ePAY Healthcare

ELIMINATING RISK

DELIVERING PEACE OF MIND

Of all data breaches in the United States, healthcare entities accounted for a high percentage of incidents, more than one-third of all data breaches in the country

Adherence to PCI DSS (Payment Card Industry Data Security Standards) protects patient financial data and provides peace of mind.

# Eliminating Risk in Healthcare Payments

## *Outsourcing delivers security and peace of mind*

**Beyond HIPAA** The new age of financial data protection

Personal data protection, including the safeguarding of payment information, is a rapidly growing threat faced by all businesses, whether web-based or brick and mortar. The facts are shocking.

Data theft began with breaches in the credit card industry, costing financial organizations literally billions of dollars over the past decade and striking fear into the hearts of the American public, as identity theft became a very real problem. In fact, credit and debit card fraud was reported as the number one fear of Americans in the midst of the global financial crisis, superseding that of terrorism, computer and health viruses and personal safety. (Source: Unisys Security Index)

What started in the financial services sector rapidly expanded to other industries. Recent high profile data breaches, human error and cyber security incidents have shown that business, industry and government agencies are all at risk.

Healthcare is not immune to security breaches, and some believe the industry is a growing target.

⌘ *According to the U.S. Department of Health & Human Services, since September 2009 to present, 17,000 patient records are breached per day, on average.*

In a recent study published in “Healthcare Finance News” on Feb 4, 2014, if you have 1,000 patients in your system whom you have served over the course of time, it will cost approximately $200,000 to recover from this security breach event if your system is compromised in any way- for example by a hacker or even accidental loss of information by an internal employee.

*“The average cost of a class-action lawsuit is staggering – Patients who’ve had their health records compromised often band together to seek damages. A study by Temple University’s Beasley*

*School of Law found that the average settlement award in data breach class-action suits is $2,500 per plaintiff, with average attorney fees of $1.2 million. Sometimes the potential costs are even higher, as in the $1 billion lawsuit filed in 2011 against Sutter Health*.” (Source: Healthcare Finance News, February 4, 2014)

While the security breach expenses are staggering, there are other costs not so easily quantified that can cripple an organization’s growth and sustainability. Few incidents can damage a company’s reputation and compromise trust more than the breach or loss of personal data. These events not only impact a company’s customers but also open the door for increased scrutiny from regulators, privacy advocates and the media. The costs are simply too high to ignore.

“*The costs associated with a major data breach include both the obvious (legal/regulatory penalties, remediation, lawsuits) and the unforeseen (such as major disruptions to clinical and operational performance or lost business due to reputational damage). The total tab can easily run into the millions.*”

11.1 million
adults were victims of identity theft

Total fraud amount was
$54 billion

The average victim spent 21 hours and $373 out of pocket resolving the crime

Javelin Strategy and Research

“*A data breach involving more than 500 patient records requires HHS/media notification – when news reporters get wind of a data breach, an organization’s reputation can take an immediate hit. For example, when one of the nation’s leading healthcare providers recently notified the media of a data breach, a competitor ran a full-page ad the next day touting its own data security success*.” (Source: Avoiding Target-style notoriety, Healthcare Finance News, February 4, 2014)

Healthcare risks and threats posed by data breaches and theft are growing. Thieves and hackers are targeting industries that are easier to infiltrate by assessing the degree of security technologies and comprehensive security measures being used. Traditionally credit card companies have been most aggressive in combating the issue as they seemingly have the most to lose. Organizations large and small are at risk. While the media covers only the largest incidents, statistics prove that businesses in every industry are vulnerable.

Of all data breaches in the United States, healthcare entities accounted for a high percentage of incidents, more than one-third of all data breaches in the country. According to a 2012 HITRUST analysis, hospitals and physician practices were responsible for 32% and 28% of the total breaches in healthcare, respectively.

## Financial data regulations?

The healthcare industry is well versed in protecting patients' medical data. HIPAA laws clearly protect patients' medical records and health information. They are taken seriously and carefully adhered to by all reputable members of the medical community.

But what about protecting patient financial data? Some healthcare providers do not fully understand the threats and, as a result, may perceive it is sufficient to store patient financial data in a locked filing cabinet. While this practice already provides significant security exposure, the risk of compromising the patient's data is now further amplified through the extension of online patient portals. These additional patient services delivering online patient information and payment processing capabilities further exacerbates the provider's security planning and management complexities, as the online services add to the security workload and costs, as well as require an entirely different approach to protect against breaches related to technical vulnerabilities.

Protecting the patient's financial data requires a comprehensive approach — whether payment processing is internal or outsourced— the healthcare facility needs to ensure that practices and policies are in place to protect themselves and their patients' sensitive data. These efforts can range from:

- **Electronic** security, including data encryption techniques and access control measures
- **Technology** defenses such as secure firewall implementation and various proactive monitoring processes and systems
- **Physical** protections, including surveillance, access, and control facility design
- **Planning** measures for documentation, procedures, and long-term planning
- **Verification** safeguards such as industry compliance certifications and continuous testing, scanning, and monitoring

The amount of workload and investment to establish this type of safe and comprehensive security depends on the preferred approach of the healthcare provider. For example, facilities that develop 'in-house' patient payment services and solutions will require more initial and ongoing resources and financial investment for security planning, development, and management.

Alternatively, facilities that outsource their payment processing solutions can take advantage of significantly lower cost hosted solutions that spread the operating and security costs across hundreds and thousands of customers. Outsourced solutions are often preferred as they present lower cost alternatives that do not require development efforts and only require management oversight to administer. Furthermore, outsourced companies focused on a particular solution typically have an established core competence. When it comes to a critical aspect of your operation, such as security, where any failures can have a substantial negative impact on service and expenses, this expertise allows you to minimize your risk.

## PCI certification—the highest level of protection

PCI DSS (Payment Card Industry Data Security Standards) certification is an example of the security costs that can be minimized with an outsourced solution. This certification process is an expensive and time-consuming requirement to establishing and maintaining a high level of security

when processing payments. However, it is a critical component of payment processing and necessary for either ‘in-house’ applications or in contracts with outsourced partners.

In 2006, in an effort to combat fraud and improve the security of financial information, the credit card industry established stringent standards known as PCI DSS. This multifaceted security standard includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to help organizations proactively protect customer account data. The standard is now well known, widely adopted and provides wide-ranging benefits for organizations and their customers.

### ePAY Healthcare – a secure option to protect all patient payments

ePAY Healthcare holds the highest PCI DSS Level 1 certification. This is a vital aspect of an ongoing commitment to customers who trust us to securely facilitate payments for their healthcare facilities while providing complete protection of their patients’ data. A comprehensive annual PCI certification audit includes document collection and analysis, vulnerability scanning and penetration testing, as well as regularly recurring scans throughout the year.

In security terms, this means that ePAY is ensuring that your payment processes adhere to PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. Operationally, ePAY Healthcare plays a vital role in ensuring that patient payment card data is kept safe throughout every transaction—and that both providers and their patients have the utmost confidence against the pain and cost of data breaches.

ePAY Healthcare employs the mandated primary control objectives and performs monthly activities that are part of PCI compliance.

*ePAY Healthcare’s PCI DSS control policies:*

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Monitor and test networks regularly
- Maintain an information security policy

### ePAY Healthcare also offers enhanced patient services and cost savings

Outsourced payment options provide an ideal way to eliminate risk while providing a range of benefits to healthcare providers and their patients. With ePAY Healthcare, easy and secure online payment options provide patients with maximum clarity and convenience. The patients' ability to plan their financial obligations, securely access their balances and process payments, and view less confusing statements and track payments is critical to meeting their financial obligations and protecting their personal information.

For the healthcare facility, online service options can isolate and protect sensitive payment information using advanced security technologies that remove the manual, human, and process vulnerabilities. Additionally, self-payment options facilitate faster payments, increase cash flow, streamline billing and payment functions, and decrease workload, freeing up staff time to deliver care, not chase payments or manage the security process.

All sensitive banking and credit card information is securely transferred, encrypted, and stored in ePAY Healthcare's state-of-the-art, PCI-certified, data center.

### Step forward and protect your organization

Whether in a business environment or in daily life—on paper, over the phone or online—we all divulge personal data, including financial information. Doing so today comes with greater risks. When personal financial information is requested, most of us carefully consider the risks inherent in passing on this information. We all share this sensitivity.

For healthcare organizations, calming customer fears is only one reason to take preventive security measures. There are also very real risks and reasons for taking steps to protect financial data. Healthcare needs to actively plan for security, as every organization's responsibility for data is quickly being redefined and the need for security measures rise. ePAY Healthcare has been integrating comprehensive payment processing solutions with various financial and enterprise systems for more than 30 years. Protect your patients; protect yourself. It's just good business.