Healthcare providers leak your data

The recent implementation of the General Data Protection Regulation (GDPR) in Europe was another step in the ongoing effort to prevent data breaches and protect your personal and patient information from sophisticated online attackers. Personal data has become a valuable commodity sought after by hackers as many large institutions have fallen prey to, can attest. Surprisingly, a new study shows more health data leaks were caused by healthcare providers than hackers or other external cyber-attacks.

Research from a new joint study conducted by Michigan State University and Johns Hopkins University has shown that in relation to personal health information, more than 50% of recent personal health data breaches were the result of internal factors within hospitals, doctors offices and insurance providers.

You might also like: UK Cyber-Attack, Radiology Response

The findings of the joint 2017 study, show the enormity of data breaches in hospitals in the United States, with 1,800 incidents of large data breaches of patient information over a seven year period where 33 hospitals had more than one significant data breach.

John (Xuefeng) Jiang, lead author and associate professor of accounting and information systems as Michigan State University's Eli Broad College of Business, states that while there is no perfect way to store information, more than half the cases they reviewed were not triggered by external factors but were the result of internal negligence.

Jiang and co-author Ge Bai, associate professor at the John's Hopkins Carey Business School, investigated 1,150 cases from October 2009 to December 2017 to identify what triggered the personal health data breaches that affected 164 million patients. When a hospital experiences any data breach they need to report the incident to the Department of Health and Human Services and classify what they believe is the cause, says Jiang "these causes fell into six categories: theft, unauthorized access, hacking or an IT incident, loss, improper disposal or 'other'."

They found 53% of personal health data breaches resulted from healthcare providers internal issues. "One quarter of all the cases were caused by unauthorized access or disclosure – more than twice the amount that were caused by external hackers," said Jiang. "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."

Although some of the issues seem to be common sense, Jiang said the big mistakes may lead to even greater accidents and seemingly harmless mistakes can risk patient's personal information. From the total external breaches 33% were the result of theft and only 12% attributed to a hack.

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

Sophisticated software and hardware security can protect against theft ad hackers but Jiang and Bai recommend that healthcare providers set simple protocols and internal policies to secure processes and prevent patient data leaks caused internally. Procedures include moving from paper to digital to store medical records, safe storage, creating non-mobile polices for patient protected information and using encryption solutions. For patient health information communication procedures should include mandatory verification of mailing recipients and content encryption.

"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."

As a next step Jiang and Bai are planning to analyse the specific kind of data that is hacked from external sources in order to determine exactly what cyber attackers are interested in stealing from patient data

Source: JAMA Internal Medicine

Image Credit: iStock

Published on : Tue, 20 Nov 2018

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.