Call for Industry Change on the Perception of Protected Health Information

J.P. Larson

Medical device security is a topic of great interest for healthcare delivery organizations (HDOs). Considering that more than 400 breaches currently are under investigation by the Department of Health & Human Services,[1] the loss and theft of protected health information (PHI), including that stored on or transmitted by medical devices, is a very real concern.

In general, medical records are of high value to threat actors, who could use the information to, for example, get prescription drugs or file claims under another person's medical identity. Within an HDO, these records can be found and are stored on the medical devices of multiple manufacturers.

HDOs are taking steps to assess risks on medical devices that store, transmit, and display PHI. This article addresses a privacy risk found on medical devices. HDOs should be mindful of and concerned about patient safety and care delivery risks when conducting risk assessments; however, this is not the focus of the current work.

A security review of a medical device (i.e., Windows Embedded tablet with leads to capture various patient health measurements) raised concerns regarding the extent of PHI it contained. A sample set of five patient records stored on the device was analyzed. Table 1 shows a representation of the labels and format used for the dataset. (Actual data were removed for patient safety reasons.)

In documentation (i.e., the Manufacturer Disclosure Statement for Medical Device Security [MDS2] form) and interviews, the manufacturer of the medical device stated that the device does not contain PHI. In the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, PHI is defined as any information about health conditions, provision of healthcare, or payment for healthcare that can be linked to a specific individual (45 CFR § 160.103). Furthermore, for a record to not be considered PHI, all 18 identifiers listed under 45 CFR § 164.514 (e.g., name, geographic location, date of birth, social security number) must be removed. In other words, de-identifying PHI (and creating data that cannot be restricted under HIPAA and can be shared [e.g., for research purposes]) requires removal of these 18 identifiers.

Therefore, according to the current industry perception of PHI, the manufacturer would be correct because the combination of first name and date of birth (as shown in Table 1) is not sufficient to uniquely identify a patient. However, taking into consideration the visual record of a patient's first name and date of birth, along with the knowledge of the geographic state of the HDO, could a patient be uniquely identified with the assumption that he/she resides in close proximity to the HDO?

A quick search at a reverse lookup website, using only the date of birth and state for one patient, yielded fewer than 100 results, which included last names and addresses. After the first name was added to the filter, the number of results was fewer than 10. Knowledge of last name becomes trivial at this point, as

J.P. Larson, *CISSP, CISA, CIoTSP, Pentest+, is a medical device cybersecurity specialist at Christiana Care in Newark, DE. Email: jp.larson@christianacare.org.*

Key Takeaways

- During a security review of a medical device (i.e., Windows Embedded tablet with leads to capture various patient health measurements), concerns emerged over the extent of protected health information (PHI) it contained.
- With a patient's first name and date of birth (from the medical device), along with knowledge of the geographic state of the health delivery organization, the author was easily able to identify the exact patient using readily available tools (e.g., a reverse lookup website).
- Based on the two methods for de-identifying PHI (i.e., HIPAA Privacy Rule and Safe Harbor), it would appear that the medical device in question does not meet HIPAA requirements for de-identification of PHI.

Name	Patient ID	Date of Birth
Brian	Bk	12-Jun-1954
Ronald	Rs	25-May-1942
Marsha	Mt	06-Sept-1963
Joseph	Jw	21-Oct-1944
Ameen	Ac	17-Jun-1950

Table 1. Representation of five patient records stored on a medical device. Actual data were removed for patient safety reasons.

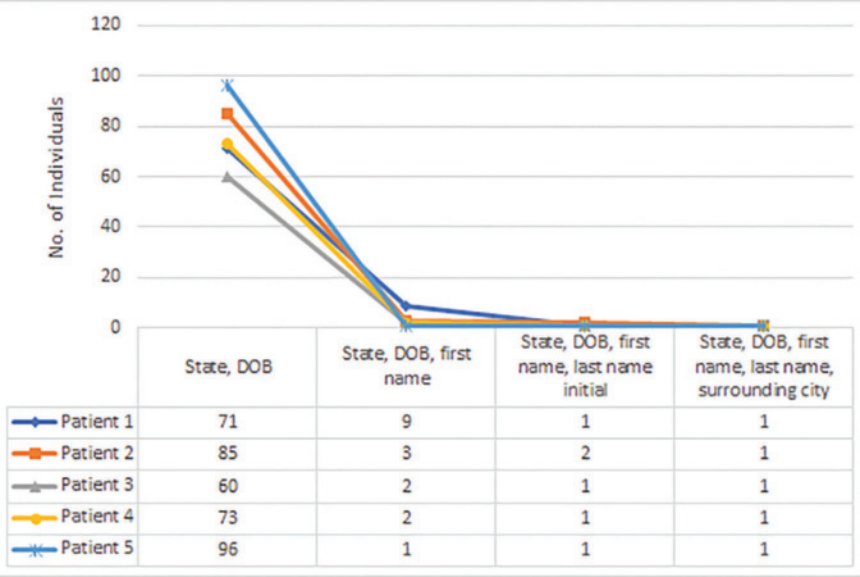

Figure 1. Analysis of how sample data shown in in Table 1 could be used to uniquely identify individual patients. Abbreviation used: DOB, date of birth.

social engineering tactics, social media sites, and reverse address and phone lookups can be used to find the exact patient.

Figure 1 displays the results of each additional identifier, assuming the values in the "Patient ID" column in Table 1 represent the initials of the patients' first and last names. The state in which the HDO was located also was taken into consideration, considering the likelihood that a patient would visit the HDO in closest geographic proximity. The results shown in Figure 1 illustrate that each patient in the sample dataset could be uniquely identified based on first name and date of birth, combined with knowledge of the geographic state of the HDO.

The HIPAA Privacy Rule outlines methods for sufficient de-identification of patient data (45 CFR § 164.514). The first method is expert determination. As demonstrated in this article, data for a medical device labeled as having no PHI were found to be insufficiently de-identified. An excerpt from 45 CFR § 164.514 is as follows:

"*Implementation specifications: Requirements for de-identification of protected health information.* A covered entity may determine that health information is not individually identifiable health information only if: (1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information."

The second method is Safe Harbor. Of note, HIPAA does not specifically mention full first and last names; it only mentions names. Geographic information can be implied by the HDO location and the assumption that patients, with high likelihood, reside within reasonably close proximity to their care provider. Finally, the presence of the full date of birth in the medical device would qualify as PHI. An excerpt of the identifiers in Safe Harbor Method (from 45 CFR § 164.514) is as follows:

"(2)(i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older."

Based on the two methods for de-identifying PHI, it would appear that the medical device in question does not meet HIPAA requirements for de-identification.

One key phrase is from the HIPAA Privacy Rule (i.e., "in combination with other reasonably available information") requires clarification. Although the patient record on the medical device contains only first name and date of birth, possessing knowledge of the HDO's geographic state and use of readily available Internet search tools allows data to be correlated and, as a result, PHI to be formed. Henceforth in this article, this will be referred to as "relatable PHI," as the additional information to create PHI can be found publicly.

This security review of a medical device calls into question how PHI is perceived by the healthcare industry. Although a patient record on a medical device might not contain a full name, identifiers can be leveraged to determine patient-identifying information, and as a result, the device should be classified as containing PHI.

Asset management platforms should include fields to document devices that store PHI, relatable PHI, and personally identifiable information. HDOs would be wise to identify manufacturers of medical devices as business associates, especially when PHI is stored, transmitted, or displayed. Although HDOs are the custodians of PHI, business associate agreements create a shared responsibility between the HDOs and manufacturers.

The tendency to become fixated on whether a specific medical device interacts with PHI can cause HDOs to forget the big picture, which is ensuring the safety of patients by protecting PHI. One needs to take the perspective of a threat actor and question whether the data observed could be profitable. If the answer is "yes," then the data must be secured.

Until a change occurs in the way that PHI is identified and de-identified, HDOs can implement controls, such as ensuring accurate records in asset management, monitoring the flow of data to untrusted end points, configuring data loss protection, encrypting data at rest and in motion, and securing devices when not in use.

One needs to take the perspective of a threat actor and question whether the data observed could be profitable. If the answer is "yes," then the data must be secured.

Resources for You

AAMI offers a variety of resources to help healthcare delivery organizations and medical device manufacturers develop effective cybersecurity practices and programs, including:

- *Medical Device Cybersecurity: A Guide for HTM Professionals*
- AAMI TIR57:2016, *Principles for medical device security—Risk Management*
- AAMI/ISO FDIS 14971:2019, *Medical devices—Application of risk management to medical devices*
- Set of 80001 TIRs, which address the application of risk management for IT networks incorporating medical devices
- Courses on the development of medical device software

Details on these and other resources can be found by visiting the AAMI Store (**https://my.aami.org/store**).

Reference

1. Department of Health & Human Services. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed Feb. 8, 2019.