SMARTMETER
Engaging Health Data

The Importance of Health Data Security Workflows in Remote Patient Monitoring and Remote Therapeutic Monitoring

Written by:
William Bassett, CMO
March 2023

Table of Contents

Expanding Demand Drives Data Security Concerns

A fundamental tenet of every remote patient monitoring (RPM), remote therapeutic monitoring (RTM), Chronic Care Management (CCM), and health technology company is the protection of patient health information. Putting patient data in a position of being stolen, modified, or repurposed carries significant risk that companies need to assess, especially in their RPM device suppliers.

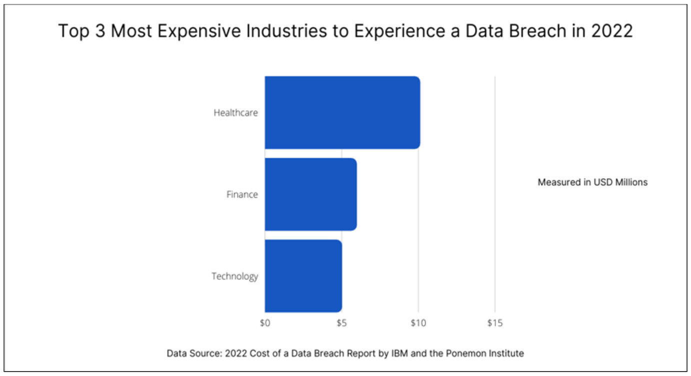
The collection and distribution of patient-generated health data, as done in RPM, requires that your device suppliers manage the patient data from the device to your platform in a highly secure manner to protect your customers and their patients. According to a Sophos report, more than 66% of healthcare services reported a ransomware attack in 2022.[1] With Malware attacks and IT-related incidents accounting for 67% of data breaches in the healthcare sector, choosing a vendor that has proven world-class technologies to protect your data is imperative.[2] If not, the financial cost of a HIPAA breach can be detrimental to the continuity of your business and the well-being of your customer's patients (see table below).

2022 HIPAA Penalty Structure[3]

Penalty Tier	Culpability	Min Penalty per Violation – Inflation Adjusted	Max Penalty per Violation – Inflation Adjusted	Maximum Penalty Per Year (cap) – Inflation Adjusted
Tier 1	Lack of Knowledge	$127	$60,973	$1,919,173
Tier 2	Reasonable Cause	$1,280	$60,973	$1,919,173
Tier 3	Willful Neglect	$12,794	$60,973	$1,919,173
Tier 4	Willful Neglect (not corrected within 30 days)	$60,973	$1,919,173	$1,919,173

The Imperative of Reliable Vendors

The rapid adoption of remote patient monitoring by healthcare professionals has captured the eye of patient monitoring device manufacturers from an assortment of overseas locations. Many foreign manufacturers may not be familiar with the rules and regulations your business must follow to maintain the safety and confidentiality of your customers' patients.



Top 3 Most Expensive Industries to Experience a Data Breach in 2022

Data Source: 2022 Cost of a Data Breach Report by IBM and the Ponemon Institute

Subsequently, these foreign manufacturers may not fully comprehend the importance and the severity of the consequences of using devices and data networks that may be vulnerable to malicious attacks. The healthcare data you manage is highly desirable, with 95% of all identity theft incidents coming from stolen healthcare records.[4] To make matters worse, protected health information (PHI) is worth about 50 times more than credit card information for those who steal it.[5]

Potential Vendor Vulnerabilities

A best practice for companies providing remote monitoring programs is to continuously monitor their vendors' approach to securing the patient-generated health data collected by the home monitoring devices. There are multiple areas in the data management workflows where a lack of security protocols might expose vulnerabilities allowing access to your data. Some of the typical workflow protocols to review include:

- A standard model for managing patient data is transporting it over the public Internet, which is susceptible to malicious attacks and can expose patient data to foreign governments outside United States borders. If your vendor uses this approach without the proper safeguards, you must consider better ways to secure patient data.
- Transport layer security is another essential aspect of providing secure communications over the Internet. It is critical to ensure communications' privacy, integrity, and authenticity. If your vendor is leveraging an "industry standard protocol," you must ask if they are doing enough to protect your patient's data.
- Monitoring devices leveraging the public Internet are at risk of allowing patient-generated health data to be sent anywhere in the world. The use of private networks constrains data flow and ensures it only arrives at its intended destination.
- Many overseas manufacturers are adding "over-the-air" software update capability to their devices as a new feature for remotely fixing errors or updating the device's firmware. Over-the-air updates performed on an unsecured public network add another vulnerability to your system, potentially allowing for tampering or capturing your data. Using a private network dramatically mitigates the risk of tampering or other malicious activity.

The Trusted and Secure U.S. Data Network for RPM

Smart Meter continues leading the RPM industry by delivering reliable technology and solutions propelling success for remote patient monitoring companies. Our collaboration with AT&T is significant for Smart*Partners* and the RPM industry as our world-class technologist created the only Private Data Network for RPM. Customers access an entire RPM data ecosystem with robust layers of security protecting patient-generated health data originating from our proprietary patient monitoring devices to your platform. Our proprietary monitoring devices can only connect and transmit patient-generated health data when connected to our Private Data Network for RPM. Our investment in data security technology ensures that your data is always protected from alteration, eavesdropping, data mining, or interception.

To learn more about the robust security and how the Private Data Network for RPM can protect your patient data, please visit www.smartmeterrpm.com. Or send an email to info@iglucose.com.

References

1. https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/
2. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/
3. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/
4. https://www.globenewswire.com/en/news-release/2022/03/31/2413675/0/en/Largest-Healthcare-Data-Breaches-Reported-in-February-2022-Confirms-Need-for-Network-Security-Based-on-Zero-Trust-Microsegmentation.html
5. https://www.dmagazine.com/healthcare-business/2019/10/why-medical-data-is-50-times-more-valuable-than-a-credit-card/