California Healthcare News®
cahcnews.com
Articles, Interviews and Statistics for the Healthcare Executive

PCI DSS: One More Data Security Regulation Required for Providers

By Kevin Villanueva
Senior Manager
Infrastructure and Security Leader
Moss Adams LLP

Health care organizations are no strangers to data security regulations. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its subsequent iterations have mandated stringent data security requirements around patient privacy and protected health information. Indeed, the HIPAA privacy and security rules have precipitated a cultural shift in the health care industry, altering how covered entities and their business associates operate.

Now the Payment Card Industry Data Security Standard (PCI DSS) is slowly doing the same. However, knowledge of this industry regulation among health care providers isn't as deep as it is with HIPAA. In fact, providers often believe that because their organization is in compliance with HIPAA, it's also in compliance with the PCI DSS. This isn't the case. While HIPAA's data security requirements apply to protected health information, the PCI DSS is exclusive to debit and credit card transactions.

The PCI DSS was formulated by the major card brands (MasterCard, Visa, American Express, JCB, and Discover) in 2004. Its goal is to provide a set of standardized technical requirements for securing payment card data. While the card brands each have their own unique data security compliance programs, the PCI DSS is universally accepted by the card brands as the de facto set of data security measures to which all merchants and service providers that take payment card information need to adhere.

Health care providers that accept debit and credit cards as payment for co-pays, lab fees, and services rendered are subject to PCI DSS compliance. This applies to all forms of payment card transactions—carbon-copied card swipes, electronic card swipes, e-commerce sites, etc. Simply put, if you accept debit and credit cards as a means of payment for goods and services, you need to comply with the PCI DSS. Failure to do so can result in anything from heavy fines from the card brands to permanent revocation of the ability to process payment card transactions.

The PCI DSS mandates that merchants and service providers who accept payment cards follow a set of 12 security requirements:

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.

3. Protect stored cardholder data.

4. Encrypt transmission of cardholder data across open, public networks.

5. Use and regularly update antivirus software.

6. Develop and maintain secure systems and applications.

7. Restrict access to cardholder data by business need-to-know.

8. Assign a unique ID to each person with computer access.

9. Restrict physical access to cardholder data.

10. Track and monitor all access to network resources and cardholder data.

11. Regularly test security systems and processes.

12. Maintain a policy that addresses information security.

Many will look at this list and think that the requirements are basic data security principles and they're already observing many of them. However, each of the 12 requirements have multiple subrequirements that provide detailed prescriptive guidance on how the requirements are to be applied to the cardholder data environment and systems. If the subrequirements aren't followed as described by the PCI DSS, the merchant or service provider fails in complying with the standard. While the HIPAA security rule allows for a good amount of interpretation of the implementation specifications and how the covered entity or business associate applies controls to meet the spirit of the requirement, the requirements under the PCI DSS are more circumscribed.

To add to the confusion, a merchant or service provider may have different validation requirements to demonstrate PCI DSS compliance. Merchant levels are established based on the volume of aggregated payment card transactions and are often determined by the merchant's payment card processing bank. Depending on the organization's merchant level, either an on-site security assessment by a PCI qualified security assessor (QSA) or completion of a self-assessment questionnaire, along with quarterly network vulnerability scans, may be required. For example, merchants who are classified as Level 1 (over six million card transactions annually) are required to undergo an annual on-site security assessment by a PCI QSA and have quarterly vulnerability assessment scans performed.

Although distinctly different in what the regulation applies to, some of the data security controls required under the PCI DSS can also be applied to the HIPAA security rule. These include:

- Requirement 1, Install and Maintain a Firewall Configuration to Protect Data—HIPAA Section 164.312(e)(1)

- Requirement 5, Use and Regularly Update Antivirus Software and Programs—HIPAA Section 164.308(a)(5)

- Requirement 8, Assign a Unique ID to Each Person with Computer Access—HIPAA Section 164.312(a)(1)

Efforts to comply with both HIPAA and the PCI DSS don't have to be conducted in separate silos. Yes, the data and scope are different for each. However, applying sound security controls and protections around critical and sensitive data should be an ongoing process, and one that should be generally followed in health care organizations. With this axiom guiding data security initiatives, complying with HIPAA and the PCI DSS can be a combined process—resulting in a stronger data security environment and a better chance at successful compliance with both requirements.

A PCI QSA, Kevin Villanueva has been in the IT field since 1997 and leads the firm's information security and infrastructure practice. In addition to conducting HIPAA and PCI DSS compliance audits, he specializes in technology security assessments, penetration testing, systems auditing and assessments, network and system design, disaster recovery planning, and systems integration, implementation, and support. You can reach him at (206) 302-6542 or kevin.villanueva@mossadams.com.

Reprinted with permission from the California Healthcare News. To learn more about the California Healthcare News visit cahcnews.com.