DrChrono Payments: Stripe PCI Compliance

Last modified on 09/18/2024 2:06 pm EDT

We take securing patient information, including credit card numbers very seriously. As such, we secure patient financial information according to PCI DSS, or the Payment Card Industry Data Security Standard. The standards are mandated by card brands such as Mastercard and Visa, but administered by the Payment Card Industry Security Standards Council.

Stringent controls regarding the storing of financial information are regularly audited to ensure compliance with stated regulations. There are 12 requirements for creating and maintaining a secure network that safeguards sensitive financial information.

Some of the controls include:

- Maintaining a firewall that scans all network traffic and blocks untrusted networks from accessing the system.
- Protecting stored cardholder data with encryption, hashing, masking, and truncation strategies.
- Performing regular updates of anti-virus software.
- Restricting access to financial data to only authorized personnel who have a business need to access the information.
- Tracking and monitoring all access to cardholder data.
- Regular testing of security systems and processes to identify any new vulnerabilities so they can be addressed.
- Maintaining a strong information security policy for all personnel to understand the sensitivity of the stored information and their responsibility to protect it.

If you have any questions regarding PCI Compliance, please reach out to 844-202-8515.