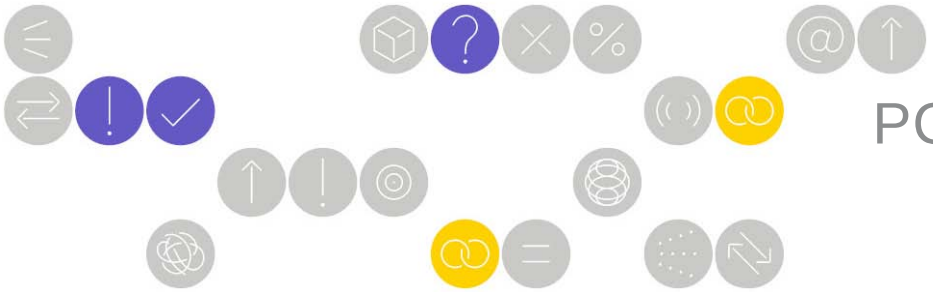
vantiv™



PCI Compliance in the Healthcare Industry

March 2012

Healthcare providers must treat PCI DSS standards with the same care as HIPPA laws

Health care providers are acutely aware of the requirements set forth by the complex network of state and federal data privacy protection laws (e.g., HIPAA) to maintain protected health information (PHI). Yet, it's been widely identified that the healthcare industry as a whole is sorely lagging in compliance with PCI DSS, a set of Data Security Standards set forth by the Payment Card Industry designed to enhance payment card data security. Why the discrepancy? Perhaps it is the misconception that by meeting HIPAA requirements a healthcare provider is also complying with PCI DSS.

Make no mistake - the two are different. HIPPA mandates the protection and security of protected health information while PCI DSS requires the protection and security of cardholder data. Healthcare providers are not exempt from PCI DSS requirements simply because they are HIPAA compliant a mistake that can place healthcare providers t at risk.

This issue is receiving more scrutiny in recent years. The rise in consumer directed healthcare has led to a dramatic increase in patient payments - with patients increasingly using their own credit or debit card to make co-payments or paying large portions of their bills as a result of the increased popularity in higher-deductible health insurance plans, health savings accounts (HSAs), and flexible spending accounts (FSAs).

Fraud Is Shifting to Smaller and Mid-Size Merchants

Hackers have generally targeted their attacks against large businesses, having successfully accessed a number of large cardholder databases. They have stolen large quantities of unprotected card numbers. In response, large businesses have invested heavily in PCI DSS compliance and other preventive security measures, causing hackers to change their strategy. Instead of targeting stored data, now hackers have turned their attention toward intercepting card numbers while transactions are being processed (in motion) through the retailer's network. Several notable, large data breaches that have occurred in the past few years were the result of an organized assault by a multi-country hacker team that used sophisticated means to capture unencrypted card authentication data traveling over the network on its way to the payment switch.1

Businesses of all sizes, but most notably large businesses, have been forced to adopt new technologies designed to secure vulnerable points. These investments, while successful, have cost billions of dollars to deploy. The National Retail Federation estimates that merchants spent more than $1 billion on PCI compliance in 20092 to protect cardholder data.

As large businesses have made the necessary security enhancements to fend off attacks, hackers have turned their attention to small to mid-size retailers. Please note that while hospitals and health care systems may look and feel like a large business, many times the processing of card transactions is decentralized, potentially making it as susceptible to a breach as a small or medium sized merchant or business. A 2010 report by Verizon shows that the number of breach incidents is increasing and that more than 63% of reported data breaches occurred with businesses that have 100 or fewer employees. 3 That study cites, "Criminals may be making a classic risk vs. reward decision and opting to play it safe" in light of recent arrests and prosecutions following large-scale intrusions into financial services firms. Numerous smaller strikes on hotels, restaurants and retailers represent a lower-risk alternative, and hackers may be taking greater advantage of that option.

# Employees	Incidents	Percentage
1-10	46	6.10%
11-100	436	57.4%
101-1,000	74	9.70%
1,001-10,000	49	6.50%
10,001 – 100,000	59	7.80%
100,000+	55	7.20%
Unknown	40	5.30%
Total	**759**	**100%**

2011 Data Breach Investigations Report
Verizon, 2011

What This Means for the Healthcare Industry

Many healthcare practices consist of only a handful of employees. These small to mid-size healthcare practices typically spend less time and money on PCI compliance or other ways to secure cardholder data. Coupled with the misconception that being HIPPA compliant means you are PCI compliant, a dangerous combination arises.

PCI DSS requirements are extensive and can be difficult to understand. The result is that security falls by the wayside and sets the practice up as a prime target for hackers. If breached, the financial and reputational impacts to the practice are extensive, and can compromise revenues and business continuity.

Evaluate Your PCI Compliance Status

Healthcare practices need a partner that can help answer the questions, “What does it mean to be PCI compliant? How can I tell if I am?” The good news is that easy-to-use, online tools are available to help you evaluate your current compliance status and offer guidance about how you can improve your network security. By asking you a series of questions about your processing environment, the tools will help you to identify areas of non-compliance and will also provide direction on correcting deficiencies. This can provide you with valuable insights about where to focus your time and investments.

Take Action

Individuals turn to healthcare experts for regular, preventative checkups as well as when they are ill. Don’t make the mistake of turning to a payment expert after it is too late and your data has been compromised. Seek preventative help now.

Vantiv, a leader in healthcare payment processing solutions can address these challenges and more.

[1] End-to-End Encryption, Tokenization, and EMV in the US, Javelin Strategy & Research, 2010
[2] http://www.nrf.com/modules.php?name=Pages&sp_id=1052 Accessed Dec. 22, 2009
[3] 2011 Data Breach Investigations Report, Verizon, 2011