Cybersecurity in a Complex Healthcare Ecosystem

David M. Snyder, MBA, PE, CISSP, CSM

November 2020

Cybersecurity risk management for supply chains with multiple vendors is complicated. Each vendor is clearly responsible for its own system, but who minds the overall end-to-end concerns? This article asserts that coordination across organizational boundaries is needed to assess and mitigate cybersecurity risks in remote patient monitoring systems.

In healthcare, consider the systems that comprise remote patient monitoring.

> "**Remote patient monitoring (RPM)** uses digital technologies to collect medical and other forms of health data from individuals in one location and electronically transmit that information securely to health care providers in a different location for assessment and recommendations."[1]

Examples of network-connected RPM devices include wearables (e.g., smart watches), glucose monitors, pacemaker monitors, blood pressure cuffs, pulse oximeters, continuous positive airway pressure (CPAP) machines, scales, and more. Such devices are part of the family of the Internet of Things (IoT).

In some cases, there is a hazy line between measurement and intervention. For example, the integration of a continuous glucose measurement with an insulin pump to provide what amounts to an "artificial pancreas" for monitoring blood glucose levels and delivering insulin for treatment of diabetes.

A 2019 survey of physicians showed "Two in three, or 68 percent, of physicians surveyed strongly intend to use remote patient monitoring technology…" However, the survey report also indicates "Health care professionals view data security as the main barrier to technology uptake."[2]

The majority of recent cybersecurity analysis for medical devices has focused on devices used within hospitals and clinics. Cybersecurity for RPM is different in a number of ways.

THE RPM ECOSYSTEM

RPM is a "system of systems" – a physical and digital chain consisting of devices connected to networks, connected to other networks. Typically, there are multiple stakeholders involved in the provision and operation of these systems These include device manufacturers that depend on a supply chain for software and hardware components, communications networks, data

[1] *Remote Patient Monitoring*, Center for Connected Health Policy, https://www.cchpca.org/about/about-telehealth/remote-patient-monitoring-rpm

[2] *CTA Survey Finds High Demand for Remote Patient Monitoring Devices*, 11 April 2019, https://www.cta.tech/Resources/Newsroom/Media-Releases/2019/April/CTA-Survey-Finds-High-Demand-for-Remote-Patient-Mo#/

integrators, and the clinicians who are the ultimate users of the data (Figure 1). Also, various interfaces with humans, including patients, caregivers, developers, network engineers, and system administrators.

Sometimes RPM equipment connects to an application on a smartphone or to a home network. Other times, the equipment is set up to communicate directly to a cellular carrier. Cloud platforms are increasingly used to collect RPM data and store and process it for consumption by clinicians.

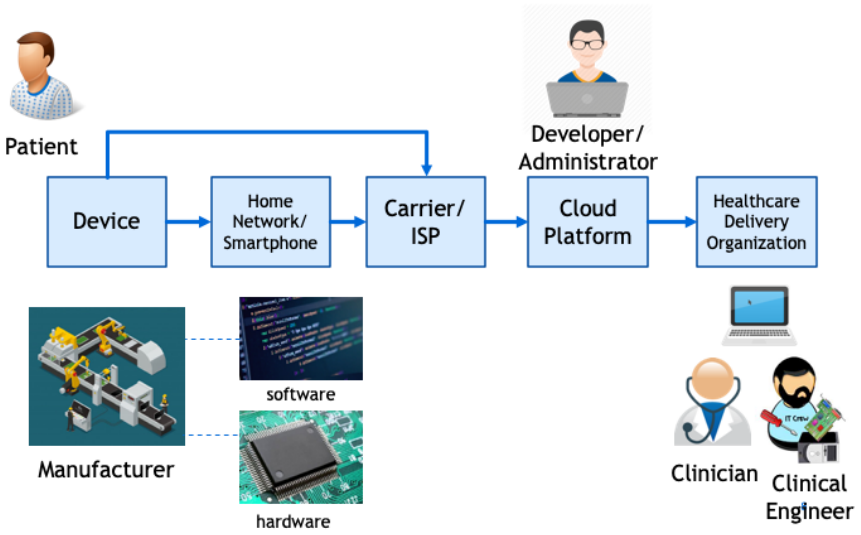

Figure 1

Each of the boxes in Figure 1 represents a component in the overall system that can be attacked to either disrupt the process or steal data. In some cases, an attack can "pivot" to a different system in the chain. An example of such an attack is the 2013 breach at Target Stores. Unauthorized access to Target's network was achieved via the network access that had been granted to Target's heating, ventilation, and air conditioning (HVAC) contractor.[3] Cybersecurity researchers have documented how endpoint devices, such as network-connected medical devices, can be used as an entrance to attack a network.[4] Conversely, unauthorized access to a network can allow an attack on an endpoint device (Figure 2).

[3] *Inside Target Corp., Days After 2013 Breach*, Krebs, Brian, 21 September 2015, https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

[4] *Identifying the attack surface for IoT network*, Rizvi, S, Orr, RJ, Cox, Austin, Ashokkumar, Prithvee, and Rizvi, Mohammad, 10 January 2020, https://www.sciencedirect.com/science/article/pii/S2542660520300056

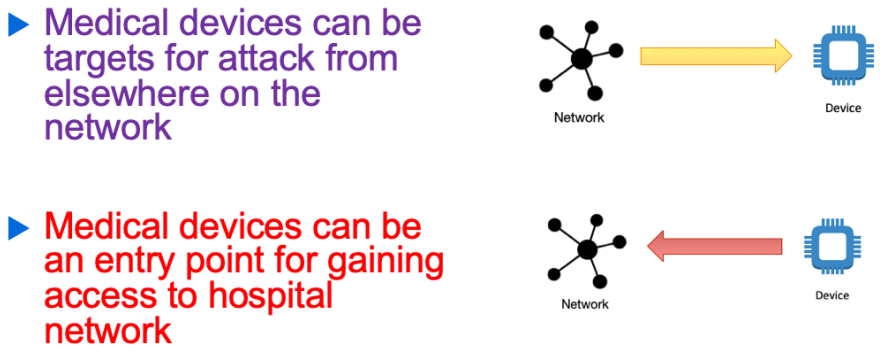

Figure 2

Attacks on healthcare delivery organization (HDO) networks via device or interim partner vulnerabilities are a bigger concern than attacks on individual devices. This is because more harm can be done if a healthcare delivery organization network is compromised. Attacks on these networks can not only result in theft of personally identifiable information, but also interruption of service, such as what occurs in a ransomware attack.

GUIDANCE

The US National Institute of Science and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) is working on a project to provide a reference architecture that will address the security and privacy risks for HDOs leveraging telehealth capabilities such as RPM.[5] The work product will be a Cybersecurity Practice Guide similar to the ones it has produced for Infusion Pumps and Picture Archiving and Communication Systems. NCCoE's project description shows a high level architecture that is similar to the model described above.

The "system of systems" described above is essentially a supply chain. In *Risk Management Framework for Information Systems and Organizations*, the NIST provides guidance on managing supply chain risk.

> "The growing dependence on products, systems, and services from external providers, along with the nature of the relationships with those providers, present an increasing amount of risk to an organization. Risk may increase based on the likelihood of occurrence and adverse impact from threat events such as the insertion of counterfeits, unauthorized production, tampering, theft, insertion of malicious software and hardware, as well as poor manufacturing and development practices in the supply chain, including the failure to build in security or privacy capabilities that enable an organization to better manage risk in its environment."[6]

[5] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

[6] *Risk Management Framework for Information Systems and Organizations*, NIST, December 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

In a RPM digital supply chain with multiple vendors involved, it is necessary to take a "trust, but verify" approach. Clauses can be put in a contract or a "Business Associate Agreement" to require a supplier/partner (vendor) to maintain a good cybersecurity posture, but it is unlikely that the vendor can absolutely guarantee protection. When only written assurances of "best efforts" to prevent cybersecurity incidents are provided, it behooves the buyer/user to perform due diligence and monitor whether these efforts are effective.

> "The typical 'flow down' of contractual requirements to downstream organizations in the supply chain is a necessary but insufficient part of third-party risk management. Simply assuming third parties like vendors are protecting one's information assets can be disastrous. Organizations should perform an appropriate level of due diligence before sharing information with third parties consistent with the risk they present based on the sensitivity and amount of information being shared as well as the purpose for which the information is shared."[7]

When there are several organizations involved, a holistic view of the system from end to end and a coordinated approach are needed.

This issue has been recognized by the US Food and Drug Administration.

> "Cybersecurity risk management is a *shared responsibility among stakeholders* [emphasis added] including the medical device manufacturer, the user, the Information Technology (IT) system integrator, Health IT developers, and an array of IT vendors that provide products that are not regulated by the FDA. *FDA seeks to encourage collaboration among stakeholders* [emphasis added] by clarifying, for those stakeholders it regulates, recommendations associated with mitigating cybersecurity threats to device functionality and device users."[8]

But how is this collaboration supposed to occur? Figure 3 describes the dilemma.

[7] *Solving the Third-Party Risk Management Problem*, HITRUST, https://hitrustalliance.net/uploads/Solving-the-Third-Party-Risk-Managment-Problem.pdf

[8] *Postmarket Management of Cybersecurity in Medical Devices,* FDA, December 2016, https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices

Whose Job Is It?

- This is a story about four people named **Everybody**, **Somebody**, **Anybody**, and **Nobody**.
- There was an important job to be done and **Everybody** was asked to do it.
- **Everybody** was sure **Somebody** would do it.
- **Anybody** could have done it, but **Nobody** did it.
- **Somebody** got angry about that, because it was **Everybody's** job.
- **Everybody** thought **Anybody** could do it but **Nobody** realized that **Everybody** wouldn't do it.
- It ended up that **Everybody** blamed **Somebody** when **Nobody** did what **Anybody** could have done.

Apparently an adaptation of "The Responsibility Poem" by Charles Osgood attributed to Charles R. Swindoll
https://www.goodreads.com/quotes/829722-this-is-a-story-about-four-people-named-everybody-somebody

Figure 3

One possible solution is for the healthcare delivery organization that is the receiver of the data to oversee the end-to-end process. Alternatively, the data platform vendor that consolidates, analyzes, and formats the data may be in a position to provide the needed coordination. On the other hand, it is difficult to imagine how device manufacturers could coordinate all of the stakeholders.

Whichever organization takes the lead, one of the first steps is to characterize all of the components and stakeholders in the system of systems. This includes categorizing the information processed, stored, and transmitted by the system. NIST provides a number of useful guidance documents on how to approach cybersecurity as a part of supply chain risk management (SCRM), including *Framework for Improving Critical Infrastructure Cybersecurity*.[9]

Consistent with the RPM model described earlier, NIST's *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks* points out that, "There is often heterogeneous ownership of IoT devices," and emphasizes the challenges inherent in maintaining cybersecurity for such equipment. [10]

> "…an IoT device may transfer data to manufacturer-provided cloud-based service processing and storage. Data may also be sent to a cloud service to aggregate data from multiple IoT devices in a single location. These cloud services may have access to portions or all of the devices' data, or even access to and control of the devices themselves for monitoring, maintenance, and troubleshooting purposes. In some cases, only manufacturers have the authority to do maintenance; an organization attempting to install patches or do other maintenance tasks on an IoT device may void the warranty. Also, in IoT there may be little or no information available about device ownership,

[9] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,* NIST, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
[10] *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks,* NIST, June 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf

> especially in black box IoT devices. This could exacerbate existing privacy redress difficulties because the lack of accountability limits individuals' abilities to locate the source of and correct or delete information about themselves, or to address other problems. Another concern with heterogeneous ownership is the effect on device reprovisioning—what data may still be available after transferring control of a device."[11]

In its risk assessment guidance, NIST recognizes the issues inherent in multi-organization systems.

> "The purpose of risk assessments is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or *threats directed through organizations against other organizations*; [emphasis added] (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur." [12]

The fact that end users have to depend on their suppliers doing a good job with respect to cybersecurity is not a new concept. A fair amount has been written about this.

> "Vendor risk management (VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance."[13]
>
> "A vendor risk assessment, sometimes called a third-party risk assessment, is a process that helps companies choose and monitor their business partners."[14]
>
> "From a compliance perspective, HIPAA regulations require that covered entities perform third party due diligence as it relates to ePHI, but the Security Rule does not specify exactly how to do it."[15]

VRM has most often been thought of in terms of third party risks. Recently, there has been discussion of "fourth party risk."

> "Just when you thought you had your arms around your vendor management program, auditors and examiners have been requesting information about your "vendor's vendors" as of recent years."
> "It's understandably confusing to figure out where to draw the line on your vendor's vendors, aka fourth parties. Are you responsible for "managing" all of your fourth party

---

[11] Ibid
[12] *Guide to Conducting Risk Assessments,* NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
[13] *Vendor Risk Management,* Gartner, https://www.gartner.com/en/information-technology/glossary/vendor-risk-management
[14] *How to Conduct a Vendor Risk Assessment in 9 Steps,* 17 July 2020, https://i-sight.com/resources/how-to-conduct-a-vendor-risk-assessment-in-9-steps/
[15] *Third Party Risk Management for Healthcare Cybersecurity*, CI Security https://ci.security/resources/news/article/third-party-risk-management-for-healthcare-cybersecurity

> vendors? What about your fourth party's vendors, referred to as fifth parties? That may be something we see more emphasis on in 2019. What's next?"[16]

As a final thought, remember that the ever-changing cybersecurity landscape means it may not be possible to anticipate and mitigate all threats. In the event an incident occurs, there needs to be a plan to respond and recover. In an environment with multiple vendors, response coordination has to be planned and rehearsed before something happens. The objective is to make sure the entire remote patient monitoring system is resilient.

> "Cyber resiliency (also referred to as cyber resilience) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources."[17]

If you work for a health care delivery organization that is on the receiving end of a remote patient monitoring system, what are you doing to make sure all of the components in that system are secure and that you are ready to respond to problems?

If you are one of the vendors in remote patient monitoring system, what are you doing to make sure your upstream and downstream partners in the system are secure?

If you are not sure how to do this, you'll probably want to obtain assistance to reach out to each of the organizations that comprise the end-to-end system and figure out an approach to make sure a holistic security framework is conceived and implemented.

* * *

David Snyder is a cybersecurity professional experienced at facilitating discussions among ecosystem members, analyzing complex processes, and orchestrating cross-functional and cross-organizational efforts.

Inquiries: https://42tek.com/contact/

[16] *Fourth Party Vendors: How Far Do You Need to Go?*, Venminder Experts, 21 May 2019, https://www.venminder.com/blog/bank-credit-union-4th-party-vendors-management

[17] Cyber Resiliency FAQ. MITRE, https://www.mitre.org/sites/default/files/PR_17-1434.pdf