DOI: 10.1111/1475-6773.13202

DEBATE-COMMENTARY

HSR Health Services Research

Cybersecurity implications for hospital quality

As health care continues to digitize information, concerns of data privacy and cybersecurity also grow. When breaches of patient data occur, the response of health care delivery organizations to intense regulatory and public scrutiny can vary widely, potentially introducing technologies that could adversely impact patients. In this issue, Choi et al[1] attempt to quantify the possibility that some responses delay the timeliness of critical patient diagnoses and treatments.

They compared health care organizations that reported significant protected health information breaches to those who had not, and found that on average there was a 2.7-minute increase in "door to EKG time" in hospitals undergoing their third year of breach remediation, and a 0.36 percentage increase in mortality at year two. While we appreciate the importance of examining untoward effects of addressing data breaches, we have questions about the causal pathway and therefore the validity of the findings. The authors' proposed hypothesis for these findings is delays in electronic health record (EHR) access, order entry, review, and data collection introduced by postbreach data remediation efforts. However, an analysis of these specific time intervals was not performed, and we are left to wonder if the results could alternatively be explained by unobserved confounders. As such, we believe that caution should be taken in concluding that security interventions, which may or may not have been implemented by breached hospitals, directly resulted in worse outcomes.

Some of the remediation efforts may include technical and process-based security controls commonly deployed in most health care delivery organizations. It is very likely many of the health care organizations in the control group implemented increased cybersecurity measures during the study period as part of a natural cybersecurity maturation process to reduce risks of future breaches or disruptive cyberattacks. Without the details of which controls health care organizations implemented and how they were applied, it is difficult to know that the security remediation efforts of hospitals with a data breach are different from those health care organizations in the comparison group would have been undertaking to fulfill requirements of the 2009 Health Information Technology for Economic and Clinical Health (HITECH) Act.[2]

Furthermore, most hospitals have implemented workflow optimizations to reduce "door to EKG" times that are unlikely to be affected significantly by security controls. Emergency departments have widely implemented standing orders for triage personnel to rapidly obtain EKGs without an additional physician or nurse approval for patients presenting with chest pain.[3] Additionally, most modern EKG machines are designed to operate without the need to log in with a password or even be connected to electronic health records (EHRs) to limit potential delays. Clinicians staffing emergency departments rely on those obtaining the EKGs in the context of a potentially acute cardiac event to bring paper EKG tracings for rapid interpretation. We would expect that these widely utilized practices and medical device designs would protect the timeliness of EKG collection from the breach remediation effects cited by the authors.

We fully agree with the authors that cyberattacks on critical hospital infrastructure are likely to pose a bigger threat to patient safety than security controls implemented after a breach of protected health information. Threats such as ransomware from sophisticated adversaries have increasingly plagued health care,[4] resulting in well-documented patient care disruptions.[5] To prevent the impact of these threats, health care organizations are deploying security interventions such as multifactor authentication, data loss prevention, strong encryption, and intrusion detection software, in addition to monitoring new cyberthreats that may require additional controls. Not implementing these technologic controls leaves health care organizations extremely vulnerable to devastating patient safety consequences under the hands of malicious hackers and misguided malware. For example, if ransomware infected computer tomography (CT) scanners of a regional stroke center rendering them unusable, it would likely delay diagnosis of ischemic or hemorrhagic strokes. The treatment of each is very different and time-sensitive. This delay in diagnosis could impact patient care and safety.

A balance must be struck between cybersecurity and usability of systems that support patient care. This is particularly important in time-sensitive medical conditions dependent on rapid diagnosis or treatment such as severe sepsis, trauma, stroke, and MI. Overly restrictive cybersecurity efforts lacking clinical workflow insights risk introducing novel patient harms as well as user backlash and mistrust of necessary future cybersecurity controls as new threats emerge and evolve. Furthermore, the unique multiuser and multidisciplinary workflow requirements of health care complicate simple "off the shelf" applications of security products deployed in other industries. Software engineers and security professionals must design and build security solutions informed by clinical workflow to minimize the risk for patients' safety. Collaboration between physicians and health information experts may help to achieve this goal.[6,7]

Choi and colleagues highlight the importance of understanding the workflow impact of cybersecurity controls in the health care environment in order to prevent potential patient harm. Further research into the risks of cyberattacks on electronic

medical systems is an increasingly important endeavor that will serve as the foundation for safer and more secure future system development.

ACKNOWLEDGMENTS

Joint Acknowledgment/Disclosure Statement: There were no other contributors to this manuscript other than listed below. The authors are employed by both UCLA and UCSD which encourage and support academic publications from faculty.

Disclosures: The authors have nothing to disclose.

Disclaimers: The authors have no disclaimers.

Christian Dameff MD[1]
Michael A. Pfeffer MD[2]
Christopher A. Longhurst MD[3,4]

[1]*Department of Emergency Medicine, University of California San Diego, San Diego, California*
[2]*Department of Medicine, David Geffen School of Medicine at UCLA, Los Angeles, California*
[3]*Department of Medicine, University of California San Diego, San Diego, California*
[4]*Department of Pediatrics, University of California San Diego, San Diego, California*

Correspondence
Christian Dameff, MD, Department of Emergency Medicine, University of California San Diego, 200 W Arbor Dr. San Diego, CA 92103.
Email: cdameff@ucsd.edu

ORCID

Christian Dameff https://orcid.org/0000-0001-9613-2603
Michael A. Pfeffer https://orcid.org/0000-0002-8958-0843
Christopher A. Longhurst https://orcid.org/0000-0003-4908-6856

REFERENCES

1. Choi SJ, Johnson ME, Lehmann CU. Data breach remediation efforts and their implications for hospital quality. *Health Serv Res*. 2019;54(5):971-980. https://doi.org/10.1111/1475-6773.13203.
2. Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. *JAMA*. 2018;320(3):231-232.
3. Retezar R, Bessman E, Ding R, Zeger SL, McCarthy ML. The effect of triage diagnostic standing orders on emergency department treatment time. *Ann Emerg Med*. 2011;57(2):89-99.e2.
4. Gordon WJ, Fairhall A, Landman A. Threats to information security – public health implications. *N Engl J Med*. 2017;377(8):707-709.
5. Nigrin DJ. When "hacktivists" target your hospital. *N Engl J Med*. 2014;371(5):393-395.
6. Longhurst CA, Pageler NM, Palma JP, et al. Early experiences of accredited clinical informatics fellowships. *J Am Med Inform Assoc*. 2016;23(4):829-834.
7. Singer JS, Cheng EM, Baldwin K, Pfeffer MA. The UCLA Health Resident Informaticist Program – a Novel Clinical Informatics Training Program. *J Am Med Inform Assoc*. 2017;24(4):832-840.

SUPPORTING INFORMATION

Additional supporting information may be found online in the Supporting Information section at the end of the article.