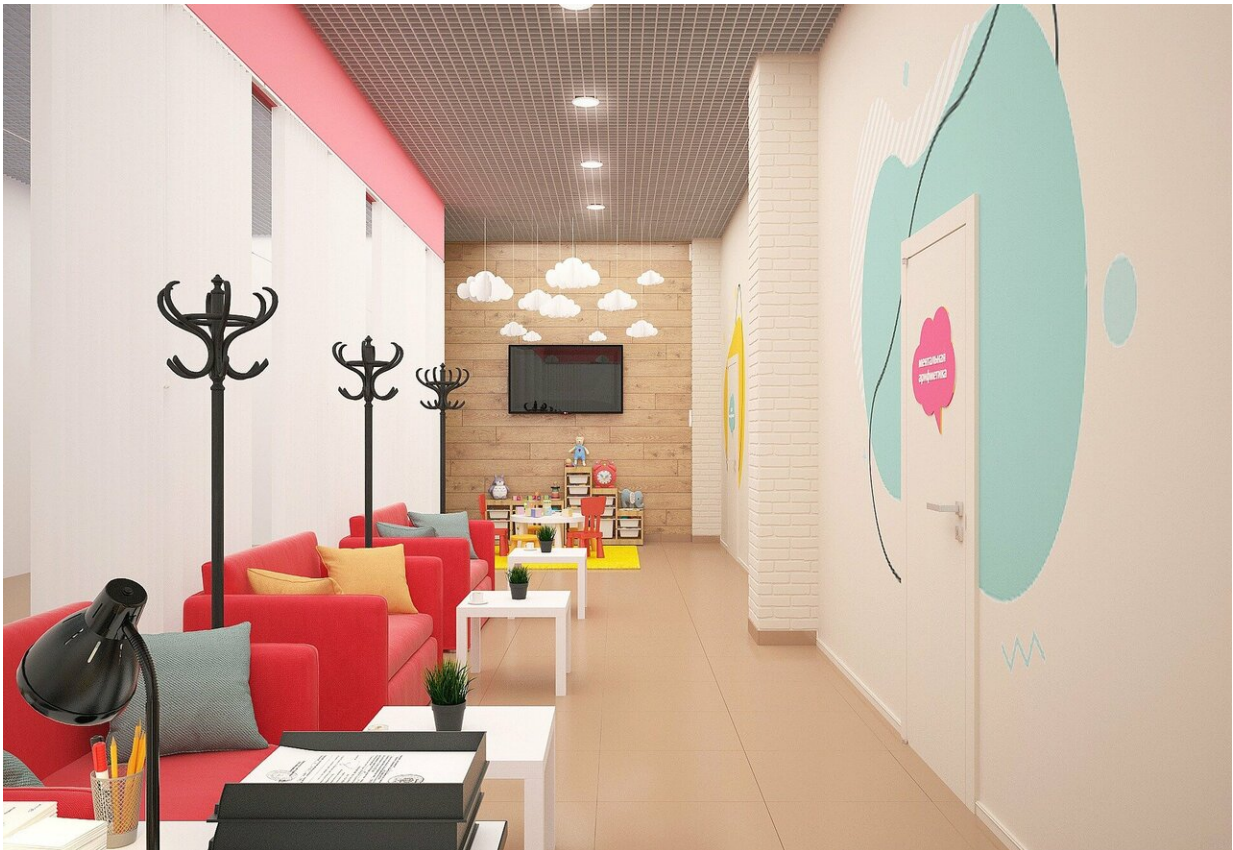


Data breach fixes could impact patient care: study

October 8 2019, by Liz Entman



Credit: CC0 Public Domain

IT security measures implemented following data breaches at hospitals may cost valuable time in delivering life-saving care, according to new research by Eric Johnson, Ralph Owen Dean and Bruce D. Henderson

Professor of Strategy at Vanderbilt's Owen Graduate School of Management, and Christoph Lehmann, professor of pediatrics and biomedical informatics at Vanderbilt University Medical Center.

The paper, "Data breach remediation efforts and their implications for [hospital quality](#)," appears in the October issue of *Health Services Research*. Sung Choi, assistant professor of health management and informatics at the University of Central Florida, is the lead author.

"In the security economics world, there's a lot of discussion about who bears the cost of [data breaches](#)—individuals or firms," Johnson said.

"We often see bad outcomes for consumers when their credit card information is stolen, for example, but we don't necessarily see firms bearing the full cost of losing that data. What we wanted to see here was whether there were any implications for patients when their data is stolen."

Hospitals are required by law to report data breaches to federal authorities, who then may open an investigation and oversee corrective action. This could mean enhanced authentication processes, longer passwords, quicker logout times for idle computers, and so forth. Johnson and his colleagues wondered if these new processes and additional security steps could be delaying care at crucial moments by impeding quick access to computerized systems.

Minutes and seconds matter for a [hospital](#): When a patient arrives at an [emergency room](#) with chest pain, he or she needs to be seen immediately. Medical guidelines state that the patient should receive an EKG as soon as possible—within 10 minutes at most—and HHS tracks this quality metric for all Medicare-authorized hospitals. It also tracks the 30-day mortality rate for heart attacks.

Using the HHS breach data and quality data on more than 3,000

hospitals from 2012-2016, Johnson and his coauthors were able to see if there was change in care quality in the years following a breach.

"We found that following a breach, time-to-EKG and [mortality rates](#) both rose, and continued to rise for about three years before tapering off," Johnson said, noting that the average time-to-EKG increased by as much as 2.7 minutes, and an increase in the 30-day mortality rate for heart attacks that translated to as many as 36 additional deaths per 10,000 heart attacks per year.

He explained that data breaches are often not discovered right away and that there is usually another lag while the breach is investigated and security updates are recommended and implemented. "So this long timeframe tells us that in breached hospitals, it's the remediation efforts—not the breach itself, but the post-breach remediation efforts—that are impacting these time-sensitive processes and patient outcome measures."

Johnson cautioned that they were not able to determine exactly what was causing the change after the [breach](#) or which security measures in particular may be associated with the delay, but he said these findings suggest that [federal authorities](#) and hospitals need to carefully consider usability when recommending and implementing changes.

"Security solutions designed to prevent future breaches may require usability assessment or include some sort of 'break glass in case of emergency' functionalities to ensure providers can quickly get the information they need when they need it most," he said.

More information: Sung J. Choi et al. Data breach remediation efforts and their implications for hospital quality, *Health Services Research* (2019). [DOI: 10.1111/1475-6773.13203](https://doi.org/10.1111/1475-6773.13203)

Provided by Vanderbilt University

Citation: Data breach fixes could impact patient care: study (2019, October 8) retrieved 3 May 2024 from <https://medicalxpress.com/news/2019-10-breach-impact-patient.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.