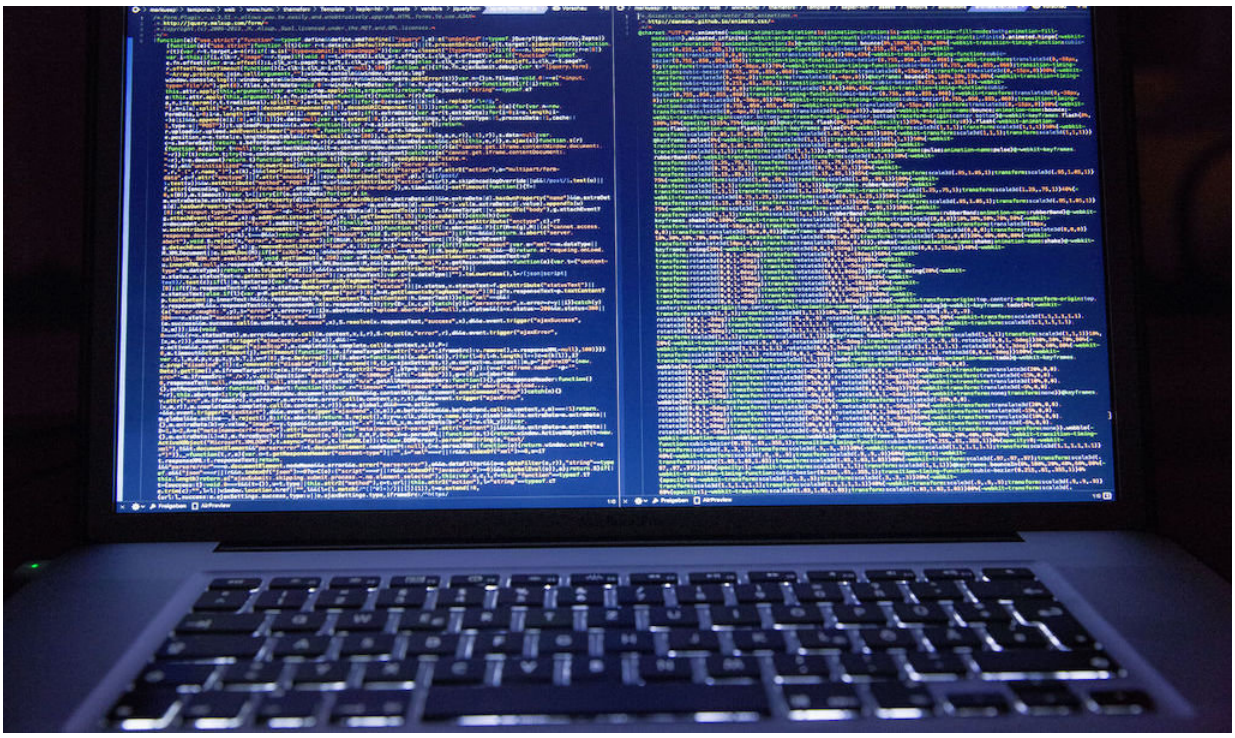
Healthcare providers—not hackers—leak more of your data

November 19 2018



More than half of personal health information leaks happened because of internal issues with medical providers. Credit: PxHere - CC0

Your personal identity may fall at the mercy of sophisticated hackers on many websites, but when it comes to health data breaches, hospitals, doctors offices and even insurance companies are oftentimes the culprits.

New research from Michigan State University and Johns Hopkins University found that more than half of the recent personal health information, or PHI, data breaches were because of internal issues with medical providers—not because of hackers or external parties.

"There's no perfect way to store information, but more than half of the cases we reviewed were not triggered by external factors—but rather by internal negligence," said John (Xuefeng) Jiang, lead author and associate professor of accounting and information systems at MSU's Eli Broad College of Business.

The research, published in *JAMA Internal Medicine*, follows the joint 2017 study that showed the magnitude of hospital data breaches in the United States. The research revealed nearly 1,800 occurrences of large data breaches in patient information over a seven years, with 33 hospitals experiencing more than one substantial breach.

For this paper, Jiang and co-author Ge Bai, associate professor at the John's Hopkins Carey Business School, dove deeper to identify triggers of the PHI data breaches. They reviewed nearly 1,150 cases between October 2009 and December 2017 that affected more than 164 million patients.

"Every time a hospital has some sort of a data breach, they need to report it to the Department of Health and Human Services and classify what they believe is the cause," Jiang, the Plante Moran Faculty Fellow, said. "These causes fell into six categories: theft, unauthorized access, hacking or an IT incident, loss, improper disposal or 'other.'"

After reviewing detailed reports, assessing notes and reclassifying cases with specific benchmarks, Jiang and Bai found that 53 percent were the result of internal factors in healthcare entities.

"One quarter of all the cases were caused by unauthorized access or disclosure—more than twice the amount that were caused by external hackers," Jiang said. "This could be an employee taking PHI home or forwarding to a personal account or device, accessing data without authorization, or even through email mistakes, like sending to the wrong recipients, copying instead of blind copying or sharing unencrypted content."

While some of the errors seem to be common sense, Jiang said that the big mistakes can lead to even bigger accidents and that seemingly innocuous errors can compromise patients' personal data.

"Hospitals, doctors offices, insurance companies, small physician offices and even pharmacies are making these kinds of errors and putting patients at risk," Jiang said.

Of the external breaches, theft accounted for 33 percent with hacking credited for just 12 percent.

While some data breaches might result in minor consequences, such as obtaining the phone numbers of patients, others can have much more invasive effects. For example, when Anthem, Inc. suffered a data breach in 2015, 37.5 million records were compromised. Many of the victims were not notified immediately, so weren't aware of the situation until they went to file their taxes only to discover that a third-party fraudulently filed them with the data they obtained from Anthem.

While tight software and hardware security can protect from theft and hackers, Jiang and Bai suggest health care providers adopt internal policies and procedures that can tighten processes and prevent internal parties from leaking PHI by following a set of simple protocols. The procedures to mitigate PHI breaches related to storage include transitioning from paper to digital medical records, safe storage, moving

to non-mobile policies for patient-protected information and implementing encryption. Procedures related to PHI communication include mandatory verification of mailing recipients, following a "copy vs. blind copy" protocol (bcc vs cc) as well as encryption of content.

"Not putting on the whole armor opened health care entities to enemy's attacks," Bai said. "The good news is that the armor is not hard to put on if simple protocols are followed."

Next, Jiang and Bai plan to look even more closely at the kind of data that is hacked from external sources to learn what exactly digital thieves hope to steal from patient data.

Provided by Michigan State University