively easily when a vulnerability is discovered, by firmware or software updates or patches as noted in the safety communications discussed above. An exponentially larger concern, from both a liability and exposure standpoint, arises from cybersecurity vulnerabilities in institutional medical devices. This includes network- and wifi-connected devices, as well as mobile devices, used by hospitals, clinics, doctors' offices, healthcare facilities (e.g., rehabilitation facilities, nursing homes, assisted living, etc.), healthcare systems, and home healthcare workers.

Brand-new devices arriving in hospitals today were designed using technology that may already be out of date.

The devices in any particular facility can include (but are not limited to) infusion pumps, dialysis machines, MRI and other imaging machines and modalities, patient monitors, ventilators, surgical equipment, and other devices which may include life-support and/or life-saving equipment, and all of which are connected to central nursing stations as well as the facility's main computer system and hard drives. Depending on the size of the facility, there may be dozens (in a small medical practice) to hundreds of thousands (in a large healthcare system) of medical devices in use at the same time. Each kind of device (and even different brands of the same or similar devices) likely requires its own complex software, and may have potentially divergent wireless capabilities, all of which operate adjunct to wired medical devices and software within an overarching ethernet system.

Compounding the problem is the fact that medical devices go through about five or six years of testing and clinical trials before receiving FDA approval, thus brand-new devices arriving in hospitals today were designed using technology that may already be out of date.[9] Additionally, healthcare institutions typically do not replace devices that are functional, and vendors do not manage the devices or software updates, so many of the devices in use now may be ten to twenty years old (before cybersecurity was a real concern)[10] and it may be unclear whether each device's software has been routinely updated or patched to address current connectivity issues/risks. The internet of things ("IoT") offers the ability to connect devices and program them to report information to a central location to isolate individual devices that may "go rogue," but the IoT is a hacker's paradise.[11] As a result, the nature and scope of the potential cyber risks is vast, and some risks are more obvious than others.

Clearly, healthcare providers/institutions are particularly vulnerable to the "usual" cyber risks such as manipulation, theft, destruction, unauthorized disclosure, or lack of patient data availability to providers, which can happen through network transfers (via email, remote access or file transfer), spyware or malware, or spear phishing attacks; theft or loss of external or portable networked medical devices; and denial of service attacks. Indeed, many hospitals in the U.S. and abroad were hit by the WannaCry and SamSam ransomware attacks in 2017 and 2018. In a simple data breach scenario where patient

information is compromised, statutes and case law dictate that the institution whose records were hacked will be liable to the patients whose PII/data was breached. (That is not the subject of this paper.)

The complexities of today's medical devices raise a number of unique potential risks, including but not limited to the following: electromagnetic interference; untested or defective software or firmware; misconfigured networks or poor security practices; failure to timely install manufacturer security software updates/patches to medical devices; installation of software updates to a medical device that cause disruption to/malfunction of another medical device(s); improper disposal of patient data or information including test results or health records from medical devices; uncontrolled distribution of passwords/disabled passwords/hard-coded passwords for software intended for privileged medical device access (e.g.. to administrative, technical and maintenance personnel); unauthorized device setting changes or reprogramming; targeted hacking of mobile health devices using wireless technology to access patient data, monitoring systems and implanted medical devices.[12] Who may be liable under these scenarios, and what insurance policy(ies) may respond (if any), in the event that a medical device (either personal or institutional) is compromised by a cyber risk, is a far more complex question.

II. FDA Guidance

On October 18, 2018, the FDA issued for public comment a new "draft" guidance regarding "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" ("New Guidance"), which is intended to provide recommendations to medical device manufacturers about the device design, labeling, and documentation that the FDA expects to see in premarket submissions. The stated purpose of the guidance is to address growing concerns about the potentially grave consequences of cybersecurity incidents involving networked or wifi-connected healthcare and medical devices.

The New Guidance covers Premarket Notification (510(k)) submissions (including Traditional, Special, and Abbreviated); De Novo requests; Premarket Approval Applications (PMAs); Product Development Protocols (PDPs) that contain software (including firmware) or programmable logic; as well as software that is a medical device. While manufacturers are required under Quality System Regulations to establish and maintain procedures for validating the device's design, including software validation and risk analysis, the New Guidance recommends that validation also include design controls to ensure medical device cybersecurity and device safety and effectiveness, which may make it easier for the FDA to "find your device meets its applicable statutory standard for premarket review."

The New Guidance is noteworthy in several respects:

- It creates a two-tiered classification of cybersecurity risk for medical devices. "Tier

1" devices (highest risk) are those internet connected devices (wireless or not) which, if compromised, could cause harm to multiple patients (e.g., pacemakers, insulin pumps, etc.). All Tier 1 premarket submissions would be required to include a design and risk assessment that addresses all of the new recommended cybersecurity design controls. "Tier 2" includes all non-Tier 1 devices, for which manufacturers would have the option to include a risk-based rationale for why certain recommended design controls are not appropriate.

- It adopts a framework similar to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, for designing "trustworthy" devices, including a list of design controls to accomplish these goals, such as ID, passwords, timed limited sessions with automatic logout, layered authorization, NIST standards of cryptography, a "deny by default" approach to connection, and the ability to update with software patches to address future vulnerabilities.
- It requires that manufacturers include a Cybersecurity Bill of Materials ("CBOM") to identify the commercial and/or off-the-shelf software and hardware components included in the device that could render the device vulnerable to hacking. The intent is to enable end users to take their own protective measures if any of those components are later discovered to have vulnerabilities.
- It expands the FDA's labeling requirements beyond directions for use, purposes and conditions of use (including hazards, warnings, precautions, and contraindications) to include relevant security information, and recommends fourteen new items to be included in medical device labeling, including: a CBOM, instructions for downloading version-identifiable software and firmware from the manufacturer, instructions for how to respond upon detection of a cybersecurity vulnerability or incident, and, if known, information about when the manufacturer is expected to stop providing security patches or software updates.[13]

On the same day, the FDA and U.S. Department of Homeland Security (DHS) also announced a new Memorandum of Agreement (MOA) to implement "greater coordination and cooperation between the two agencies for addressing cybersecurity in medical devices." MOA defines the roles between the FDA's Center for Devices and Radiological Health and DHS' Office of Cybersecurity and Communication to ensure that "such collaboration can lead to more timely and better responses to potential threats to patient safety." The DHS National Cybersecurity and Communications Integration Center (NCCIC) will continue to serve as the "central medical device vulnerability coordination center" while also communicating with the FDA to address systemic cybersecurity risks and vulnerabilities.[14]

On October 1, 2018, the FDA announced the issuance of a new *Medical Device Cybersecurity Regional Incident Preparedness and Response Playbook*, which outlines a framework for health delivery organizations and other stakeholders to plan for and respond to cybersecurity incidents involving medical devices, and protect patient safety.

The New Guidance, MOA and Playbook signal significantly increased regulatory scrutiny over medical device manufacturers going forward, during both pre-marketing product development/approval and post-marketing.

According to the FDA," [t]he healthcare sector knows how to prepare for and respond to natural disasters. It is less prepared, however, to handle cybersecurity incidents, particularly those involved in medical devices. Recent global cyber attacks highlighted the need for more robust cybersecurity preparedness to execute an enhanced, effective, real-time response that enables continuity of medical operations."[15]

The New Guidance, MOA and *Playbook* signal significantly increased regulatory scrutiny over medical device manufacturers going forward, during both pre-marketing product development/approval and post-marketing. This necessarily increases the focus on the reliability of the related software, not just the medical device itself. It also raises a question as to whether just the device manufacturers will face potential liability, or if the software designers and manufacturers (whose products must now be identified separately in the product labeling and warnings prior to the medical device receiving FDA approval) may face new or expanded liability as a result of a medical device cyber failure in the context of data breaches, and potentially in the context of cases involving injury or death resulting therefrom.

III. Regulatory Issues

Managing medical device cyber risks is critical both from a liability and underwriting perspective, especially in light of the current global regulatory environment. The European Union's General Data Protection Regulation ("GDPR"), which took effect in May 2018, imposes swift notification requirements in the event of a breach (within 72 hours), as well as substantial fines for violations, including up to 4% of a violator's annual revenue for the most serious breaches. Indeed, a medical device manufacturer's and/or healthcare provider's GDPR requirements can be triggered by a medical device cyber incident involving a single patient or client anywhere in the EU, once a breach is conclusively determined to have occurred.

Additionally, all fifty U.S. states have now enacted separate breach notification statutes, of which New York's 2018 regulations are among the most stringent. Thus, a breach involving a medical device that exposes more than one patient's data/information could potentially trigger notice requirements under multiple states' and countries' data protection laws (for example, a central nursing station at a major cancer hospital treating patients from all over the world is breached through a hack into a single patient's external heart monitor, for which the wifi connection software had not been updated in over two years).

It also bears noting that California recently enacted a strict privacy law that takes effect in January 2020, under which consumers will have the right to discover what personal information and data is being collected about them, who is collecting it, to whom such data is being sold, and to request that all such information/data is deleted. Consumers will have a private right of action under the statute, but the state Attorney General will also have enforcement rights. Violators would be subject to penalties of up to $7,500 per

violation. As with other California statutes like Prop 65 and ADA, it is foreseeable that this may open the door to extensive litigation against companies that are not vigilant about data protection, including medical device manufacturers and healthcare providers.

IV. Potential Liability Exposures

a. Product Liability

Strict liability for damages flowing from data breaches due to software defects/vulnerabilities is a new exposure for medical device manufacturers.

Products liability establishes the liability of manufacturers, processors, distributors, and sellers when a defect in their products causes personal harm or property damage to others, under theories of negligence, or strict liability for design defect, manufacturing defect or failure to warn.[16] While medical device manufacturers have been the subject of product liability litigation for decades in the context of bodily injury/death claims, strict liability for damages flowing from data breaches due to software defects/vulnerabilities would be a new exposure for medical device manufacturers that presents a number of highly complex questions of first impression.

The threshold question is whether such claims are viable. In our opinion, this is highly questionable. The economic loss theory generally bars recovery for loss of productivity, business disruption and other common damages caused by software defects. Thus, there must be some claim for property damage or bodily injury for such a claim to survive. If so, the question then becomes whether the medical device is defective simply because it was hacked.

Cases discussing liability for defective software to date have done so only in the context of financial services and have only speculated as to whether strict liability should be imposed. Those courts reached disparate conclusions.[17] In the products liability context, the seminal question would be whether the injuries/damages were caused by a defect in the product, which can be a design defect, a manufacturing defect or inadequate warnings, for which the manufacturers/distributors/sellers can be held strictly liable.[18] There are a number of stumbling blocks in applying these theories to products where the alleged defect is a software vulnerability.

1. Design Defect

   Determining whether a design defect exists requires application of a risk-utility test to assess whether the foreseeable risk of harm posed by the product could have been reduced or avoided by adopting a reasonable alternative design.[19] This is particularly challenging in the context of medical devices and other IoT connected products. For example, do all products have to incorporate the same level of security? (Does an implantable cardiac defibrillator require the same level of security as the national military defense system? Does a smart-phone controlled hearing aid?) When determining the "state of the art" for purposes of reasonable design

alternatives, technology changes so swiftly that a device (and the attendant software) may be reasonably secure at the time of manufacture, but not at the time a patient is using the product even if only a few months later. This is true of medical devices, where based on the FDA approval process, the product may not reach the market for five or six years after it was designed.

Malware and other hacking tools evolve daily. Thus, courts applying a reasonable alternative design theory would have to determine whether a plaintiff can show a reasonable alternative design that could have reduced or avoided a cyber-attack at the time the product was designed. An IoT device may not be vulnerable, even in retrospect, at the time that it was designed or even when it was sold. However, security analysts and hackers (both "white hats" and "black hats") regularly discover new vulnerabilities, requiring software vendors to update their products. Unlike other product manufacturers, this gives medical device and other IoT manufacturers and vendors an ongoing post-sale obligation to monitor/maintain the software to address defects that almost certainly did not exist and could not have been foreseen or warned of when the product was designed or manufactured.[20]

2. Manufacturing Defect

   An argument could be made that some software vulnerabilities are more like manufacturing defects that should be subject to a strict liability analysis. Toward this end, plaintiffs could argue that certain kinds of coding errors and oversights or bugs that are difficult to detect could be viewed as random errors in the software production line. In that regard, a court could potentially view them as comparable to flaws in a traditional manufacturing line that would cause an exploding soda bottle.[21] However, as discussed above, such vulnerabilities typically are not discovered until post-sale and are subject to software patches or updates that resolve the problems on an ongoing basis. The issue will be the nature and extent of the alleged damage caused by such a defect and whether there was any non-economic loss.

3. Failure to Warn

   Product manufacturers have traditionally had a duty to warn of risks that they know about or reasonably should have known about. The FDA's New Guidance includes a requirement that medical device manufacturers include software warnings in 501k applications, including a materials list that will disclose off-the-shelf and commercial software included with the product so end users can assess potential vulnerabilities. Failure to clearly disclose all software would raise a potential liability issue. As noted above, however, an IoT device and software may not be vulnerable when manufactured or sold and vulnerabilities that caused later damage may not even have existed at the time. Thus, under traditional products liability theories, there would be no duty to have warned about a risk that did not exist at the time.

   Unlike traditional product manufacturers, however, medical device and software manufacturers and vendors may have an ongoing duty to update their software to correct new vulnerabilities. Moreover, unlike traditional product manufacturers

who have little post-sale involvement with the product or the purchaser, IoT manufacturers and software vendors likely have all of the information and access needed to trigger a post-sale duty to warn about new defects that did not exist at the time of sale, even though such a duty has not previously been imposed on vendors. Additionally, patches or updates to software and firmware are the only solutions for such vulnerabilities. Thus, the potential exists for a court to impose a post-sale duty to warn on a software vendor to ensure that it continues to secure embedded software that is still in use.[22]

4. Other Issues

   Another complex question is who may be liable (in whole or in part) for design or manufacturing defects in software that accompanies medical devices. To the extent that the device manufacturer hires outside entities to develop, design and manufacture the software that enables device connectivity, and/or that design and manufacture component parts of the device that store or transmit data, perform connectivity functions, or incorporates off-the-shelf or other commercial software for those purposes, questions of fact will exist as to which entity(ies) will bear liability for each component that is deemed to be defective and caused the resulting damages. Allocation of liability may also be impacted by contractual indemnification issues. This aspect may also have a significant impact on the amount of insurance that may be available to respond to a claim or lawsuit.

b. Professional Liability

Vulnerabilities in medical devices also create a new form of liability exposure for medical providers. The healthcare industry, much like the financial industry and retail industry, is a prime target for liability flowing from a data breach. Patients that discover that their medical devices can be accessed and controlled by third parties are likely to seek recovery not just from the manufacturers of the device, but also the medical professional that selected, recommended and installed the device. Medical devices that contain vulnerabilities can also be used as an access point for nefarious third parties looking for a way to unlock the voluminous amount of personally identifiable information (PII) and protected health information (PHI) stored by medical providers. Such breaches can lead to class actions brought by large groups of affected patients. Doctors, nurses, hospitals and insurers need to be aware of the potential liability associated with implanting a device that can be hacked.

The potential liability facing professionals for medical device hacks has many layers. To be sure, there is no clear path to victory for such a claim as the issue has not been heavily litigated, and each incident is unique. Using recent examples of claims involving unsafe medical products along with regulations and guidelines governing how medical providers must protect their patients, we are able to identify a host of legal issues that will likely be front and center in a lawsuit against a healthcare provider following a medical device hack.

The initial hurdle that plaintiffs will have to clear in order to pursue professionals is establishing that actual harm has been suffered. The mere installation of a device that could theoretically be hacked may not be enough. The U.S. Supreme Court recently addressed what a plaintiff must show in order to establish it has standing to pursue a claim. In *Spokeo, Inc. v. Robins,* the Court recognized that a party must first establish that it is presenting the court with a case or controversy as required by Article III of the Constitution in order for the lawsuit to proceed.[23] The court explained that the mere fact that others have been injured as a result of a similar product or wrongdoing is not enough. Instead, a party must show that "he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"

Satisfying this threshold requirement will depend on the nature of the incident and the damage done by the third party actor. Hacks on implanted medical devices usually come in one of two forms. A passive attack occurs when a third party acquires access to data such as a patient's private information. An active attack occurs when a hacker is able to send commands to the device or prevent messages from being sent to the device. The latter form can have widespread impact if the messages intended for multiple patients contain inaccurate information, or the messages are prevented from being sent in the first place.

Whether the device creates the potential for a passive or active hack, a plaintiff exposed to a vulnerable device may be able to establish standing in order to plead a viable claim. Using the *Spokeo* standard, a plaintiff may allege that it has to incur the cost of implementing a fix to the vulnerability, or has to have the device replaced altogether. A plaintiff could also contend that its protected health information (PHI) has been accessed as a result of the vulnerability, causing it to incur costs to monitor its credit. Conversely, an isolated allegation that a party would not have purchased the equipment had they known of the vulnerability would likely not be enough to establish standing. Similarly, a contention that the device could potentially be hacked may not identify the concrete harm needed to establish standing.

Courts have analyzed the standing requirement in the context of analogous claims involving defective or counterfeit surgical mesh implanted into a plaintiff's body. In that scenario, where a plaintiff merely alleges that it would not have purchased the surgical mesh if it had known it was counterfeit and not what was represented, courts have held that the claim does not identify sufficient injury to confer standing on the plaintiff.[24] Conversely, allegations that the plaintiff must incur costs to replace defective mesh are enough to plead a viable claim. It stands to reason that a plaintiff complaining of a vulnerable medical device has to show more than a concern of future theoretical harm.

In the event a plaintiff is able to survive a challenge based on standing, establishing liability will require proof that the professional failed to meet the standard of care in

protecting its patient and its patient's information. In an age when security cannot be assured, providers may argue that they took adequate steps to protect their patients' information. The success of that defense would hinge on the medical provider showing that it followed all regulations governing how providers must protect patients and their PHI.

Just as the FDA has published guidance on what medical device manufacturers can do to ensure devices are secure, government agencies have also created guidelines setting standards for how medical providers protect patients and safeguard their confidential information. The Health Information Portability and Accountability Act of 1997 (HIPAA) imposes a duty on medical professionals to implement policies and procedures that protect their patients' information. The HIPAA Security Rule requires that providers implement procedures that ensure electronically stored information is secure from third parties. Covered entities and business associates must have a written security plan that contains administrative safeguards, physical safeguards and technical safeguards.

A failure to comply with these guidelines can lead to hefty fines imposed by the U.S. Department of Health and Human Services Office for Civil Rights (OCR). Through August 2018, OCR has settled or imposed a civil penalty in 55 cases, resulting in a total dollar amount over $78 million.[25] These regulations can similarly be used to as a blueprint for plaintiff's counsel to establish that the provider was negligent in failing to take steps needed to safeguard the health and security of its patients by utilizing flawed medical devices.

The threat of liability increases when a vulnerability is publicly known and yet a medical provider still utilizes that flawed device or technology. For example, researchers have criticized Medtronic, which manufactures pacemaker programmers and other relevant equipment, for apparent vulnerabilities that could allow a hacker to remotely access that equipment.[26] The alleged flaws associated with its Carelink 2090 pacemaker have been widely discussed. Similarly, in July 2015, the FDA issued a warning concerning the security risks associated with Hospira's Symbiq infusion pumps. The FDA has issued similar warnings for various products.[27] Once these vulnerabilities are publicly known, a plaintiff may contend that the hack of that equipment was predictable, and the medical provider was negligent, if not reckless, in continuing to use it on patients. A provider that uses devices and technology with known vulnerabilities could be seen as consciously putting its patients' health and security at risk, leading to increased exposure.

Similarly, a provider that fails to properly update its systems can be held responsible for an attack that could have been easily preventable. Replacing outdated systems with new, more secure systems is one way to stay ahead of hackers. Even with newer systems, regular updates and patches of security vulnerabilities need to be promptly implemented in order to close any known security gaps.

These updates come at a cost, sometimes requiring equipment to be taken offline for a substantial period of time to ensure the equipment is no longer vulnerable to third party access. Some providers have installed firewalls like Medmon, that "triggers response

Patient safety must take priority over cybersecurity requirements.

mechanisms that could warn the user or jam the malicious communication."[28] Ensuring that the devices are encrypted where possible also provides an extra layer of security that could prevent a hack. Medical providers need to appreciate that the time and cost associated with fortifying security systems are wise investments.

Because complete security cannot be assured, there are steps a medical provider can take to mitigate damages flowing from a device hack. Encrypting information is not only necessary, it also can prevent use of information accessed through the hack. A quick response to any intrusion is also critical so affected third parties are adequately notified and steps can be taken to ensure PHI and PII cannot be used for nefarious purposes. Those measures do not, however, insulate an entity from bodily injury claims. Although rare, a device hack that results in bodily injury could lead to significant damages.

Analyzing the nature and scope of liability facing medical providers concerning vulnerable medical devices is complex and multifaceted. Aside from displaying its due diligence by using state of the art devices and taking steps to minimize potential damages, medical providers facing a lawsuit resulting from a device hack would correctly assign blame on the third party hackers. Additionally, contracts between medical providers and device manufacturers also may allow the risk to be shifted to the party that designed and manufactured the flawed device. The liability landscape facing medical professionals relating to implanted medical devices will continue to evolve quickly. Medical providers and their insurers should closely monitor how courts treat such incidents in civil lawsuits so that correct steps can be taken to reduce risk and improve the way that patients' health and confidential information is protected.

V. Insurance Implications

The insurance implications raised by medical device cyber risks are equally complex and multifaceted. While federal privacy laws like HIPAA and HITECH require increased protection for patient data, these statutes do not regulate or promote effective cyber security by healthcare providers or facilities, or medical device manufacturers. Data breach legislation and mandatory reporting requirements enacted by all 50 states, along with the FDA's increased regulatory scrutiny in light of recent events, has clearly increased cybersecurity awareness in the healthcare environment.

Nonetheless, the nature of these products and the environment in which they are used mandates that patient safety must take priority over cybersecurity requirements. The challenge from a risk management perspective, and of paramount concern from an underwriting perspective, is how to close the gap — minimizing the compromise to ensure patient safety while still effectively managing/responding to the evolving

cybersecurity threat. Because the risk of a breach can never realistically be reduced to zero, the question then becomes how policyholders effectively mitigate risk and what factors will an insurer evaluate when placing coverage for that risk.

a. Risk Management

Medical devices are an integral component of medical networks so their security should be an integral component of cybersecurity protection. This mandates a high level of collaboration between the medical personnel and IT professionals, as well as collaboration by medical device manufacturers and network vendors, and potentially cybersecurity experts. "The cybersecurity vulnerabilities that are associated with medical devices are similar to any other networked system. What delineates the medical device environment from other networked environments is the potential detrimental impact on patient safety that exploitation of cybersecurity vulnerabilities may have. To shift the protection of medical devices to more mainstream cybersecurity protection will require the acceptance of medical devices as standard connections in the implementation of a network. This shift is essential, given the current lack of governance of networked medical devices, together with limited risk management, reliance on medical device regulatory approval, lack of awareness of the actual security risks, and lack of preparation by organizations to deal with the risks."[29]

In order to ensure that medical devices do not increase cyber exposure for healthcare providers, a set of internal best practices should be developed, especially for network-connected devices that are new, or continuously evolving. A provider should first understand which medical devices fall within its purview in order to be prepared to respond to any potential vulnerabilities in those devices. Only then will the provider be able to identify proper protocols to ensure that updates and patches are timely and properly implemented. The medical provider should also assess the location of its patient population in connection with each individual device — are its users domestic or international? Are the protocols in place to protect patient privacy uniform system-wide, or are there variations depending on the location of patients? Understanding the size and location of patients using devices will allow providers to be better prepared to respond to vulnerabilities.

From a risk management perspective, providers must also be vigilant when selecting vendors that manufacture, develop and service medical devices, as well as those companies that host related data and information. It is critical that the provider fully vet prospective vendors to ensure that they are retaining only competent and reputable companies that will take the steps necessary to safeguard the provider's systems and its patients. Along those same lines, contracts with vendors should be drafted to require the vendors to incur costs necessary to fix and update potential vulnerabilities. Contracts should also contain broad indemnification provisions in favor of the provider to ensure any costs or damages incurred by the provider or its patients can be shifted to the vendor. Medical providers should also take steps to ensure that the vendor maintains

adequate levels of insurance that would cover the provider in the event of a breach or loss. Finally, the provider should designate an internal representative to oversee vendor relationships and compliance to ensure that risk mitigation steps are being properly investigated and implemented.

b. Underwriting Implications

From an underwriting perspective, insurers are taking a very close look at policyholders' internal IT policies and procedures. Insurance carriers will want to evaluate the prospective insured's global "asset management," such as controls on how devices are networked, limitations on how each device can communicate within the network, and controls to swiftly identify and isolate devices that malfunction or are breached to minimize exposure to the rest of the network. An insured's ability to control ID/passwords and user access to devices that store/transmit patient data is also an important factor. As explained above, the insured's software update/patch management procedures will be considered in determining whether regular and timely updates are implemented to minimize hacking risk. A policyholder's proven compliance with regulatory standards (HIPAA, HITECH, GDPR and state privacy statutes) is also an important factor in considering risk.

The underwriter's job will also require an understanding of the interplay between various types of coverage purchased (and available to) the prospective insured. As explained further below, the there are many iterations of cyber policy forms being offered in the marketplace, resulting in significant variations in the scope of coverage offered to the policyholder depending on the insurer involved and the coverage purchased. Identifying whether a potential loss associated with medical devices can properly be assigned to medical malpractice coverage, cyber/tech E&O coverage, or some other type of coverage should be considered in identifying potential exposure to the policyholder and insurer.

Properly pricing risk in this arena also presents its challenges. An insured facing a breach could encounter a combination of claims involving government fines/penalties, civil lawsuits and injunctive relief, not to mention first party loss and expense incurred by that insured. In a legal environment that lacks uniformity when it comes to first party and third party damages flowing from a breach, it can be difficult to accurately price a policy that would cover a breach relating to medical devices. Still, underwriters will examine the type of information collected by the device and stored by the prospective insured to evaluate what exposure could flow from a breach. A company that stores sensitive medical information about a patient may face increased liability for third party claims as compared to a company that maintains records on patient cholesterol levels. It is also important for the underwriter to consider the number of records stored by the device and connected systems, and the number of individuals that could be impacted by a breach. Finally, factors that are typically considered in underwriting other lines of coverage (the policyholder's revenue, size, location, etc.) will be factored into the equation.

VI. Coverage Implications

While software vulnerabilities in medical devices present an emerging and previously unforeseen risk for data breaches/cybersecurity exposures (especially from a product liability perspective as discussed above), the insurance coverage issues are virtually identical to those raised by data breaches from non-medical devices that have occurred in hospital or other health care settings. Traditional insurance policies were not designed to address these emerging risks, thus gaps in coverage exist. Cyber and Technology E&O policies are needed to ensure that manufacturers and healthcare providers are equipped to address the foreseeable exposures.

In the event of physical harm (bodily injury or death) to patients caused by medical device compromise or failure as a result of a breach (e.g., a hacker accesses a device remotely and reprograms or changes settings), medical device manufacturers and sellers, and/or software, services or component part providers may have coverage under their CGL/products liability policies. Depending on what defect is alleged to have ultimately caused the harm, coverage issues may include who is an insured/additional insured under each such policy; priority of coverage; other insurance clauses; expected/intended exclusions; contractual liability exclusions; and business risk exclusions.

Absent actual bodily injury, CGL policies generally do not cover data breaches under Coverage A unless there is a claim for physical damage to or loss of use of tangible property, which has been held to mean actual damage to or loss of use of computer hardware. This is because the ISO CG 00 01 policy form has, since 2001, defined "property damage" to exclude damage to or loss of use of electronic data,[30] and in 2004, was amended to exclude all damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data.[31]

Courts are split and case law is still emerging as to whether data breaches are covered under Coverage B of a CGL policy.[32] A seminal issue in this regard is whether there was mere access to personal information or a subsequent publication or misuse of same.

These entities may also have coverage under cyber policies/programs where GL/products coverage is insufficient or unavailable, provided that the cyber policies are customized to address such risks. Technology E&O policies may also provide "contingent bodily injury" coverage for bodily injury caused by digital events otherwise insured under such policies.

The most foreseeable scenario is that medical device software vulnerabilities result in malware attacks causing business income losses to healthcare institutions or other providers. In that case, medical device manufacturers, and software, service and component part providers, may be covered for such financial losses under E&O policies, or cyber policies under certain circumstances (e.g., if the device is on the manufacturer's network). The healthcare provider's own financial losses from compromised medical

devices on its own network could potentially be covered under first party property policies, as well as cyber policies, which are likely to afford broader coverage.

Healthcare providers may also look to medical professional policies, but those will necessarily have some limitations in the context of cyber exposures. E&O policies may cover costs of third party claims resulting from professional services causally connected to data security incidents, provided that the claims or allegations involve "professional" misconduct, and the acts/omissions were undertaken within a "professional" capacity, as defined by policy; and it may include "damages arising from violation of 'privacy' laws." E&O policies generally do not, however, cover first party costs (unless added by endorsement), or costs not arising from "professional services." In the absence of any specific cyber exclusions, policyholders can argue for a broad interpretation of coverage. However, it is unclear whether any particular policy will ultimately be broad enough to cover medical device failures that resulted from faulty software codes, networks and computer technology (IT services as opposed to professionals services) absent some specific cyber liability or technology E&O coverage provisions, or separate policy(ies).

Another possible scenario is that medical devices are hacked allowing patient data to be stolen (like the Anthem breach, requiring notice under GDPR and multiple states' statutes/regulations, forensics, and other response costs), or medical devices are commandeered for Denial of Service/Distributed Denial of Service attacks (resulting in loss of use of third parties' computer systems). This would lead to potential liability for the healthcare institutions' financial loss as well as possible theft/disclosure of patient information. Here, medical device manufacturers, software and component part manufacturers may only have coverage under Technology E&O policies and true cyber policies. Healthcare providers may only have coverage under true cyber policies for harm to third parties resulting from security failures for medical devices for which they are responsible (e.g., a security failure caused by the hospital's failure to apply a software update or protect passwords/IDs as opposed to a defect in the device itself or the manufacturer's failure to provide the software update).

Another potential scenario is cyber extortion (ransomware attacks like WannaCry and SamSam, perpetrated through medical device vulnerabilities). Healthcare institutions lacking adequate advance backup or whose backup systems were also infiltrated, may face prolonged shutdowns to repair their systems. New "wiper viruses" may also require hardware replacement. Device manufacturers, software, service and component part providers facing potential liability for device failures may have coverage under E&O or cyber policies, but there may be gaps in coverage if the policies are not issued by the same insurer. Healthcare providers may have coverage under cyber policies or special crime policies for the costs of addressing the extortion threat only. Business interruption claims may be covered separately under first party property and cyber policies.

VII. Conclusion

Healthcare institutions must devise and implement protocols to guard against vulnerabilities created by devices.

Newly developed medical devices and advancements to existing products create the potential for improved patient care. Increased interconnectivity between those devices and healthcare networks allow medical providers to offer prompt treatment to patients. With those benefits, however, come additional potential cyber exposures to medical providers. Medical devices with security vulnerabilities can allow hackers full access to a medical provider's network, where it may store a high volume of confidential and sensitive patient information. Such devices can also create an increased risk of potential harm to patients. To ensure its network is secure, healthcare institutions must devise and implement protocols to guard against vulnerabilities created by those devices. From selecting the proper vendors, to promptly implementing updates and purchasing new equipment, to purchasing the proper form of insurance coverage, medical providers can take steps to minimize the potential losses flowing from a cyber incident involving medical devices.

While providers can reduce the likelihood that a breach occurs, medical devices and associated software are changing at such a quick pace that breach prevention is far from certain. In that vein, insurers that issue policies to healthcare providers should understand the regulatory and legal landscape relevant to a breach originating from a medical device. Novel theories of product liability and professional liability may be pursued by impacted patients. Government regulators could seek penalties for failing to preserve the security of the devices and healthcare networks. Providers face their own potential loss for reduced productivity and system restoration costs. Insurers must therefore undertake a detail-oriented underwriting process in order to evaluate risk presented by a potential policyholder that utilizes medical devices. Insurers should also look for ways to assist their insureds with risk mitigation tools and qualified experts to assist in responding to a breach. When policyholders, brokers, insurers and vendors work together, they can ensure that the insured's risk is mitigated, the proper coverage is purchased, and the right steps are taken to respond to a breach involving medical devices.

Bios

Cheryl P. Vollweiler, Esq.
Partner, New York
TRAUB LIEBERMAN

Cheryl counsels clients on insurance coverage issues relating to cyber risk, technology and data security, products liability, general liability, premises, property damage and first-party policies, and represents insurance companies in complex coverage disputes in U.S. litigation and international arbitration. Cheryl can be reached at cvollweiler@tlsslaw.com or at (914) 586-7039. To learn more, visit www.tlsslaw.com.

Brian C. Bassett, Esq.
Partner, Chicago
TRAUB LIEBERMAN

Brian concentrates his practice in the areas of insurance coverage and excess monitoring. He represents insurance companies in complex claim disputes involving the interpretation of standalone cyber policies and endorsements affording data breach coverage. Brian can be reached at bbassett@tlsslaw.com or at (312) 275-3015.

Scott Swift
Cyber Claims Manager

During his 17 years in the insurance industry, Scott has handled Cyber, Tech, Media, and Professional E&O claims. Prior to joining AXIS, Scott was in private practice with a national law firm litigating pharmaceutical and medical device lawsuits. Scott earned his law degree from the University of Kansas School of Law where he served as Editor-in-Chief of the *Journal of Law and Public Policy*. Scott can be reached at scott.swift@axiscapital.com or at (816) 292-7295.

References

[1] The U.S. Food and Drug Administration ("FDA") defines "medical device" in Section 201(h) of the Food, Drug & Cosmetic Act to mean "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part or accessory which is: recognized in the official National Formulary, or the United States Pharmacopoeia, or supplement to them; intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals; or intended to affect the structure of function of the body of man or other animals, and which does not achieve its primary intended purpose through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purpose." http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/ucm051512.htm

As defined above, a medical device is regulated by the FDA and is subject to pre- and post-marketing regulatory controls. IN 2011, the FDA issued the Medical Device Data System (MDDS) rule, which extended medical device regulation to include software, electronic or electrical hardware, including wireless, that makes claims to be useful for the medical purposes described in the MDDS classification (i.e., not generic software). The MDDS classification includes systems that act as mechanisms to transfer, store,

convert, or display medical device data without controlling or modifying the function parameters of a connected medical device http://www.fda.gov/medicaldewvices/productsandmedicalprocedures/generalhospitaldevicesandsupplies/medicaldevicedatasystems/ucm251897.htm

[2] https://wayback.archivet.org/7993/20170722144742/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

[3] https://www.reuters.com/article/us-hospira-fda-cybersecurity-USKCN0Q52GJ20150731

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

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

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

[7] https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm623184.htm

[8] https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

[9] https://www.bna.com/device-makers-combating-n73014482033/

[10] https://www.businessinsurance.com/article/20181009/NEWS06/912324484/Medical-devices-cyber-security-internet-of-things-cyber-risks

[11] Id.

[12] Russell L. Jones, CISSP, CIPP/G and Sheryl Coughlin, PhD, MHA, Networked medical device cybersecurity and patient safety: Perspectives of health care information cybersecurity executives" Deloitte Center for Health Solutions (2013)

[13] Shanna Pearce, *"FDA Issues New Draft Cybersecurity Guidance for Medical Devices*", Nov. 29, 2018, https://www.natlawreview.com/article/fda-issues-new-draft-cybersecurity-guidance-medical-devices

[14] https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm623574.htm?utm_campaign=10162018_PR_FDA%20and%20DHS%20announce%20partnership%20to%20address%20medical%20device%20cybersecurity%20threats&utm_medium=email&utm_source=Eloqua

[15] ttps://www.mitre.org/sites/default/files/publications/pr-18-1550-Medical-Device-Cybersecurity-Playbook.pdf

[16] Rusted M. and Koenig T. (2005), "*The tort of negligent enablement of cybercrime*", Berkeley Technology Law Journal, Volume 20 (4), 1553, available at: http://scholarship.law.berkeley.edu/btlj/vol20/iss4/4 (accessed 18 September 2017).

[17] See, e.g., Frances E. Zollers et al., *Landings for Software: Liability for Defects in An Industry That Has Come of Age,* 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 745 n.1, 756 n.57 (2005) (listing articles dating back to 1971 that have "speculated" about liability for various types of defective software); see also Michael D. Scott, *Tort Liability for Insecure Software*, 67 MD. L. REV. 425, 469 n.267 (2008) (summarizing calls to impose strict liability during the last twenty years); Michael Rustad, The Commercial Law of Internet Security, 10 HIGH TECH. L. J. 213, 258 n.220 (1995) (listing prior commentators who have recommended extending strict products liability to defective software dating back more than thirty years)

[18] *Restatement (Third) of Torts: Prod. Liability* §2 comment a.

[19] See, e.g., *Tincher v. Omega Flex, Inc.*, 104 A. 3d 328 (Pa. 2014).

[20] Butler A. (2017), "*Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?*", University of Michigan Journal of Law Reform, Vol 50 (4), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr

[21] See, e.g., *Escola v. Coca Cola Bottling Company of Fresno*, 150 P. 2d 436 (Cal. 1944) (holding bottling company liable for harm caused by exploding soda bottle)

[22] https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr

[23] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[24] See *Bowman v. RAM Med*., Inc., 2012 U.S. Dist. LEXIS 75218, 10-cv-4403 (D. N.J. May 31, 2012) (customers who had counterfeit surgical mesh implanted in their body could not establish standing where they only alleged that they would not have purchased the mesh if they knew it was counterfeit).

[25] https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html.

[26] Lily Hay Newman, *A New Pacemaker Hack Puts Malware Directly On The Device* (Aug. 9, 2018) https://www.wired.com/story/pacemaker-hack-malware-black-hat/

[27] https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm

[28] Ania Monaco, *Keeping Hackers Out of Implanted Medical Devices* (July 16, 2012), http://theinstitute.ieee.org/technology-topics/smart-technology/keeping-hackers-out-of-implanted-medical-devices.

[29] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[30] ISO CG 00 01 04 13 Section V. Definitions 17 "property damage" provides, in pertinent part, as follows: "For the purposes of this insurance, electronic data is not tangible property. As used in this definition, electronic data means information, facts or programs stored as or on, created or used on, or transmitted to or from computer software, including systems and applications software, hard or floppy disks, CDROMs, tapes, drives, cells, data processing devices or any other media which are used with electronically controlled equipment."

[31] See Exclusion P "Access or Disclosure of Confidential or Personal Information and Data-Related Liability," although it is noteworthy that in 2013, ISO issued two versions of Exclusion P "Access or Disclosure of Confidential or Personal Information and Data-Related Liability" have been available, one of which excludes any damages arising out of the loss of electronic data, regardless whether such damages cause BI or PD; the other of which carves out an exception for damages relating to BI caused by the loss of electronic data (ISO forms CG 21 06 04 14 and CG 21 07 05 14), thus the existence of coverage under Coverage A will be heavily dependent on the precise policy wording at issue in any particular case.

[32] See, e.g., *Travelers Indem. Co. v. Portal Healthcare Solutions*, LLC, 2016 LEXIS 6554 (4th Cir. 2016) and Zurich Am. Ins. Co. v. Sony Corp. of America, 2014 N.Y. misc. LEXIS 5141 (NY Sup. Ct. 2014)(both holding that Coverage B "publication" includes availability online and potential for third party to access without proof of access or misuse); but see *Total Recall Information Management Inc. v. Federal Ins. Co.*, 115 A.3d 458 (Conn. 2015), aff'd 83 A.3d 664 (Conn. App. Ct.)(holding that "publication" requires proof of third party access, as well as publication or misuse of the purloined data, thus no coverage existed under Coverage B for data breach).