White Paper:

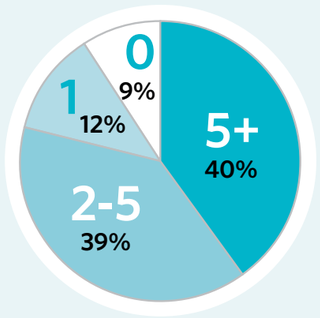
Are there Payment Threats Lurking in Your Hospital?

With all the recent high profile stories about data breaches, payment security is a hot topic in healthcare today. There's been a steep rise in data breaches in the healthcare industry over the last two years. Collectively the cost to U.S. healthcare providers has grown to an estimated average of $2.1M per breach.[1]

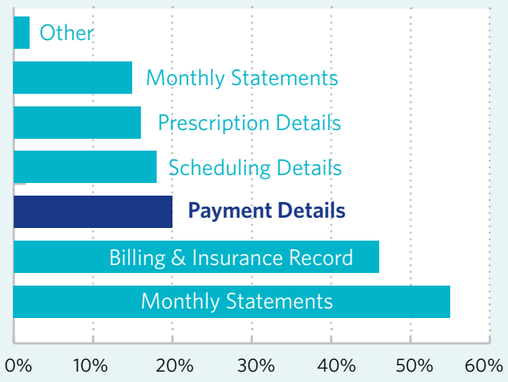
Elavon

The Annual Benchmark Study on Privacy and Security of Healthcare Data published by Ponemon Institute in 2015 revealed the over **90%** of healthcare providers have experienced at least one breach in the last 24 months. Clearly no one is immune and breach can happen to your organization. The perpetrators will steal all types of data including medical records, insurance information and payment details. In 20% of instances, Ponemon reported payment details were stolen.

Healthcare Organizations Breaches, last 24 months



What are the Hackers after? 2014 Compromises by Data Type



So who is after your payment data?

Many attacks are perpetrated by external actors for financial gain, such as:

- 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)

But almost more alarming are the dishonest individuals, such as vendors, suppliers and employees, with internal access to electronic or paper based customer data who engage in crimes of opportunity, stealing cardholder data and bank account information.

Perpetrators, both internal and external, generally seek payment and financial data as well as personal information which they can quickly sell and convert into cash.

Unfortunately many healthcare providers do not feel they are prepared for the growing threat of data breaches. In our recent survey of nearly 80 healthcare providers, over half of them expressed to Elavon that they did not feel they had the right technologies and/or the right personnel to detect and manage a breach.[2]

Cybercriminals and other perpetrators are aware that many healthcare providers are underprepared and they are taking advantage of this opportunity – criminal attacks on healthcare organizations are up 125% compared to 5 years ago.[3] While payment data may not be compromised in every instance, it is certainly at risk whenever an attack occurs.

Insufficient technologies and a lack of knowledgeable staff hamper effectiveness at identifying and resolving breaches. Putting off an investment in payment security now can lead to devastating consequences down the line in terms of monetary loss and penalties.

AREAS OF EXPOSURE IN HEALTHCARE

In 2015 Verizon released a report identifying industries most vulnerable to data breach. They estimated around 80% of breaches were perpetrated by external actors.[4] Areas of susceptibility for healthcare included Point of Sales systems, web applications, and malware.

- A Point of Sale/Point of Service (POS) breach usually tends to be a multi-step attack. Often a secondary system is compromised which allows the criminal to access and attack the primary POS system.
- Web application attacks occur when a thief exploits a vulnerability of an e-commerce website, enabling them 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 taking control of existing functionality and once inside it is programmed to perform malicious actions. For example malware can be programmed to steal card data from a POS.

Over 50% of providers do not feel prepared to detect and manage a breach.

Addressing threats & preventing card data breaches

The Point of Sale (POS) software is the usual suspect when a card data breach is detected. Typically malware is installed on POS software which enables a data breach to occur but it is not the only concern. We recognize healthcare providers increasingly rely on web portals and mobile payments, in addition to traditional POS devices, for payment acceptance. Therefore it is necessary to secure payments in all types of environments.

PCI-DSS (Payment Card Industry Data Security Standards) compliance is generally recognized as the starting point for payment security. The PCI standards establish a strong set of best practices but this still may not be enough to achieve truly comprehensive security.

A layered approach to security – in addition to PCI-DSS compliance – offers the best means to counter more sophisticated attacks.

Before delving into the topic of layered security, let's talk more about PCI. 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. These requirements provide guidance on how to apply security technologies, policies and protocols to protect card data. It is your baseline of security.

Think about your home. PCI compliance is similar to placing your valuables in a safe and locking the doors to your house. These basic measures decrease the likelihood that your valuables will be stolen.

PCI is not a one-time activity. Just like securing your home, PCI has to be part of daily practices. There's a tendency to view compliance with a checklist mentality but PCI is an ongoing process that requires vigilance. You can't just complete the checklist one time and assume you're done. Your card data environment requires constant monitoring and periodic compliance review.

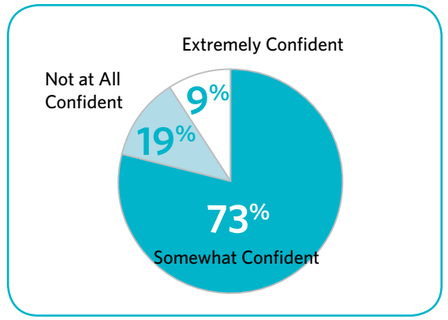
Every organization that accepts card payments must adhere to these requirements. They provide a standardized framework for establishing policies and procedures within your own organization.

As part of best practice, PCI provides guidelines for:

- 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.

Needless to say, payment security depends on more than just policies and procedures. Implementing appropriate technologies such as EMV, encryption and tokenization can further enhance PCI compliance within your organization. As always, technology is most effective when there are documented practices in place to guide their use.

Confidence about card data location



HOW CONFIDENT ARE YOU THAT YOU KNOW WHERE ALL YOUR CARD DATA IS LOCATED?

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

In our recent survey of 90 healthcare providers, 73% of them revealed to Elavon they were only somewhat confident that they knew where card data was stored within their organization and 19% were not confident at all.[5]

Consider the employee laptop. Do any of your employees store card data on their hard drive? If so, is it password protected? If the laptop is stolen could the thief gain access to systems where card data is stored?

In 2014, SecurityMetrics examined data from thousands of scans conducted on business networks. The scans revealed that 61% of businesses did not know where all their card data was stored.[6] In other words, the card data was located outside what was defined to be the card data environment. Your card data environment 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.

The ultimate goal of the PCI requirements is to protect any systems that touch payment card data. PCI starts with determining the scope of your card data environment. Improper scoping contributes to compromises. For example, card data hiding in error logs could be your undoing.

All organizations need to determine the extent of the cardholder data environment. In so doing, you gain a better understanding of the people, processes and technologies that touch card data across your organization. It is critical to be sure that PCI scope is truly limited to just the defined card data environment.

Now that we've established a good baseline for security with PCI, let's move on to discuss technologies that can help strengthen payment security.

A Layered Security Approach

Returning to our earlier home security example, PCI is similar to storing your valuables in a safe and locking the doors when you're away. These are good security measures but they are not foolproof.

A sophisticated thief skilled at picking locks and cracking codes could break into your home and get into the safe. Adding layers of security such as alarms, outdoor lights, cameras and a fence would certainly further decrease opportunities for theft. All of these elements work together to provide more effective security then just one of these measures by itself. This layered approach can be applied to payments as well.

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. Layered security helps ensure that WHEN – not if – a breach occurs, any data stolen is not useful to the thief or harmful to the organization or consumers. The premise is, *if there's nothing to find, there's nothing to steal.*

So what tools are available to reduce fraud and thwart the efforts of hackers and other data thieves? There are three primary security technologies available to protect different aspects of the payments system.

- **EMV** protects against counterfeit card use in face-to-face transaction situations. EMV is sometimes mistakenly confused with encryption. EMV needs to be paired with encryption and tokenization to achieve total security.
- **Encryption** protects card data in transit (while moving through the processing system)
- **Tokenization** protects transaction data that is at rest (stored in health system locations). Tokenization helps secure online transactions and new payments types such as mobile.

These three technologies work together to address vulnerabilities at all points of the payment process.

EMV

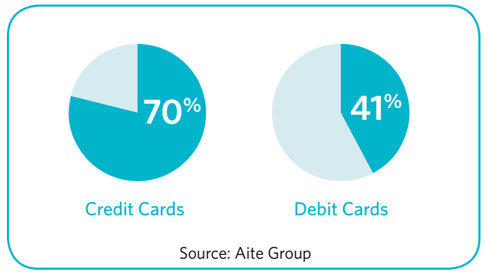
As cardholders many of us have received a chip card from our financial institution within the last few months. Card issuers are actively distributing these cards and it's anticipated that 70% of U.S. credit cards and 41% of U.S. debit cards will be EMV-enabled as of the end of 2015.[7] EMV requires the use of credit and debit cards embedded with a chip that enables card authentication to verify the card is legitimate. As noted above, EMV is designed to prevent counterfeit card use at the Point of Sale.

Once organizations start adopting EMV terminals, those that do not could see fraud shift to them. Why? Because criminals will quickly figure out that counterfeit cards can be used at magnetic stripe terminals but not at EMV terminals.

Within healthcare some areas of your business will be more likely to encounter counterfeit card use than others. For example, gift shops, cafeterias, pharmacies and elective services. While counterfeit card use may be viewed by some as less of a concern in healthcare, no industry is immune from this threat.

As consumers gain more experience using new chip cards in EMV terminals in retail, restaurant and hospitality environments their expectations will shift, and many will expect to see their healthcare providers using EMV terminals. And as consumers increasingly adopt contactless payments, EMV terminals can provide the functionality for healthcare organizations to accept these payment types (e.g. ApplePay, AndroidPay).

Chip Cards in U.S. by end of 2015



Source: Aite Group

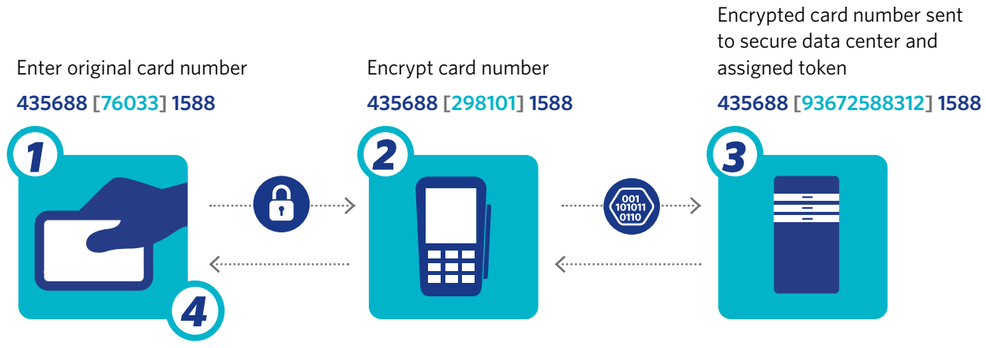
ENCRYPTION & TOKENIZATION

If you have seen the 2014 movie "The Imitation Game" then you know that encryption is not a new technology. It's been around for decades. Encryption is a method of converting card data into another form, called ciphertext, which cannot be easily understood by anyone except authorized parties. It protects card data while it is in transit through the POS system and over the payment network by essentially scrambling the data. In so doing, encryption eliminates usable information ***before it leaves the payment terminal and enters the POS*** or network.

Protecting data at rest is also critically important. Tokenization protects card data at rest by removing it from your 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 processes, such as card-on-file transactions, purchase analytics, and voids and refunds. If you wish to remove cardholder data from your processing environment then tokenization is a key component.

Tokens can be stored indefinitely and used with multiple business applications. Tokens are card-based so businesses 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 eliminates portability by making the token identifier worthless outside a specific business' environment. A token can be shared across an entire business enterprise so the same card token would be recognized at a hospital, a pharmacy and an urgent care clinic that all operate as part of the same healthcare system.

Encryption and tokenization data flow



Healthcare systems have complex, interconnected payment environments often consisting of multiple facilities including hospitals, clinics, long-term care facilities, hospices, foundations, pharmacies and retail operations. Your daily focus is on caring for people; not payment security. Using advanced technologies and vendor provided solutions can enable your organization to:

- increase payment card security
- remain compliant with PCI requirements
- reduce the scope of your card data environment
- segment any residual card data onto a segregated network away from clinical data and EHR systems

PCI Compliance is your starting point for security. But to further mitigate the risk of a card data breach, your organization should include EMV, Encryption and Tokenization as part of your payment security strategy.

Elavon is a leader in payment security offering specialized solutions designed for healthcare. Our dedicated healthcare team can provide expertise and products to help your organization improve revenue cycle management and payment processes. Learn about payment security and our healthcare solutions by visiting www.costcopaymentprocessing.com/healthcare.

1 Ponemon Institute, 5th Annual Benchmark Study on Privacy & Security of Healthcare Data, 2015
2 Elavon sponsored HFMA Webinar, "Is a Payment Threat Lurking in your Hospital", Live Polling Survey, October 7, 2015.
3 Ponemon Institute, 5th Annual Benchmark Study on Privacy & Security of Healthcare Data, 2015
4 Verizon Data Breach Investigations Report 2015
5 Elavon sponsored HFMA Webinar, "Is a Payment Threat Lurking in your Hospital", Live Polling Survey, October 7, 2015.
6 SecurityMetrics The Danger of Storing Card Data Infographic, 2014
7 Aite Group, EMV: Lessons Learned and the U.S. Outlook, June 2014

Elavon