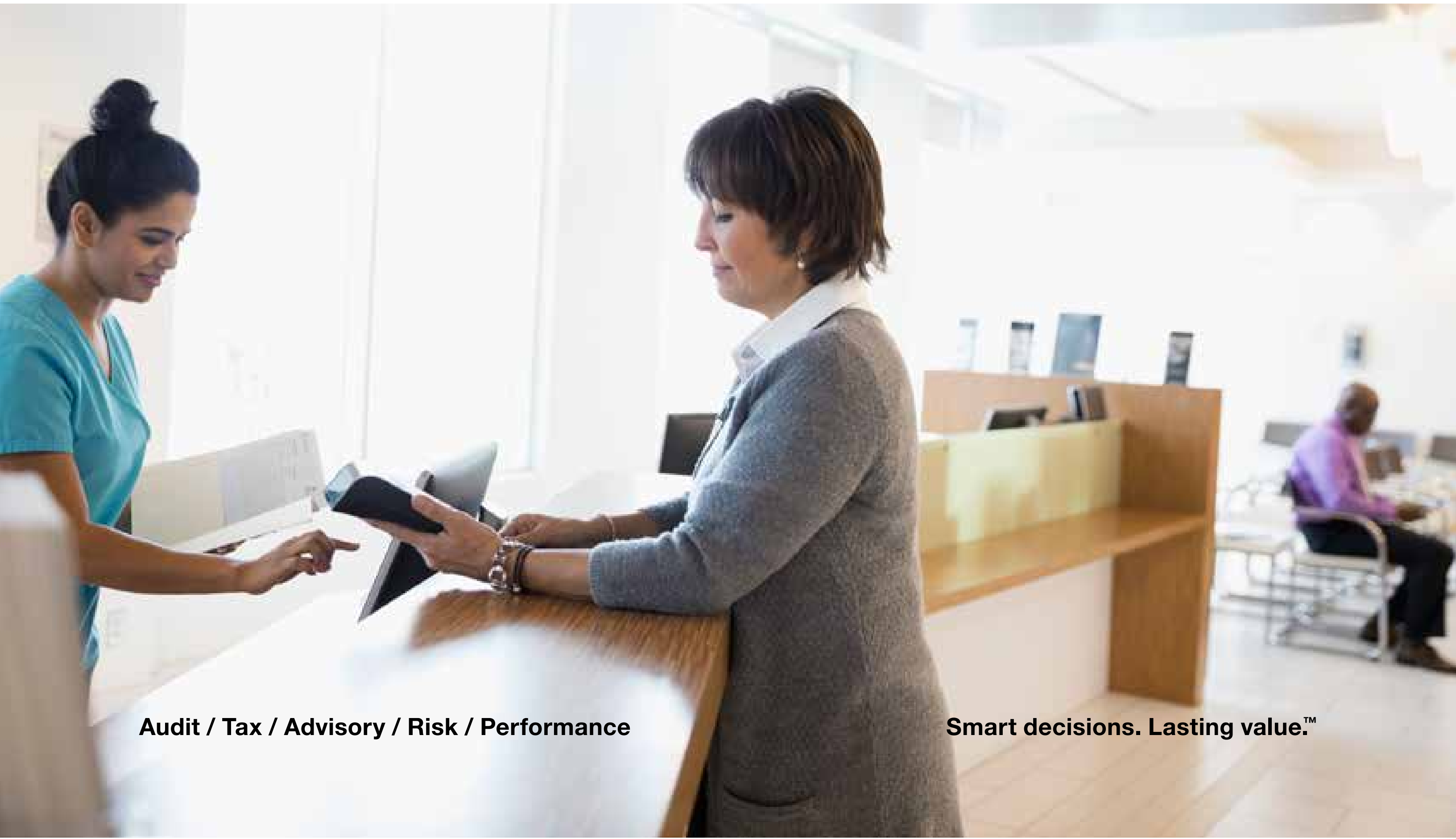
December 2018

Protecting Cardholder Data

A Healthcare Security Concern

An article by Brandon P. Breslin, CISA, QSA, CTGA; Angie K. Hipsher-Williams, CISA, QSA, CTGA; and Jonathan J. Sharpe, CISA, QSA



Audit / Tax / Advisory / Risk / Performance

Smart decisions. Lasting value.™

Cardholder data security is a growing concern for healthcare organizations. Today's healthcare industry services many areas that accept payment cards, including credit, debit, and health savings account cards. And with a growing number of types of card readers, applications, and other third-party service providers accepting payments at different locations, the risks of a data breach continue to rise within hospitals.

Incidents of high-profile payment card data breaches within the industry are significantly on the rise. According to a 2018 report by Verizon, 24 percent of all breaches occurring in 2017 were in the healthcare industry.[1] Of those incidents, miscellaneous errors, malware, and hacking were the three most common areas of data compromise.[2] With a data breach potentially resulting in negative financial and legal consequences and costly reputational damage, the stakes are high for today's healthcare organizations to protect sensitive patient information, including cardholder data.

Because of these escalating concerns about data breaches in the healthcare industry, any healthcare organizations that accept payment cards should review their documented internal policies and procedures related to cardholder data. They also should explore increasing data security within their environments to reduce cybersecurity risk.

Identifying and reducing cardholder data risk

All healthcare organizations that store, process, or transmit cardholder data must comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI compliance standards provide baseline requirements and controls to get healthcare organizations thinking about security by reducing their potential data exposure risk. Though compliance with these standards is critical and required, it does not guarantee an organization's data is secure or protected from a data breach.

Overall, healthcare organizations already have been aware of and committed to securing confidential patient information, including addresses, health information, and social security numbers, for general security purposes and for purposes of complying with the *Health Insurance Portability and Accountability Act of 1996* (HIPAA). A shift in mindset is needed, however, to consider payment card data as equally sensitive and confidential. To mitigate potential risks of a payment card data breach, all patient card data must be held to the same security standards as those in place for information covered under HIPAA.

As with HIPAA-related policies, management within healthcare organizations should champion efforts to implement standardized policies and procedures that help protect confidentiality of payment card data among employees of hospitals, clinics, and other patient-facing entities. This is especially important in today's healthcare climate as healthcare organizations continue to merge and grow. When organizations add new locations and employees and evolve into much larger institutions as a result of merger and acquisition activity, the risk of data exposure grows significantly.

Top ways to identify and reduce cardholder data risk include the following:

- **Perform a data discovery exercise.** To understand risk and improve payment card security, an organization must first understand how cardholder data moves throughout the organization. The organization should perform a comprehensive audit of where cardholder data is accepted and stored (including paper and electronic storage) across the entire institution. For a larger health system, this could include multiple clinics or specialty locations. In addition, all organizations should consider the various methods by which cardholder data is provided by patients, including in person, over the phone, online, or via fax, mail, or email. This also will help make the healthcare organization aware of any third parties that may have access to cardholder data or have connectivity that would extend the cardholder data environment.

- **Do not store cardholder data unless it is absolutely required.** If cardholder data is not required for a legitimate business purpose, healthcare organizations should not store it anywhere (in paper or electronic form). If it is necessary for the organization to store cardholder data, the organization should restrict the number of personnel who are exposed to the data (including limiting third-party access where possible). For each organization, this will vary according to who needs access to payment card information for their day-to-day job functions. Limiting the number of personnel exposed to card data is especially important given another finding in the Verizon report: Of all the industries studied in the report, healthcare had the highest incidence of "internal actors" behind data breaches, with 56 percent of all breaches initiated internally.[3]

- **Devalue cardholder data by outsourcing storage of it and using technologies such as tokenization.** Another way organizations can reduce cardholder data-related risk is by working with a third-party vendor that uses tokenization technology to safely store data. In this scenario, a third party will store cardholder data on behalf of the healthcare organization. When the organization needs to access that data, such as for a recurring payment or a payment installment plan, the third-party vendor sends a "token" instead of the card number. Tokenization applications can be integrated seamlessly into a healthcare organization's billing environment. They also allow payments to be processed without healthcare organization employees having access to the full payment card number.

- **Use point-to-point encryption (P2PE) or end-to-end encryption (E2EE) technologies.** These solutions encrypt card data throughout an entire in-person payment card transaction, making it nearly impossible for anyone to access the card number. Along with their associated tamper-resistant card readers, these solutions can be placed into a healthcare organization's existing environment and can be deployed in locations where card payments are accepted. The PCI Security Standards Council provides a list of recommended P2PE devices on its website.

- **Consider network segmentation.** When payment card information is stored on a "flat," or unsegmented, network, the risk of an individual with malicious intent accessing that information is significantly higher. For example, if someone were to compromise a device on that network, he or she potentially could "pivot" or access various critical points within the network and gain access to sensitive data. Segmented networks that use devices such as firewalls to restrict access to different segments or parts of the network, however, allow for further access restrictions and would make it much more difficult for someone to access the organization's critical network points, adding built-in layers of defense. In an appropriately segmented network, payment card data could be stored in one segment of the network that could be accessed only by necessary personnel with a legitimate business need. While network segmentation is not a requirement for PCI DSS compliance, it is highly recommended and can reduce PCI compliance scope, especially for larger, complex health systems.

▶ While these solutions do expose an organization to financial costs, they also reduce the number of PCI DSS requirements that an organization ultimately has to meet. This, in turn, also reduces the scope of a PCI compliance assessment, which can lower the cost of professional fees incurred from the use of a security assessor and the internal overhead costs of maintaining compliance. Reducing the scope of applicable PCI requirements also will help reduce the organization's data footprint and decrease the likelihood of a breach or leakage of payment card data.

Investing in security

Failure to protect cardholder data can result not only in negative financial and legal ramifications but also in significant reputational damage to an organization should a data breach occur. Investing time and resources in securing cardholder data, therefore, is of the utmost importance for today's healthcare organizations.

Organizations should be fully aware of how and where cardholder data is stored internally and with authorized third parties and understand what steps they can take to secure cardholder data. For assistance with these endeavors, organizations can consider working with PCI Qualified Security Assessors (QSAs), who have been qualified by the PCI Security Standards Council, to evaluate their current cardholder data environment and risks for a potential data breach and to discuss solutions for addressing this critical challenge.

Crowe

Learn more

Brandon Breslin
+1 404 442 1670
brandon.breslin@crowe.com

Angie Hipsher-Williams
Principal
+1 317 208 2430
angie.hipsher@crowe.com

Jonathan Sharpe
+1 317 208 2433
jonathan.sharpe@crowe.com

[1] “2018 Data Breach Investigations Report, 11th Edition,” Verizon, April 2018, p. 5, https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

[2] Ibid, p. 34.

[3] Ibid, p. 33.

crowe.com

“Crowe” is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. “Crowe” may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. The Crowe Horwath Global Risk Consulting entities, Crowe Healthcare Risk Consulting LLC, and our affiliate in Grand Cayman are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document.