TECHNICAL REVIEW

A Commitment to Healthcare Financial Data Security

RevSpring

A Commitment to Healthcare Financial Data Security

According to a new study, 90% of U.S. healthcare organizations feel vulnerable to data security threats. In fact, increases in cybersecurity spending by U.S. healthcare organizations is greater than that of all other vertical markets surveyed.

As digitization continues to gain momentum, healthcare consumers' sensitive personal information is being exposed to more people in more places—and the pressure to ramp up security is intensifying. This pressure is being felt across the globe. According to the 2017 Thales Data Threat Report, Healthcare Edition:

- **90% of U.S. healthcare survey respondents feel vulnerable to data threats.**
- **81% of U.S. healthcare organizations and 76% of global healthcare organizations will spend more money on information security in 2017.**

With the advent of the Health Insurance Portability and Accountability Act (HIPAA), chances are your practice has prioritized the security of private health data. Just as important, however, is the financial component. Are you doing enough to keep your patients' financial information safe and secure?

PCI and Its Role in Protecting Consumers

Consumers today want more options for paying their bills—and healthcare consumers are no exception. In the early 2000s, the growing popularity of electronic payments—and the increased instances of fraud that came along with them—spurred the creation of the Payment Card Industry Data Security Standard (PCI DSS), a robust set of security-related requirements for any business that accepts credit cards. These standards are designed to help organizations implement security policies, technologies, and processes that protect their payment systems from costly security breaches and theft of cardholder data.

Every service provider that takes credit card payments is required to comply with PCI standards, no matter how few transactions it processes.

Why is PCI Compliance So Important?

Whether you process 10,000 credit card transactions each year or 100, it only takes a single instance of identity theft to potentially turn your business upside down. Once a data breach does occur, it triggers a cascade of events that may include the following:

- Your practice must bear the expense of a forensic investigation to determine the exact cause of the breach and the extent of it.
- The credit card company fines your acquiring bank, which in turn passes the fines on to your practice.
- Patients who have been affected by the credit card breach become frustrated and distrustful, and decide to use another healthcare provider.

As the old saying goes, "an ounce of prevention is worth a pound of curew." In today's tumultuous economic environment, your healthcare organization must strive to limit losses and manage costs. Improved financial data security through PCI compliance is a vital part of this effort.

Protecting the Interests of Our Clients, and Their Customers

After 20 years of serving the healthcare industry, RevSpring understands the need to handle patient financial data with the utmost care. Our organization is certified by the PCI Security Standards Council as being fully PCI-compliant. This certification is the result of an annual assessment that confirms our company meets all 12 of PCI DSS requirements:

- **Install and maintain a firewall configuration to protect cardholder data.**
- **Do not use vendor-supplied defaults for system passwords and other security parameters.**
- **Protect stored cardholder data.**
- **Encrypt transmission of cardholder data across open, public networks.**
- **Protect all systems against malware and regularly update anti-virus software or programs.**
- **Develop and maintain secure systems and applications.**

- **Restrict access to cardholder data by business need-to-know.**
- **Identify and authentic access to system components.**
- **Restrict physical access to cardholder data.**
- **Track and monitor all access to network resources and cardholder data.**
- **Regularly test security systems and processes.**
- **Maintain a policy that addresses information security for all personnel.**

Learn More About PCI Security Standards

While PCI compliance alone is enough to set RevSpring apart from many competitors, we don't stop there. We go above and beyond to offer payment solutions that can actually reduce your PCI compliance scope and liability. Our commitment to financial data security spans four critical areas where exposure can occur:

- POS (Point-of-Service) payments made on-site at a client's facility
- CSR (Customer Service Representative) payments made over the phone
- Online payments and phone payments made via IVR (Interactive Voice Response)

Below, we explain some of the extra lines of defense implemented at RevSpring to complement our general PCI-compliant practices.

POS and CSR Payments

POINT-TO-POINT ENCRYPTION (P2PE)

Point-to-point encryption (P2PE) is a payment card security solution that instantly encrypts card data and puts a token on the system so that card number is never exposed on the client's network. RevSpring's, myEasyView®, is a fully P2PE enabled payment solution that drives improvements in patient financial performance by matching payment options to patient needs as early as possible in the

process. For POS payments and phone transactions handled by CSRs, RevSpring clients use an external Point-of-Interaction device that enables users to swipe or key in financial card data. This device supports all payment types and allows for the processing of cardholder data apart from the staff member's workstation. Card data is never stored; instead, it bypasses the client's network and is routed for authorization directly to CardConnect, the gateway service utilized by RevSpring. CardConnect, together with other approved merchants, is listed on the PCI Security Standards Council website as a fully

P2PE-validated solution.

When using P2PE devices, the client's network has a reduction in the scope for PCI compliance—which can significantly reduce the organization's burden when completely the yearly questionnaire. In fact, it could reduce the number of questions required in the questionnaire from hundreds to just a handful.

> The 2017 Thales Data Threat Report found compliance to be the driver behind data security decision-making in the U.S. Globally, preventing breaches and protecting reputation are the leading two security priorities.

EMV COMPLIANCE

EMV involves the use of microchip-reading technology to protect consumers against the misuse of lost or stolen cards; it also makes credit card replication more difficult for identity thieves. RevSpring's POS solution allows for EMV enabled devices. All POS payment transactions are processed through CardConnect, one of only a few gateway providers facilitating EMV transactions and P2PE enabled. Combined with P2PE, EMV helps to significantly boost cardholder security.

Online Payments and IVR

mySecureBill® is RevSpring's PCI compliant user-friendly online billing portal that gives patients a wide array of online and mobile payment options. For self-serve phone payments RevSpring partnered with a vendor that provides an extra measure of protection against hackers. When a patient speaks in or keys in their credit card information, the data is encrypted and passed along for authorization and processing, then deleted and never stored—which means credit card numbers are never stored on the client's network, reducing the PCI compliance scope for the client.

Conclusion

Managing the costs and headaches associated with financial data security starts with minimizing compliance gaps wherever you can. This means choosing a vendor like RevSpring that is not only PCI-compliant, but also takes extra measures to reduce your scope. We're continually keeping one step ahead of regulatory issues—so you don't have to. When you partner with RevSpring, you get the best of both worlds: the ability to provide convenient, flexible payment solutions to patients along with the peace of mind that comes with knowing their financial data is safe and secure.

RevSpring leads the market in financial communications and payment solutions that inspire patients to pay. Since 1981, the company has built the industry's most comprehensive and impactful suite of patient engagement, communications and payment solutions backed by behavior analysis, propensity-to-pay scoring, contextual messaging and user experience best practices. Using proprietary data analytics to tailor the engagement workflows to fit individual circumstances and preferences, we improve the financial experience and outcomes for providers and their patients.

Disclaimer: The contents of this resource are not intended to serve as legal or any other advice.

