PCI DSS Compliance for Healthcare

Best practices for securing payment card data

In just five years, criminal attacks on healthcare organizations are up by a stunning **125%**.[1] Why are these data breaches happening? Both criminal outsiders and malicious insiders are at fault here. The perpetrators will steal all types of data including medical records, insurance information and payment card data. The threat of payment card data theft makes it important to follow PCI DSS compliance requirements.

[1] Ponemon Institute, Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data, May 2015.

Elavon

What is this thing called PCI DSS?

PCI DSS, the Payment Card Industry Data Security Standard, is a set of best practices all companies that accept credit card transactions must follow. This is true whether the company is big or small and regardless of transaction numbers or who actually processes that card information. PCI DSS is broad, encompassing every aspect of the extensive cardholder data environment. This includes employee training, documented policies, physical security and even online security.

The very first version of PCI DSS, was released in 2004. PCI DSS is designed as a way to both improve cardholder information security and prevent the devastating impacts of credit card fraud. On January 1, 2015, the third version of the PCI DSS was released, and it centers on making cardholder security a part of everyday life. Some of the changes found in the latest version of PCI DSS include enhanced user education and awareness, a more flexible standard and clarification for the compliance responsibilities of third parties.

The best way to look at PCI is to compare it to your home. When we leave our homes for work each day, we lock our doors. But are you content with that alone? Let's say you have jewelry in your home worth $1,000,000. Do you have enough trust to put the jewelry on display in your front window while you are away, even if your door is locked? You'd almost certainly want to secure valuables in a better location, just in case someone tried to steal them. In a way, PCI DSS is like going the extra mile to secure the cardholder's environment. Not only do you want to secure the environment, but you'll also want to prevent the intrusion from happening in the first place and limit exposure if it does occur.

What is the value of the PCI program?

While PCI DSS compliance is mandated for any organization that handles credit card data, it can be more helpful to approach your PCI program as an investment. Near-term benefits center on helping your organization through the validation process, and once implemented provide the foundation to ensure compliance in the future.

Complying with PCI DSS as a healthcare organization means embracing the opportunity to communicate with your patients and the community at large about payment data security. After all, news stories about hacking and breaches mean that consumers are more aware of this risk than ever before, and they naturally want to protect their data. PCI DSS can be an effective way for healthcare providers to show consumers exactly what's being done to protect and secure valuable cardholder data.

How do I get started?

Some of the basic components of a PCI program can be very straightforward. For example, you might want to start by assessing where card data is captured, transmitted and stored within your environment. You can map your network to locate card data and conduct a vulnerability scan for card processing services to identify any weaknesses. These scans are available online and through vendors. Vulnerability scans are required each quarter as part of a PCI program, but additional periodic scans can be an extra help. In addition, instituting a system scan process is an effective way to check items like password strength and whether security patches are properly installed.

Establishing a comprehensive PCI program doesn't need to be overwhelming. Certified PCI vendors can be hired to help you assess and scan your environment. Be sure to look for a vendor that offers data breach protection in addition to software processes like the ones mentioned above. A key benefit of data breach protection is the financial reimbursement for expenses like forensic costs, card replacement costs, any incurred fraud losses and card network assessments, conducted by Visa and MasterCard.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Source: PCI Security Standards Council, October 2010

Calculating Your Risk Factors

RISK	=	VULNERABILITY	X	EVENT COST
		likelihood of threat success		*total cost both tangible & intangible of a compromise*

For Example
This example is illustrative. It demonstrates that calculating the potential risk makes the value of investing in PCI evident.

$2,000,000	=	2	X	$1,000,000
annually at risk		*successful attacks*		*total cost per attack*

PCI – What's My Risk?

This question is one of the most common that we get from our customers. The issue isn't if your organization will be subject to attempted data compromise but unfortunately, when the attack will occur. It is critically important for you to examine just how strong your existing security practices are before settling on the right balance between time, resources and effort required to implement a solid program. We always look at the cost vs. value equation carefully so that our healthcare customers can understand that risk.

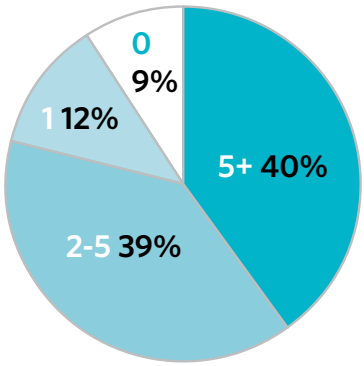
A good comparison might be car insurance. Most of us get in a vehicle daily to get to work, and every time we do, there is a high risk. Other drivers might be speeding, texting, reading, intoxicated or just distracted from the road. Our threat level when driving a car might be at a full 100%. However, our vulnerability level is more moderate, and the chance of actually having an accident might be at 50% or even less. If you're in an accident, however, the cost could be anywhere from $0 to a catastrophic amount. To safeguard against those risks, we take out car insurance. In this context, we can think of PCI as similar to insurance, in that it is a set of best practice safeguards designed to mitigate data breach risks. It is all about taking precautions to establish a secure environment and limit threats.

Every health care business, large or small, is at risk. Hackers are looking for vulnerabilities in a program, an entire system or just a specific application. When data thieves discover the vulnerability, they exploit it to compromise the system and steal valuable data. In addition to payment card data, they can steal confidential information, employee data and even the medical data of patients.

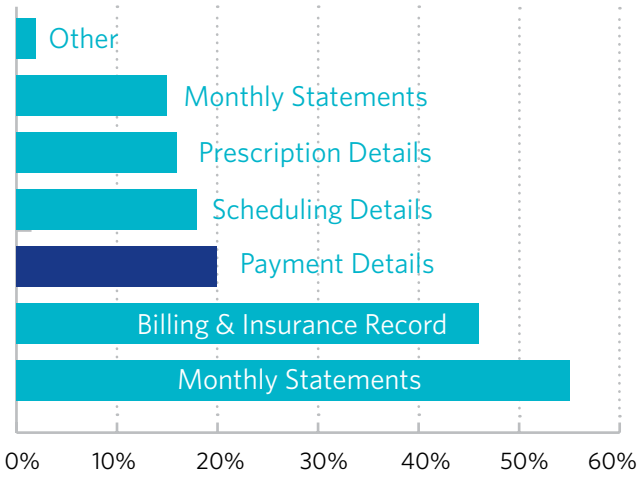
In a 2015 Benchmark Study on Privacy & Security of Healthcare Data, the Ponemon Institute found that 91% of the healthcare providers in the survey had a data breach in the last 24 months. In 20% of those cases, they reported the loss and theft of payment details.[2] This highlights the scope of the problem, bringing it to the front door of every healthcare organization.

[2] Ponemon Institute, 5th Annual Benchmark Study on Privacy & Security of Healthcare Data, 2015

Healthcare Organizations Breaches, last 24 months[2]



2014 Compromises by Data Type[2]



Inside a Breach

There's no more painful or difficult conversation than the ones we have telling customers that they might have experienced a data compromise event. Understanding how a breach investigation actually works can be helpful:

A typical breach is first identified by a card network like Visa, Discover or MasterCard. This is triggered via a Common Point of Purchase notification, or CPP. A CPP notification can identify multiple cards reporting fraudulent transactions during a specific time range at a single business. Clients can use the details of the notification to pinpoint common factors like the specific employees, terminals or systems involved. At Elavon, we take action right away when we receive a CPP notification, contacting our customer immediately and advising them about possible issues.

Next, we give customers detailed information on how to investigate the breach and how to tell if it is contained. A vital step of the process is making sure that every organization completes a thorough investigation, while taking care not to destroy any key pieces of evidence. Imagine a crowd of people trampling over a crime scene and contaminating it: that's entirely possible in the digital world, too! In some cases, a PCI Forensic Investigator, called a PFI, is needed to complete the investigation. Alternatively, the client can use the evidence to handle the investigation on their own. The client's findings can be reported to Elavon through a questionnaire, or a PFI can issue a forensic report to Elavon and card networks.

If any card data appears at risk, the various card network take action to gather information and report the risk to banks. Your organization's name doesn't need to be involved at this stage. Instead, only the necessary details regarding fraudulent use and transactions need to be passed on. Once an investigation is closed and the breach resolved, we advise our customers to revalidate their compliance with PCI DSS. After validation is complete, new PCI DSS documents will be delivered to any impacted card networks. This can be helpful in ensuring the risk of future data breaches is minimized.

***81%** of compromised businesses did not self-detect the breach.*[3]

***111 days** – median time from intrusion to containment.*[3]

Costs of a Data Breach

PCI DSS is designed to reduce the costs of a data breach in three ways. First, it lowers the risk of a payment card compromise from occurring. Second, it reduces the duration of a compromise. Third, it limits the type of data that could be exposed to criminals and fraudsters.

According to a 2015 Trustwave Global Security Report, 81% of those businesses that were victims of a data compromise didn't self-detect the breach. [3] The overwhelming majority of these catastrophic breaches are identified by Visa, Discover and other card networks. That same Trustwave report also quantified the median time period between intrusion and containment at an unimpressive 111 days! Every extra day it takes to contain or even identify a data breach is more money lost to an organization by the fraudster with undetected access to your data.

Hard costs start with the investigation itself. Card networks often require a forensic investigation before they take action. This is so that both the healthcare organization and the card networks can see when the compromise started, when it was contained and what the full scope really is. An investigation like this averages at a substantial $12,000 for a small business. A larger business could easily expect to pay much more for a full forensic investigation. After the investigation, payment networks might issue fines, fees, assessments, and card replacement costs to your organization. These are yet another example of hard costs, and they can range from a few thousand dollars to hundreds of thousands of dollars.

Soft costs can be more difficult to quantify. Although soft costs come in many varieties, the most expensive might be damage to a healthcare organization's brand. A data breach can lead to a poor image and a bad reputation among patients or the community at large. Counteracting this damage often takes a massive PR effort, which in turn takes resources away from other important tasks like patient care.

Think of a forensic investigation like a financial audit. As long as it is going on, it limits what employees can get done, and it might interfere with operational performance or managing quality of care. Another soft cost is any civil lawsuits or regulatory complaints that can pop up. Unhappy consumers may be justifiably upset that their payment data was stolen or jeopardized by their healthcare provider, and as a result, you could incur substantial expenses like legal fees and settlements.

Both hard and soft costs can hurt a healthcare organization. However, there is a way to reduce the risk of encountering these costs by preparing in advance. Engaging in PCI DSS validation and making card data security a part of the routine is the solution. As the saying goes, "An ounce of prevention is worth a pound of cure."

[3]Trustwave 2015 Global Security Report

What do I need to do in order to validate?

We've already established that any entity accepting, transmitting or storing payment card data must validate compliance with the PCI DSS. How that happens, however, can vary based on the existing protocol for card processing.

First, customers need to select the right Self-Assessment Questionnaire, or SAQ. This relates to how a customer handles payment card data presently. There are seven potential SAQs that could apply, and each is driven by the technology in place. If you can't select the correct SAQ, it might mean you aren't able to identity all the different ways you need card security. To help select the right SAQ, view the chart below.

Customers may also need to pass a vulnerability scan. This is only necessary if they connect to the Internet when processing card payments. A vulnerability scan is an automated tool that scans the network and can identify any known vulnerabilities. The NIST, or National Institute of Standards and Technology, issues an extensive list of all these potential vulnerabilities. Quarterly scans are required to achieve compliance, but many of our healthcare customers finds a more frequent cadence preferable.

A penetration test may also be required for some customers. Completed by ethical hackers, a penetration test is designed to find out whether an experienced IT professional can hack into the environment where customer cards are processed. After the penetration test, a report is issued detailing the findings. This report advises customers on any security gaps that might exist and how to close them.

SAQ	Description
A	Card-not-present businesses (e-commerce or mail/telephone-order), that have fully outsourced all cardholder data functions to PCI DSS compliant third-party service providers, with no electronic storage, processing, or transmission of any cardholder data on the business' systems or premises. Not applicable to face-to-face channels.
A-EP	E-commerce businesses that outsource all payment processing to PCI DSS validated third parties, and that have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No storage, processing, or transmission of cardholder data on business' systems or premises. Applicable only to e-commerce channels.
B	Businesses using only: • Imprint machines with no electronic cardholder data storage, and/or • Standalone, dial-out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels.
B-IP	Businesses using only standalone, PTS-approved payment terminals with an IP connection to the payment processor with no electronic cardholder data storage. Not applicable to e-commerce channels.
C	Businesses with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.
C-VT	Businesses that manually enter a single transaction at a time via a keyboard into an Internet-based, virtual payment terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels.
P2PE	Businesses using only hardware payment terminals included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce businesses.
D	Any business that does not qualify for one of the other SAQs or qualifies for more than one SAQ, or who stores credit card data in their environment.

Source: PCI Security Standards Council

For more information

Please visit the Elavon Security Center for more information at **www.elavon.com/security-center/elavon-security/safe-t.html** or visit the PCI Security Standards Council website at **www.pcisecuritystandards.org**.

ELV-MSC-1764-US-Jul 17 CAT-14158545

Elavon