Cybersecurity in a Complex Healthcare Ecosystem

David M. Snyder, MBA, PE, CISSP, CSM
42TEK, Inc.
updated June 20, 2021

Managing cybersecurity risk 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 real-time coordination across organizational boundaries is needed to assess and mitigate cybersecurity risks in remote patient monitoring systems and that there needs to be a framework to facilitate such coordination.

This year, the US National Institute of Science and Technology (NIST) published guidance that advocates just this sort of coordination.

> "Best practice organizations establish close relationships with their suppliers up to and including creating shared ecosystems between acquirers and suppliers to increase coordination and simplify the management of complex shared supply chains. Increasingly, organizations are treating their suppliers as members of their ecosystem and closely collaborating in a variety of ways..."[1]

This approach is especially suitable for 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."[2]

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 coordinate work to make sure a holistic security framework is conceived and implemented. (42TEK can help with this.)

Examples of network-connected RPM devices include wearables (e.g., smart watches), glucose monitors, electrocardiogram devices, blood pressure cuffs, pulse oximeters, pacemaker monitors, continuous positive airway pressure (CPAP) machines, scales, and more. Such devices are part of the family of the Internet of Things (IoT). COVID-19 and the growing need for post-acute and chronic disease management are driving increased demand for telehealth and RPM.

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.

---

[1] NISTIR 8276 Key Practices in Cyber Supply Chain Risk Management: *Observations from Industry,* February 2021, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

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

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."[3]

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 due to the transmission of data and commands outside hospital or clinic networks.

In healthcare, cybersecurity is most often discussed in terms of **privacy and financial losses**. A patient's health data and other personally identifiable information may be used for identity theft or to embarrass an individual. Penalties and remedial actions for cybersecurity incidents can be expensive. In a ransomware incident, besides the cost if a payment is made, there can be substantial financial losses due to the interruption of service.

Additionally, cybersecurity incidents can also directly affect **patient safety**. Harm can come from systems that are made to stop working or function incorrectly. Death or serious injury can directly result from malfunctions of pacemakers, pumps that administer medications, and other therapeutic devices. Monitoring devices that stop working, fail to communicate, or report incorrect data can result in inappropriate care decisions that can cause harm.

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 suppliers for software and hardware components, communications networks, data 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. Altogether, these form a **supply chain** to provide remote monitoring of patient biometric parameters.

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

[3] *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#/

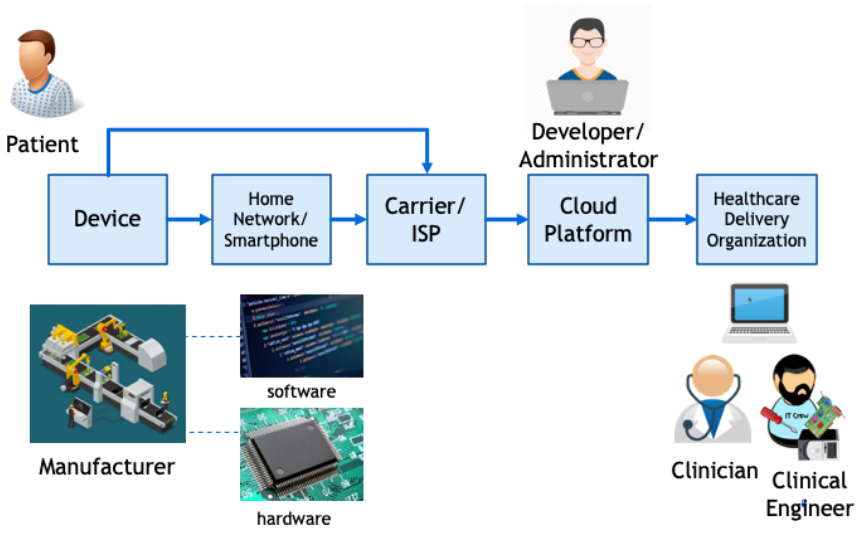

Figure 1

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.[4] Cybersecurity researchers have documented how endpoint devices, such as network-connected medical devices, can be used as an entrance to attack a network.[5] Conversely, unauthorized access to a network can allow an attack on an endpoint device (Figure 2).

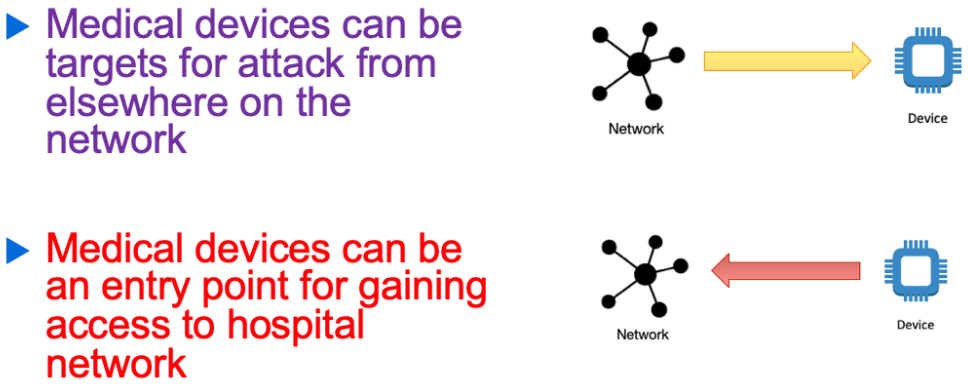

Figure 2

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

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

[5] *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

healthcare delivery organization network is compromised. Attacks on these networks can not only result in theft of personally identifiable information, but also corrupt data, or cause an interruption of service, such as what occurs in a ransomware attack.

The Open Web Application Security Project (OWASP) publishes a list of the Top 10 Web Application Security Risks and a similar list for IoT devices.[6] (Medical devices are a subset of IoT.) In its 2018 list of the Top 10 security issues associated with IoT devices, OWASP includes the following as #3:

> Insecure Ecosystem Interfaces:
> Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

A recent report on the "Top 10 Health Technology Hazards for 2021" lists cybersecurity challenges from vulnerabilities in third-party software components as number 7.[7]

The recently discovered SUNBURST attack on network management systems software produced by Solarwinds is an example of a sophisticated supply chain attack. Somehow, the attackers were able to insert powerful malware into patches that the software maker distributed to unsuspecting users. This malware allowed the attackers to gain access to the data systems of many corporate and government organizations. As of this writing, the investigations are ongoing, but it appears that thousands of organizations are affected, including at least one hospital.[8] This case definitely shows that supply chain attacks are not merely theoretical and that they do not only affect hardware. [9,10]

GUIDANCE

The 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. 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 second draft shows a high level architecture that is similar to the model described above.[11] This document includes a diagram that is similar to Figure 1 above. See Figure 3.

---

[6] *OWASP IoT Top 10 2018*, https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf
[7] ECRI, 2021, https://www.ecri.org/2021-top-10-health-technology-hazards-executive-brief
[8] SolarWinds hack also affected a hospital, major tech companies, Thwen, E., December 22, 2020, https://www.slashgear.com/solarwinds-hack-also-affected-a-hospital-major-tech-companies-22652129/
[9] *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor*, FireEye, 13 December 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attack...ges-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[10] *US officials scramble to deal with suspected Russian hack of government agencies*, Zachary Cohen, Vivian Salama and Brian Fung, CNN, 14 December 2020, https://www.cnn.com/2020/12/14/politics/us-agencies-hack-solar-wind-russia/index.html
[11] NIST Cybersecurity Practice Guide SP 1800-30, *Securing Telehealth Remote Patient Monitoring Ecosystem,* Second Draft, May 2021, https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth

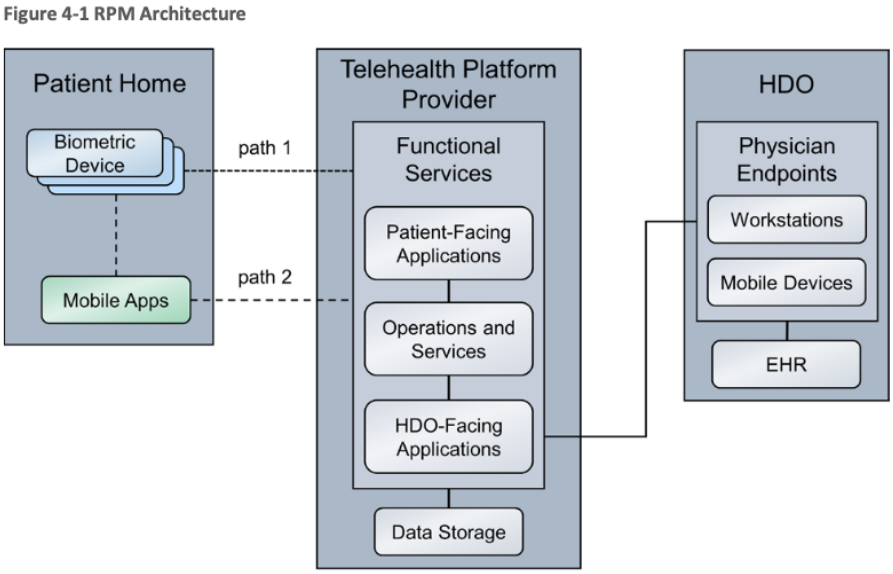

Figure 3

As explained earlier, the "system of systems" described above is essentially a **supply chain**. The NIST draft "Validating the Integrity of Servers and Client Devices: Supply Chain Assurance" provides a useful diagram showing the multiple stages in a supply chain where cybersecurity vulnerabilities may be exploited.[12] See Figure 4.

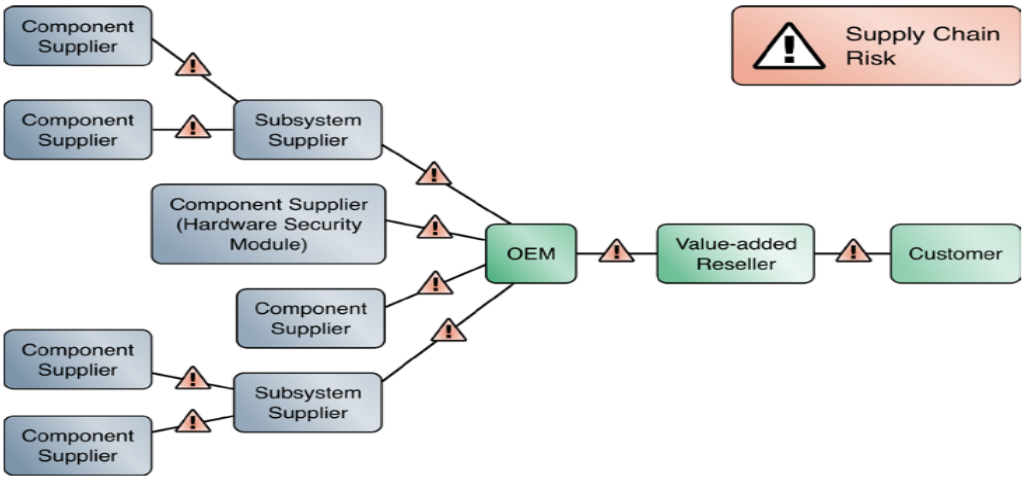

Figure 4

In *Risk Management Framework for Information Systems and Organizations*, NIST provides guidance on managing supply chain risk.

[12] Validating the Integrity of Computing Devices: Supply Chain Assurance, NIST NCCoE, March 2020, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/tpm-sca-project-description-final.pdf

> "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."[13]

Further advice for small- to medium-size organizations to implement the NIST guidance is provided in the new *Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) v.2.0* from the Healthcare and Public Health Sector Coordinating Council.[14] It includes a figure with an overview of the process (Figure 5).

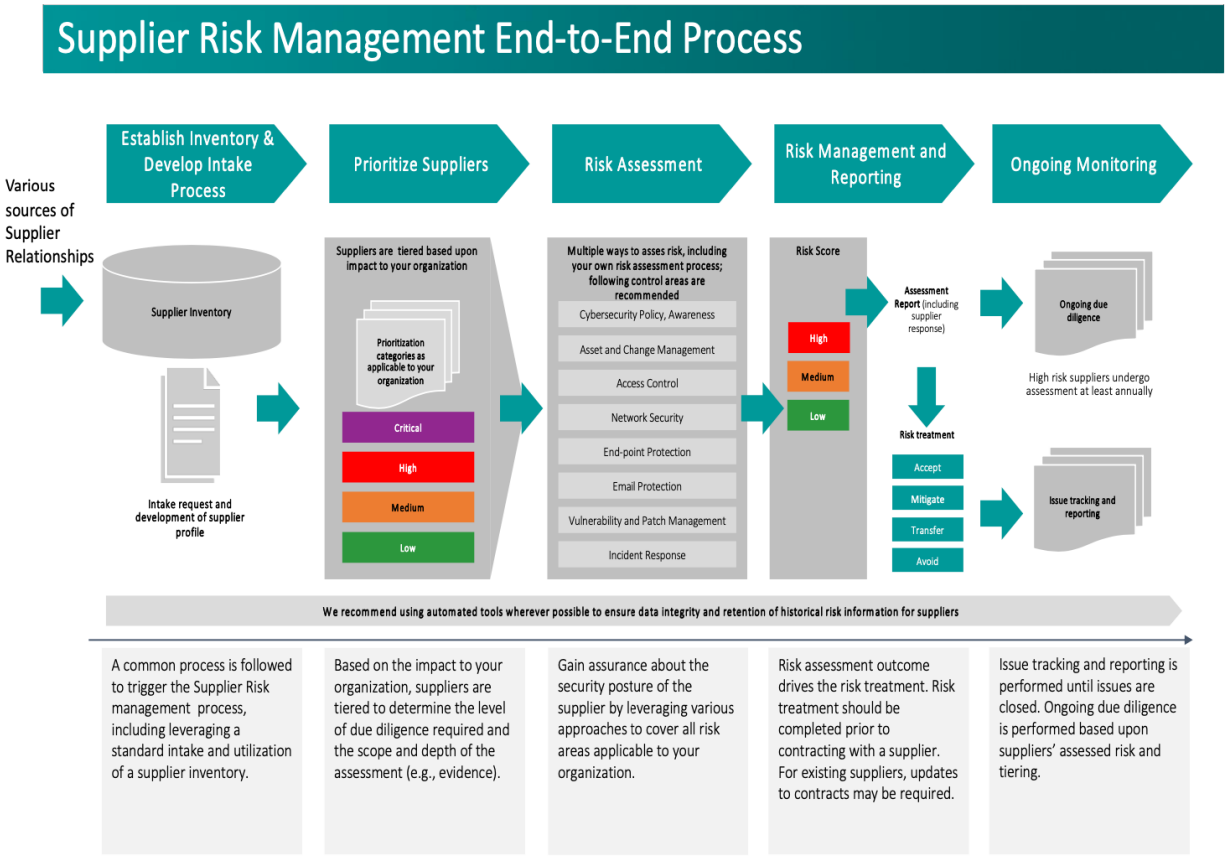

Figure 5

In a RPM digital supply chain with multiple vendors involved, a trust, but verify approach is needed. 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

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

[14] *Health Industry Cybersecurity Supply Chain Risk Management Guide (HIC-SCRiM) v.2.0,* September 2020, https://healthsectorcouncil.org/hic-scrim-v2/

protection. When written assurances of "best efforts" to prevent cybersecurity incidents are provided, the buyer/user also needs 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."[15]

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 (FDA).

> "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."[16]

But how is this collaboration supposed to occur? Figure 6 describes the dilemma.

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 6

The healthcare delivery organization that receives RPM data can oversee the end-to-end process, provided it has the needed resources to do the work. Alternatively, the data platform vendor that consolidates, analyzes, and formats the data may be in a position to provide the needed coordination. While device manufacturers definitely have a responsibility to make sure their devices are secure, it is difficult to imagine how they could coordinate all of the stakeholders.

---

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

[16] *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

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 each entity in 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*.[17]

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. [18]

> "…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, 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."[19]

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." [20]

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."[21]

---

[17] *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1,* NIST, 16 April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[18] *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

[19] Ibid

[20] *Guide to Conducting Risk Assessments,* NIST, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[21] *Vendor Risk Management,* Gartner, https://www.gartner.com/en/information-technology/glossary/vendor-risk-management

> "A vendor risk assessment, sometimes called a third-party risk assessment, is a process that helps companies choose and monitor their business partners."[22]
>
> "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."[23]

VRM has most often been thought of in terms of third-party risks. Recently, there has also 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 vendors? What about your fourth party's vendors, referred to as fifth parties?"[24]

An example of such fourth party risk occurs when a third party company provides a RPM solution to a healthcare delivery organization and the RPM solution includes a cloud platform hosted on AWS or Azure for aggregating, analyzing, and presenting data from the RPM devices. The end user may not even know that the solution provider is using AWS or Azure in the background.

In addition to periodic assessments of partners in the supply chain, NIST NCCoE guidance recommends ongoing monitoring should include issue tracking and reporting (see Figure 5 above). Typically, each partner in the RPM system will have an individual or team looking after cybersecurity concerns for its particular system. What is needed is a framework for real-time coordination across these organizational boundaries. See Figure 7.

[22] *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/
[23] *Third Party Risk Management for Healthcare Cybersecurity*, CI Security https://ci.security/resources/news/article/third-party-risk-management-for-healthcare-cybersecurity
[24] *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

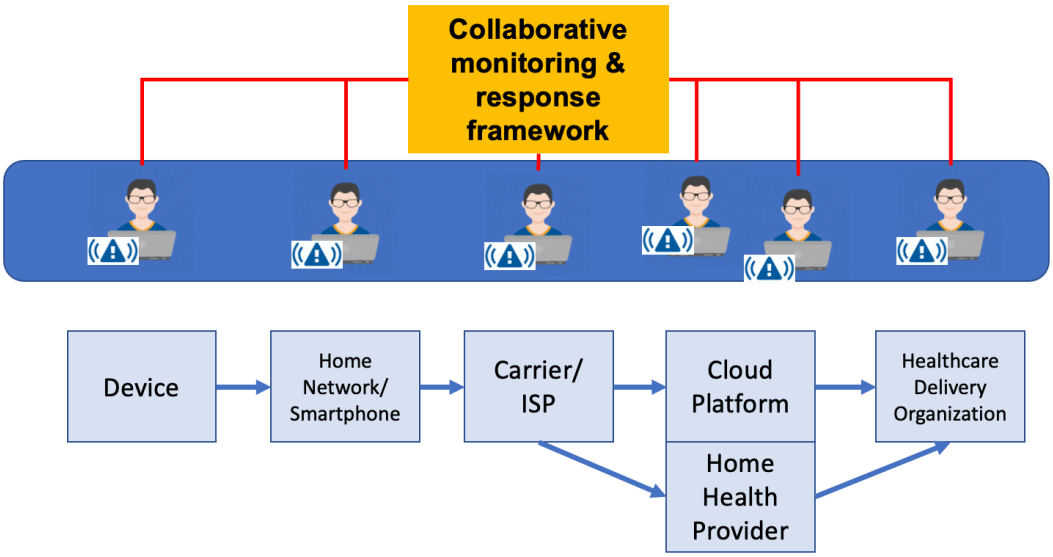

Figure 7

There is probably no one-size-fits-all solution for this. Each set of partners within an ecosystem will have to work together to define how they want to do it. In some cases, it may work well for one partner to provide the framework and facilitate coordination, or in other cases, it may make more sense for an outside service be engaged to set up and administer the framework. In most cases, coordination between the cloud platform and the HDO will be the highest priority.

As a final thought, remember that the ever-changing cybersecurity landscape means it is not 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 RPM 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."[25]

If your organization must face these issues, check whether you have the staff resources needed to work with your supply partners to assess and mitigate the risks. If not, consider enlisting help from a qualified consultant.

* * *

The author wishes to acknowledge helpful feedback on earlier drafts received from members of the Digital Medicine Society (https://www.dimesociety.org) and other members of the healthcare and cybersecurity communities.

David Snyder is a cybersecurity professional experienced at analyzing complex processes, facilitating discussions among ecosystem members, and orchestrating cross-functional and cross-organizational efforts.
Inquiries: https://42tek.com/contact/

Post Script:

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

The preceding analysis concentrates on the way multiple stakeholders need to work together to develop, implement, and maintain RPM systems securely. It is not a comprehensive survey of what it takes to build and keep these systems secure. A longer piece would address details regarding secure development practices, post-acute, long-term care, and home environments, tamper resistance, asset inventory and asset management, data flow diagrams, identity and access management, zero-trust architecture, end-to-end encryption, data provenance, logging and monitoring, threat modeling, risk assessment, vulnerability management, patching and updating, file integrity monitoring, intrusion detection, incident response, regulatory guidance and requirements, industry standards, penetration testing, change management, decommissioning, security awareness and training, and documentation of policies and procedures regarding all of the preceding items.