Treating the Whole Patient: Making PHI Security Part of the Treatment Plan

Article · January 2023

CITATIONS
0

1 author:

Soren Stauss
University of Minnesota Twin Cities
2 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Treating the Whole Patient:
Making PHI Security Part of the Treatment Plan

Soren Stauss
University of Minnesota
staus027@umn.edu

***Abstract*—For the best patient outcomes, clinical medicine and clinical cybersecurity can and should go hand in hand. This paper considers the need for clinicians to view the protected health information (PHI) security of their patients as a critical part of the overall care of the patient. Further, this paper considers the consequences of the failure to include security as part of the treatment plan, including the increased likelihood that the patient will be less forthcoming about private and uncomfortable clinical issues. Finally, this paper considers the benefits of implementing a clinical cybersecurity course of study in medical school curricula.**

It has been nearly three years since I appeared at the White House to give testimony on privacy concerns in the proposed Final Rule of the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT*. During this time, our primary concern was that certain types of software vendors would not be required to be HIPAA compliant, therefore opening the door for varying degrees of breaches of PHI, the result of which would both directly and indirectly affect patient care. Since that time, we have become increasingly aware that some of the greatest security risks come from within the clinical setting, and providers are at the forefront of this issue.

Those of us in the fields of medicine and technology have a unique vantage point in which we see the perspective of patient care through the lens of security. Like a pediatrician who can reasonably predict type II diabetes in an adolescent patient who is overweight, has a poor diet and who has genetic risk factors, we are able to predict certain outcomes based on predictors. One such predictor is the clinician who ignores the part of patient care that involves the patient's PHI security. Many, if not most, providers don't even think about PHI security, and if they do they pass it off as something that is not part of their job; it's not part of clinical practice. Nothing could be further from the truth.

During a recent discussion with a provider employed by a regional health system in suburban Chicago, he explained that he had recently received an email on his examination room computer that might be suspicious. He decided that he didn't want to deal with it, so he simply deleted the email. Soon after, the clinician received an email from IT that it was a random security test, and that he did the correct thing by deleting the email, but also should report such suspicious pieces of electronic mail in the future. Instead of being satisfied that he followed the correct procedure (whether he was consciously aware of it or not), he was annoyed that his time had been wasted. His response was that he is a busy clinician, and this cybersecurity "nonsense" was a poor use of his time. What this provider failed to understand is that taking a few seconds to ensure the security of his clinical computer terminal and software is in the best interest of his patients and is a significant part of their well-being. Instead, he dismissed it as a non-essential annoyance. He is not alone.

Hospitals have successfully used email warning systems to reduce unauthorized access to PHI by staff members.1 This has proven beneficial for preventing PHI from falling into the hands of friends and family members of patients who review PHI for personal purposes. While these are effective steps to reduce unauthorized access to PHI by staff, there have been fewer steps taken to reduce malware capable of collecting PHI for malicious use. These steps need to be taken at the clinical level, and providers are often the first line of defense against such attacks against their patients. The current escalation of events surrounding the invasion of Ukraine has highlighted a significant risk for critical systems in healthcare.2 This indicates the urgent need for a heightened level of security awareness in the clinical setting.

The issue does not stop at malware. Data breaches involving PHI often occur due to lax communication precautions between clinical staff. One of the chief complaints we receive from patients when it comes to their data security is the fact that they can hear from an examination room staff discussing their case in detail from the hall—or even the nurse's station. When conversations involving details of patient care, and the patients themselves, take place in the open, it is vitally important for all involved that identifying information be kept at a minimum, and extra care needs to be taken with volume of speech. Not only is this a likely breach of PHI, but it is disrespectful to the patient. More importantly, it makes the hospital and provider vulnerable to civil liability.

Consider a 16-year-old patient within a strict household who was diagnosed with a sexually transmitted infection and is currently being treated. With health data that is not sufficiently protected, that patient's parent or guardian can get a hold of that data and use it to punish that individual. Perhaps with that experience, that individual will no longer feel confident in confiding with his healthcare provider and will leave future medical issues undisclosed and therefore untreated.

In addition to PHI included in electronic communication, we are moving in a direction where technology will continue to have an increased role in clinical diagnosis and treatment. Robotics will have an increased role in surgical intervention, and wearable technology will detect warning signs in asymptomatic patients and will collect an array of patient data. If we are going to be in a place where we can maximize the clinical benefits of these technologies, they need to be kept secure. In order to keep them as secure as possible, we must start now by creating a culture of security in medicine. That starts by incorporating clinical security into medical education and training.

Could the introduction of healthcare cybersecurity courses in medical school assist in protecting PHI? There is evidence in this direction. We have proposed the development of a clinical cybersecurity course to seven medical schools in the United States, Singapore, and Hong Kong. Several other medical schools have introduced courses in medical informatics into their curricula. Harvard Medical School, for example, offers a Clinical Informatics elective course.3 This is an excellent step to introducing future physicians to healthcare IT security, and the elective course will likely be taken by students with an interest in clinical informatics. We believe, however, that the security of PHI is important enough to overall patient care that it warrants a required course in clinical cybersecurity.

This is a significant undertaking. The practice of medicine, including medical training, is always changing; it is vital that security begins to be increasingly incorporated into medical education

and training. When a culture of security is included as part of the holistic approach to patient care, the likelihood of a positive patient outcome increases. Isn't this the goal? When it comes to their patients' PHI, providers should consider how they would want their most sensitive information treated. This is especially true in an environment where telehealth and other electronic clinical communication with patients is the norm. We should demand the same level of privacy and security for patients as for ourselves.

References

[1] Jiang JX, Culbertson N, Bai G. Effectiveness of Email Warning on Reducing Hospital Employees' Unauthorized Access to Protected Health Information: A Nonrandomized Controlled Trial. *JAMA Netw Open.* 2022;5(4):e227247. doi:10.1001/

[2] Grabenstein, Hanna. Our private health information may be the target of a cyberattack. Are U.S. hospitals ready? *PBS.* April 1, 2022.

[3] Harvard Medical School Course Catalog 2021-2022. https://medcatalog.harvard.edu/courselist.aspx?dep=210