ClearDATA
SECURE • HEALTHCARE • CLOUD

The U.S. Data Security Crisis:
Cybercriminals Targeting Healthcare Data

Patient Health Records Attractive to Hackers

The healthcare sector is number two in data breaches in the U.S., with protected health information (PHI) worth up to 50 times more than credit cards or social security numbers alone. The most profitable kind of theft stemming from identity theft is now medical identity fraud. HIPAA lists medical identity theft as including names, Social Security numbers, driver licenses or state identification numbers, credit or debit card information, medical conditions, diagnoses, lab results, addresses, dates of birth, and health insurance data.

Medical Identity Theft Woes Run Deep

Unlike other identity thefts that simply destroy your finances, medical identity theft can also destroy your health and your life. See the side bar on the right for examples of how medical identify theft can wreak havoc. It can also threaten you and your family's safety through delayed or misdiagnosed care. As mentioned in the article linked above, "About 20 percent of victims have told us that they got the wrong diagnosis or treatment, or that their care was delayed because there was confusion about what was true in their records due to the identity theft," says Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance (MIFA).

Organizations that do not successfully protect patient health records ultimately expose their customers to this kind of problem, and also stand to lose substantial income as patients lose trust. The research states that almost half of patients said they would find a different provider if they were informed that their medical records were stolen. Considering the estimated economic value of a patient, Accenture says this could cost providers in excess of $305 billion in cumulative lifetime patient revenue over the next five years!

Legal, Federal and State Fines to Healthcare Organizations Can Exceed $100 Million

On top of the loss in patient-produced revenue, organizations that experience security incidents also incur federal or state regulatory fines that recently have reached into the millions, and legal penalties in the hundreds of millions. Nearly 90 percent of healthcare organizations represented in the Ponemon study had a data breach in the past two years, and nearly half, or 45 percent had more than five data breaches in the same time period. According to the

Example Case #1

This recent article from Consumer Reports, tells the story of a woman who went inside a convenience store to pay for gasoline and returned to her car to find her purse stolen. She cancelled her credit cards, watched her bank account for a few weeks and moved on. A full two years later, she was arrested on suspicion of acquiring more than 1,700 prescription pain pills through area pharmacies - a theft committed with her stolen health identity.

Example Case #2

In another example, a pregnant woman committed identity theft to seek prenatal care. The infant was born with drugs in its system. The woman whose medical identity had been stolen suddenly found herself speaking to child protective services and had to take a DNA test to prove she was not the mother of the drug-addicted infant so she could retain her own four children whom protective services were threatening to take.

HIPAA Journal, the average cost per record for healthcare breaches is the highest among all industries at a current average of $380 per record.

Many Organizations Are Not Prepared or Protected

If you are like many healthcare organizations, there may be gaps in your data security. In many cases, the reason isn't ambivalence, as much as budget. Healthcare providers typically have smaller IT budgets than private sector companies, and a larger set of regulations to meet. Spending on electronic health records (EHRs) has been getting most of the attention and budget, while security and prevention have been moved to the sidelines. This is further complicated by legacy systems that require changes and updates to IT infrastructures which can expose vulnerabilities, oversight, and mistakes. As the pool of data and the scope of regulations increase, healthcare IT professionals are short on time and resources. In addition, budgets that could be best utilized by building out a scalable cloud infrastructure and enhancing compliance and security protocols may be committed to maintaining and refreshing increasingly obsolete on-premise servers. Meanwhile, hackers relentlessly look for vulnerabilities and pounce on the unprepared.

About Us

ClearDATA is the nation's fastest growing healthcare cloud computing company. Top healthcare professionals trust ClearDATA's HIPAA-compliant cloud computing platform and infrastructure to store, manage, protect, and share their patient data and critical applications.

Protecting Your PHI Perimeter

Securing data is a complex science, but three things that may have helped avoid many of the 1,800 breaches reported since 2009 would be to:

- better encrypt data (in transit, in use, and at rest)
- improve internal user monitoring technology
- conduct a third-party security risk assessment

Beware the False Sense of Security

According to a PricewaterhouseCoopers (PwC) survey, 74 percent of health providers believed their security activities were effective. But, after an audit, only 22 percent actually met all advised security criteria.

ClearDATA's security risk assessment expert Carl Kunkelman states that in every assessment he has conducted he has found high, medium, and low risk gaps in security. Many of the vulnerabilities could be avoided in advance of a breach. Do you know your unknowns when it comes to data security? We can help.