White Paper

Is There a Payment Threat Lurking in Your Medical Office?

Nearly **90%** of healthcare providers experienced a breach in the last 24 months.[2]

With all the recent high profile stories about data breaches, payment secuirty is a hot topic in healthcare today. There's been a steep rise in data breaches in the healthcare industry over the last few years.

Collectively the cost to U.S. healthcare providers has grown to an estimated average of $2.2M per breach.[1]

Ponemon's Annual Benchmark Study on Privacy and Security of Healthcare Data revelaed that nearly 90 percent of healthcare providers experienced at least one breach in the last 24 months. Another 40 percent of those had more than five breaches. [2]

Who’s trying to steal payment data?

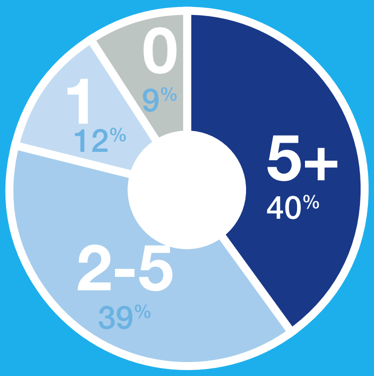
Perpetrators will steal all types of data including medical records, insurance information and payment details. Healthcare organizations reported payment details were stolen in 22 percent of data breaches.[3] Many attacks are carried out by external actors for financial gain. These include:

- Organized crime groups
- Activist and hacktivist groups (e.g., “We Are Anonymous”)
- Foreign government supported hacking operations (also known as cyber-spying)
- Terrorist supported hackers (cyber-warfare)

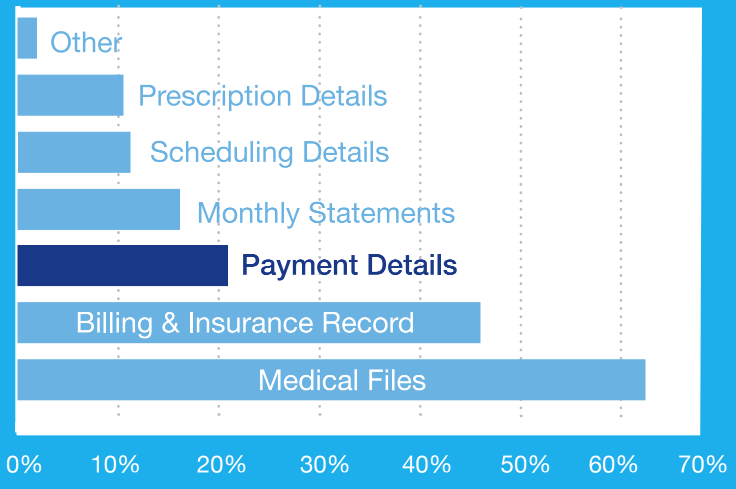
Perhaps more alarming than external criminals are dishonest vendors, suppliers and employees who steal cardholder data and bank account information via access to electronic or paper-based patient information. According to the U.S. Department of Health and Human Services, 38 percent of reported breaches were caused by unauthorized access or disclosure, of which 41 percent were due to paper records.[4] Both internal and external thieves generally seek payment and financial data, as well as personal information that they can quickly sell and convert into cash.

While payment data might not be compromised in every instance, it is certainly at risk whenever an attack occurs. Insufficient technologies and a lack of staff knowledge hamper efforts to identify and resolve breaches. Putting off an investment in payment security now can lead to devastating consequences down the line in terms of monetary loss and penalties.

Healthcare Organizations Breaches last 24 months[1]



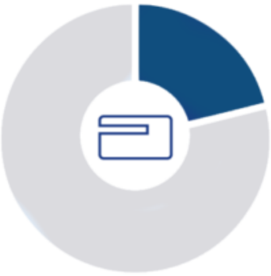
What are the Hackers after?[2] 2016 Patient data successfully targeted (healthcare organizations)



WHAT ARE PAYMENT SYSTEM RISKS?

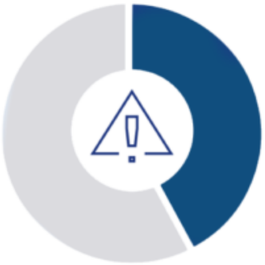
Areas of susceptibility for healthcare providers include point-of-sale systems, websites and malware. Point-of-Sale (POS) software is usually the weak link in a data breach, as it can allow the installation of malware. However, healthcare providers are increasingly imple-menting web portals and mobile devices for payment acceptance, as well as traditional POS devices. So, it’s important to secure payments in all types of environments.

- A POS breach is usually a multi-step attack in which a secondary system is compromised, allowing the criminal to access and attack the primary POS system.
- Web application attacks occur when a thief exploits an e-commerce website vulnerability in order to steal card or other payment data. The application layer sits behind the scenes, powering websites, and is a known soft spot for hackers. This is why it is vital to keep up with the latest security patches.
- Malware invades a system to take control of existing functionality. Once inside, it is programmed to perform malicious actions. For example, malware can be programmed to steal card data from a POS.



22%

of healthcare data breaches were Payment details.



38%

of reported breaches were caused by unauthorized access or disclosure.

320%

rise in cyber attacks on healthcare organizations from 2015 to 2016.

Providers need solutions to mitigate risks

Many healthcare providers realize they will continue to be targeted because they are not investing in the technologies needed to mitigate a data breach (41%).[5] Cybercriminals and other perpetrators are aware that many healthcare providers are underprepared and they are taking advantage of this opportunity. Cyber attacks on healthcare organizations increased 320% from 2015 to 2016.[6]

To effectively address these threats, healthcare organizations need solutions that:

- Increase payment card security.
- Remain compliant with PCI requirements.
- Reduce the scope of the card data environment.
- Segment residual card data onto a segregated network away from clinical data and EHR systems.

PCI-DSS IS THE FIRST STEP IN ADDRESSING THREATS

Payment Card Industry Data Security Standards Compliance (PCI-DSS) is generally recognized as the starting point for payment security. PCI is a set of security standards established for organizations that accept major credit cards including Visa®, MasterCard®, American Express®, Discover®, JCB® and China Union Pay. Every organization that accepts card payments must adhere to these requirements. They are a baseline and provide guidance for applying security technologies, policies and protocols to protect card data. Best practices of the requirements include:

- Controlling card data access on systems and physical environments.
- Monitoring and tracking card data.
- Addressing information security within the organization and with third party vendors.

PCI is not a one-time activity. Healthcare providers need to understand that they can't simply check off compliance from a one-time list and assume that's all that needs to be done. PCI compliance is an ongoing process that requires vigilance.

YOU KNOW WHERE PATIENT CARD DATA IS LOCATED?

It's a common misconception for healthcare providers to believe they know where all their cardholder data is located. But unencrypted card data hiding in unexpected places offers opportunity for hackers and unscrupulous individuals to steal it.

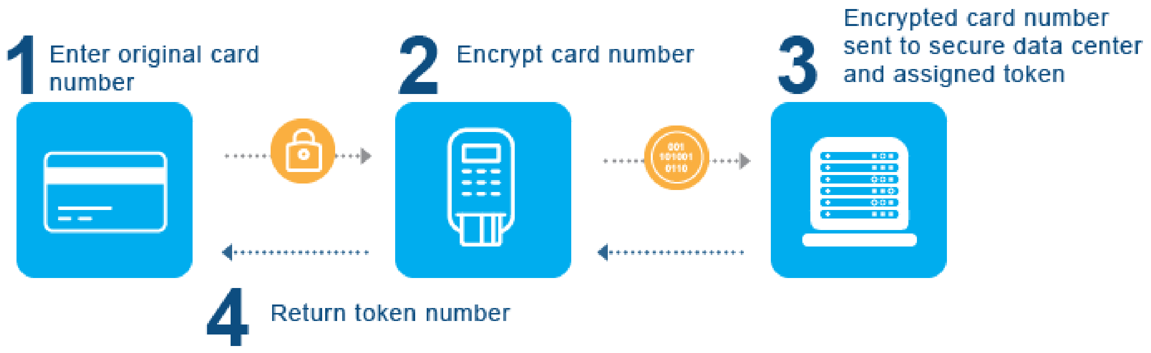
SecurityMetrics examined data from thousands of scans conducted on business networks. The scans revealed that 61 percent of businesses did not know where all their card data was stored.[7] In other words, the card data was located outside the defined card data environment, which consists of the systems that process, store and/or transmit cardholder data, as well as any component that directly connects to or supports these systems.

In our own survey of 90 healthcare providers, 73 percent revealed they were only somewhat confident that they knew where card data was stored within their organization. Another 19 percent were not confident at all.[8]

The ultimate goal of PCI requirements is to protect any systems or processes that touch payment card data. That starts with determining the scope of the card data environment. Improper scoping — card data written on pieces of paper, for instance — contributes to compromises.

All healthcare providers need to determine the extent of their cardholder data environment to gain a better understanding of the people, processes and technologies that touch card data. It is critical to ensure that PCI scope is truly limited to just the defined card data environment.

How does encryption and tokenization work?



1 Enter original card number

2 Encrypt card number

3 Encrypted card number sent to secure data center and assigned token

4 Return token number

Layer security technologies to help fight theft

PCI standards establish best practices, but still might not be enough to achieve truly comprehensive security. Payment security depends on more than just policies and procedures. Since preventing a breach has proven to be nearly impossible, proactive measures should be put in place to address vulnerability points throughout the payment lifecycle.

A layered approach to security – in addition to PCI-DSS compliance – offers the best means to counter more sophisticated attacks. So what tools are available to help Healthcare providers reduce fraud and thwart the efforts of hackers and other data thieves?

EMV, encryption and tokenization work together to address vulnerabilities at all points of the payment process.

1 **EMV®** (Europay, Mastercard and Visa) protects against counterfeit card use in face-to-face transac-tion situations. EMV requires the use of credit and debit cards embedded with a chip that enables card authentication to verify the card is legitimate. EMV is sometimes mistakenly confused with encryption. However, EMV needs to be paired with encryption and tokenization to achieve total security.

The Payments Security Taskforce estimates that, in 2017, 98 percent of all cards issued in the U.S. will be chip-enabled.[9] As consumers become more experi-enced using chip cards, they'll expect to see EMV terminals at their healthcare providers. And as con-sumers increasingly adopt contactless payments, EMV terminals can also provide the functionality for healthcare organizations to accept these payment types (e.g., ApplePay®, AndroidPay™).

2 Encryption is a method of converting card data into another form — cipher text — which cannot be easily understood by anyone except authorized parties. It essentially scrambles the data to protect it while in transit through the POS system and over the payment network. In so doing, encryption eliminates usable information before it leaves the payment terminal and enters the POS or network.

3 Tokenization protects card data at rest by removing it from the provider's environment. Tokens replace the Primary Account Number – the account number on the front of the card – with randomly generated data elements. This token is meaningless to card data thieves – and yet it can still support business pro-cesses, such as card-on-file transactions, purchase analytics, and voids and refunds. Tokenization also helps secure online transactions and new payment types like mobile.

Tokens can be stored indefinitely and used with multiple business applications. They are card-based, so healthcare providers will always get the same token back for a specific Primary Account Number, which preserves analytics. Each card will produce a different token at each merchant or business where it is used. This makes the token identifier worthless outside a specific business' environment. A token can be shared across an entire business, so the same card token could be recognized across multiple clinics or offices that all operate as part of the same medical group.

RevSpring

Intelligence. Engagement. Outcomes.™

RevSpring is a leader in patient communication and payment systems that tailor engagement touch points to maximize revenue opportunities in acute and ambulatory settings. Since 1981, RevSpring has built the industry's most comprehensive and impactful suite of patient engagement, communications and payment pathways backed by behavior analysis, propensity-to-pay scoring, intelligent design and user experience best practices.

RevSpring leverages "Best in KLAS" software and services to deliver over 1 billion smart medical communications each year that drive increased patient engagement and payment rates.

www.revspringinc.com • (248) 567-7300 • learnmore@revspringinc.com

[1] Ponemon Institute, "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016
[2] Ibid
[3] Ibid
[4] U.S. Department of Health and Human Services, Office for Civil Rights, "Breaches Affecting 500 or More Individuals Breach Report," April 23, 2016
[5] Ponemon Institute, "Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2016
[6] HealthITSecurity.com, "Healthcare Cyber Security Attacks Rise 320% from 2015 to 2016," February 15, 2017
[7] SecurityMetrics, "The Danger of Storing Card Data" Infographic, 2014
[8] Elavon/HFMA webinar, "Is a Payment Threat Lurking in Your Hospital," Live Polling Survey, October 7, 2015
[9] CreditCards.com, "Poll: 70 Percent of Consumers Now Have EMV Chip Cards," March 2016

© 2017 Elavon, Inc. All rights reserved. Elavon is a trademark in the United States and other countries. All other marks are the property of their respective owners. All features and specifications are subject to change without notice. ELV-MSC-1774-US-Jun 17 CR-13927273