Protecting Patient Payment Data:
The Implications of PCI Compliance

A white paper produced by RevSpring™

Good healthcare facilities know that today's patients like convenience, and credit cards epitomize convenience. Successful healthcare systems also recognize that patients want and need to pay with their credit cards in a multitude of ways—in person, online, over the phone. Hospitals are willing to pay a minimal percentage of the total sale to a card processor in order to keep patients happy. But with all the data breaches surrounding credit card transactions lately, how can healthcare organizations make certain that their patients' data remains secure?

The Basics of PCI Compliance

PCI compliance refers to a set of security standards, administered by the PCI SSC (Payment Card Industry Security Standards Council), designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It is important to note that PCI standards are not law, per se. Instead, these standards have been set by a partnership of the major payment brands (Visa, MasterCard, Discover, American Express, JCB) as a way to bring the whole industry up to a high security standard.

Because PCI compliance is not a law, it is not governmentally enforced. But this does not mean it can be taken lightly. In cases of PCI compliance violations, the payment brands may, at their discretion, issue fines of $5,000 to $100,000 per month to the bank that processed the payment. It is important for payment collectors to know, however, that they are not immune from penalty. Fines issued to the processing bank due to merchant security violations will likely be passed back to the merchant. Furthermore, the bank will almost certainly terminate its relationship with the merchant or significantly increase transaction fees. While it is true that these fines are not openly discussed nor widely publicized, they can be catastrophic to a business. It is important to be familiar with your merchant account agreement, which should outline your potential exposure in the event of a data breach.

In an effort to "encourage" merchants to operate with PCI-compliant practices, policies exist whereby those who do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc. if a breach event occurs.

In addition, with the 2015 EMV (Euro MasterCard Visa) liability shift, merchants of any kind who accept card-present payments are invested in a much higher share of that cost. One way or another, merchants that do not take PCI compliance seriously will be financially affected.

The Solution is Easier than You Might Expect

There is an organization that can provide clients with the necessary hardware, software, systems, and support to ensure that all manner of credit card processing adheres to PCI compliance standards. At RevSpring, we make it our business to make your business easier. We recognize that you have a health system to run and may not have the time or expertise to implement stringent security protocols. Our extensive work in the health data industry has prepared us to assess your hospital's needs, anticipate problems, and implement intelligent solutions that fit your goals, all while maintaining compliance throughout the entire system. We know that the billing cycle consists of many moving parts, and we will work with you to put in place practices that maintain an environment of data security. This can mean anything from training, to system assessment, to a top-down overhaul of your entire billing and payment process. We will work within your budget and expectations to deliver the kind of security you need.

Top-of-the-Line Technology and Tools

So how do you reduce PCI DSS scope? A quick and easy solution is to update your hardware. We have a direct relationship with our hardware manufacturer, who produces hardware on demand, as we order it, to fit our clients' specific needs. The hardware utilizes a proprietary, peer-to-peer encryption process, ensuring that our clients are able to protect card data whether entered through the swipe method, manual key entry, or EMV. We work with our manufacturer to deliver hardware that is easy to use and is preset to function according to PCI-compliant practices.

Many hospitals may not realize that the need for PCI compliance reaches into all manner of payments, including payments taken over the phone. In instances of manual key entry, PCI compliance is especially important, as human error becomes a significant factor. Our experience has shown us that human error is usually the most likely cause of data security issues. We also know that proper instruction is the first line of defense against such potentially costly mistakes. Consequently, clients who implement our hardware and software not only receive the latest, most secure hardware systems, but also the necessary instruction, explanation, and training to make those systems work at their best. In short, we will not only install your new hardware, but will help your employees learn to operate the new technology according to PCI-compliant methods.

Security Measures Go Well Beyond Payment Initiation

We have received the coveted Point-to-Point Solution certificate, which means our applications, software, and underlying systems have been audited and certified from point-to-point as a secure payment solution. This is not a small feat—a quick glance at the PCI Council website shows that many other data processors have not achieved this notable recognition.

Making separate systems work effectively can be difficult. That's why we build all of our billing and payment processes around a central platform. This serves a variety of purposes. Patients love the ease of the payment process. Employees love the standard design layout and simplified functionality. Administrators appreciate that everything works together and reports can be generated via such an integrated system. In short, we've made the entire payment collection process easier and safer for all those involved: patients, customers, and staff.

Integrity and Diligence Guaranteed

RevSpring has built its reputation on providing top-of-the-line payment and billing solutions for healthcare systems. We model integrity not only in the way we protect our clients' data, but also in the way we do business. Our clients tend to agree—to date, we've implemented over 2,500 payment portals and processed over 12 million payments, valued above $2.2 billion. Each payment is conducted on systems which are independently validated and confirmed compliant with:

- PCI DSS v3.1
- PCI P2PE Application
- HiTrust
- SSAE 16, SOC 2 Type II
- HIPAA/HiTech

Compliance issues are too important to leave to chance. If you are worried about these, or other compliance problems, give RevSpring a call. We'll be happy to talk you through the process and determine if our payment hardware and payment systems would be right for your organization.

RevSpring

Intelligence. Engagement. Outcomes.™

RevSpring is a leader in patient communication and payment systems that tailor engagement touch points to maximize revenue opportunities in acute and ambulatory settings. Since 1981, RevSpring has built the industry's most comprehensive and impactful suite of patient engagement, communications and payment pathways backed by behavior analysis, propensity-to-pay scoring, intelligent design and user experience best practices.

RevSpring leverages "Best in KLAS" software and services to deliver over 1 billion smart medical communications each year that drive increased patient engagement and payment rates.

www.revspringinc.com • (248) 567-7300 • learnmore@revspringinc.com

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