HealthManagement
Promoting Management and Leadership

# Safeguarding Payment Information: Essential Security Measures in Healthcare


In today's digital age, protecting payment information in healthcare has become increasingly critical. Patients are more concerned than ever about the safety of their financial data, with 95% expressing worries about data breaches affecting their medical and payment information. This apprehension extends to the involvement of Big Tech companies, with 65% of patients distrusting these entities with their health data, and 54% uneasy about the security measures implemented by vendors managing their payment information. The need for robust security protocols is evident as cyber threats become more sophisticated and frequent.

### Enhancing PCI Compliance in Healthcare

One of the fundamental steps healthcare providers can take to secure payment information is adhering to the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS provides a comprehensive framework for securing credit card transactions. This involves rigorous measures such as encrypting payment data, maintaining secure networks, implementing strong access control measures, and regularly monitoring and testing networks. These protocols are crucial in protecting against data breaches, which can be particularly costly in healthcare, where the average breach costs have soared to 12 million Euros. Ensuring PCI compliance not only safeguards sensitive payment information but also helps healthcare providers avoid significant fines and maintain trust with their patients.

### The Role of Payment Tokenization and vP2PE

Beyond PCI DSS compliance, healthcare providers can adopt advanced technologies like payment tokenisation and validated point-to-point encryption (vP2PE) to further secure payment data. Payment tokenisation is a process where sensitive payment information, such as the Primary Account Number (PAN), is replaced with a unique, randomly generated token. This tokenisation means that even if the data is intercepted, it cannot be used by cybercriminals, as the tokens hold no intrinsic value and cannot be reverse-engineered to retrieve the original data. This technology is particularly beneficial in preventing fraud and unauthorised access to payment information.

Validated point-to-point encryption (vP2PE) enhances security by encrypting payment data at the point of interaction—such as when a patient enters their payment details—through to the payment processor. This encryption process ensures that the data remains secure throughout its transmission, preventing unauthorised access during the transaction. The PCI Security Standards Council's P2PE standard requires rigorous testing and validation, ensuring that the encryption methods used are up to the highest security standards.

### A Secure Future for Patient Payment Information

As cyber threats continue to evolve, healthcare providers must prioritise the security of patient payment information. Providers can protect sensitive financial data from breaches and cyberattacks by implementing PCI DSS compliance, payment tokenisation, and vP2PE. These technologies safeguard patient data and enhance patients' trust and confidence in their healthcare providers. In an environment where data security concerns are paramount, adopting these advanced measures is essential for protecting patient information and ensuring the integrity of healthcare services.

**Source:** HealthcareITtoday
**Image Credit:** iStock

Published on : Wed, 24 Jul 2024