WHITE PAPER

6 Alarming Facts About Electronic Health Records

AXIOMATICS
a LEONARDO company

Background

One of the most difficult issues for a CIO to tackle is the ability to know who has access to what critical data and why. In the the case of healthcare and insurance providers, Electronic Health Records (EHR) contain even more valuable information than most data sources due to the sensitive and detailed nature of the information.

EHR systems are built to share information with other healthcare providers and organizations – such as laboratories, specialists, medical imaging facilities, pharmacies, emergency facilities, and school and workplace clinics – so they contain information from all clinicians involved in a patient's care. More channels of information flow means more access to private patient information.

The heightened investment in EHR systems has unfortunately not been matched with corresponding investments in security.

Here are 6 alarming facts about electronic health records and the companies who need to protect them.

What information does an electronic health record (EHR) contain?

- Administrative and billing data, including DOB and social security numbers
- Patient demographics
- Progress notes
- Vital signs
- Medical histories
- Medications
- Immunization dates
- Allergies
- Radiology images
- Lab and test results
- Diagnoses

1. If you store or process medical records, your security threat level is extremely high

More than 25 million patient records were reportedly compromised as of October 2016. And then, in November, the cases spiked: There were 57 health data breaches—the most in any one month in 2016, according to the Protenus Breach Barometer.

EHR data can be exploited in several ways, including submitting false medical claims, acquiring controlled and prescription substances, creating fake identities, extorting patients, accessing government benefits, and obtaining medical devices.

The healthcare industry suffers 340% more security incidents and attacks than the average industry, while health companies are more than 200% more likely to encounter data theft. To put some numbers to this, PwC recently calculated that the average number of daily security incidents to be 117,339 – that's 42.8 million in the year, almost double the amount that occurred in 2011. That's a lot of incidents, and healthcare.

2. Your development team has better things to do

While the allure of a new challenge and the opportunity to build something may sound appealing to a development team, maintaining logic built into an application is costly and inefficient for upfront development and maintenance costs. Not to mention, it's not great for a developer's morale to be stuck writing and rewriting security code. The welcome challenge quickly becomes a tedious and repetitive chore.

IBM research shows that the vast majority of cybercrime is highly organized and generating unprecedented profits, noting that the largest bank heist in history was $30 million compared to the annual $445 billion cost of cybercrime. Solo cybercriminals are also out there, however. Trend Micro observes that these different classes of criminals also dwell in different forums, with petty thieves showing up in more easily accessed sites, and organized cyber thieves residing in closed forums of their own. Put yourself in the position of the hacker – which data would you target?

3. Your colleagues and employees are undermining your security protocols

You may consider your organization's security threats as external in nature. While hackers often attack applications or databases from outside your organization, do not underestimate the amount of internal and privileged users who could unknowingly (or even worse - maliciously) expose your critical data.

According to a recent report, "22.3% of healthcare workers share their passwords with other users." Users share passwords for a variety of reasons, including when delegating work or simply when a coworker asks for it, according to the survey. However, password sharing undermines security protocols and places an organization at increased risk for a data breach.

What's even more concerning is that employees were responsible for more than half of November 2016's breaches, a notable increase from past months.

4. Compliance isn't getting any easier

"Maintaining compliance in the years ahead is expected to become more challenging," says Jeremiah Talamantes, president of Red Team Security – an IT security consultancy in Saint Paul, Minnesota. "This is particularly notable when it comes to compliance requirements catching up with emerging technology. The impact of telemedicine and IoT medical devices, for example, will continue to outpace compliance security and privacy making risk management arduous."

Technology is a key ingredient for a strong and effective security strategy in an era of regulated compliance. But so is a culture of vigilance and caution.

"Maintaining a culture of compliance is key to improving any organization's privacy and security efforts," says Lindsay Petrosky, an Attorney focusing on Data Privacy and Security at Jackson Kelly PLLC in Charleston, West Virginia.

Compounding the fact that EHR are the most valuable and sought after forms of PII (by criminals) they are also exposed to the highest number of stakeholders. The eHealth matrix spans across multiple roles and third parties – from insurance advisors and claims adjusters, to MDs, surgeons and nurses, to clinic receptionists and pharmaceutical retail outlets. With all these stakeholders touching a health record at any given time, dynamically managing who can see what, from where and for what reason is critical.

5. A lot can happen in three months

The victims of medical identity theft are a) seldom informed by the provider that their data has been stolen and b) only find out about the theft an average of three months or more after the theft occurs.

Minimizing the exposure of sensitive material with dynamic authorization will reduce the likelihood of EHR theft. Advanced dynamic auditing capabilities will help you to identify who has accessed what data.

6. Healthcare fraud will cost you a fortune - and your reputation

Annual healthcare fraud losses in the US range between $90 billion and $210 billion from a total annual expenditure of $3 trillion. Naturally, this is bad news for health insurers who are footing much of the bill. While not all fraud is due to stakeholders having too much (or the wrong) access to sensitive data, a percentage of it is. A large percentage of that cost can be minimized by dynamically controlling who can access what data and for what reason.

Dynamic authorization from Axiomatics uses multiple attributes:

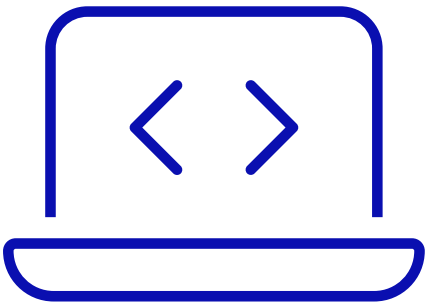
- Role
- Location
- Device in Use location; device in use; time of day; purpose of use; and data source – to enforce access to data inline with corporate policies and regulations.

This means that sensitive data can only be accessed and used by those that have permission to do so, under the correct conditions.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240