ePAY Healthcare Security Overview

ePAY Healthcare provides world-class security with extensive experience in delivering applications that are certified or comply with PCI, HIPAA, NACHA, and Service Organization Controls assessments (SAS70 replacement). With rigorous adherence to security, ePAY is able to help providers and health care facilities lower risks associated with financial transactions, improve on-site payment processing security, and dramatically reduce the cost of compliance. Our clients range in size from organizations with no full-time compliance or security staff to nationwide organizations with significant internal audit and security teams. ePAY's approach ensures that each provider has a trusted, certified, and compliant solution.

ePAY Healthcare Application Security

- ePAY adheres strictly to industry standards to protect Customers' data.
- ePAY uses standard, well-reviewed cryptographic protocols and message formats (such as SSL and PGP) when transferring the ePHI data used in the ePAY application such as Last name, First name, Date of Birth and demographic information such as State, City and Zip Code.
- ePAY addresses the HIPAA Privacy Rule by ensuring administrative, physical, and technical safeguards are in place.
- Credit card processing adheres to PCI Data Security Standard (PCI-DSS) Level 1 – the highest level of certification.
- ePAY utilizes tokenization in accordance with PCI Data Security Standard (PCI DSS). With tokenization, the solution eliminates the storage of sensitive data, adding another layer of protection beyond encryption.
- ePAY prohibits the storage of card numbers, magnetic stripe data and security codes on client devices.
- Two-factor authentication and strong password controls are required for administrative access to systems.
- Security systems and processes are tested on a regular basis by qualified internal and external teams.
- Access to secure services and data is strictly logged, and audit logs are reviewed regularly.
- Security policies and procedures are carefully documented and reviewed on a regular basis.
- Detailed incident response plans have been prepared to ensure proper protection of data in an emergency.

Physical and Network Security

- ePAY Healthcare's network and servers are housed in a secure datacenter which is a Service Organization Controls (SOC 3) and PCI Level 1 certified facility.
- The datacenter with SOC 3 certification provides the level of assurance related to 1) security, 2) availability, 3) processing integrity, 4) confidentiality and 5) privacy of a system and its information.
- In operational terms, it means that ePAY's technology ensures the payment data is secured throughout every step of the payment transaction. Customers can have confidence that they are protected from having to endure the time consuming and costly implications of a data breach.

Compliance and Certifications

- ePAY Healthcare, classified as a "Level 1 Service Provider," maintains full compliance with the Payment Card Industry Data Security Standard (PCI DSS).
- In security terms, it means that that we are meeting our requirements to ensure a customer's payment process adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.