Nextech

Payments Security

Healthcare breaches cost $9.23 million per incident—a $2 million increase over the previous year.*

So how do you make sure to keep your patients' payment data secure?

SECURITY-FIRST DESIGN

Store all payment information securely, with a trusted partner who incorporates a "security-first" design into their software design versus separate pieces of software across multiple organizations. This reduces both the number of places that store your customer information as well as the associated risk, thereby minimizing the number of opportunities for that customer information to be compromised.

SECURELY STORED ON FILE

Offer the ability to take payments in a variety of ways by having the cards securely stored on file as a token and automatically processed per certain criteria:

- **Recurring** – Securely save the card on file for ongoing payments
- **Payment plans** – Securely save the card on file for installment plans that have a finite end date
- **Automatic Billing** – Set up the ability to automatically bill for a predetermined sequence (daily, weekly, monthly, yearly)

ELIMINATE PAPER

Eliminate the need to keep patients' credit card numbers on a physical piece of paper and potentially accessible to others

For more information or to schedule a demo, contact us at www.nextech.com or (866) 857-8557.

*IBM Report: Cost of a Data Breach Hits Record High During Pandemic – July 28, 2021

HOW DO WE DO THIS?

Contact EMV Card Processing

Utilizes industry-standard chip technology when inserted into the card reader.

Contactless EMV Card Processing

Allows you to wave your card or Apple Pay/Samsung Pay/Google Pay over the terminal to process your payment, leveraging payment-card-industry-compliant payment terminals and card readers.

Practice Management Integration

Provides another layer of access, protecting transaction information through user sign on and permission within the PM software, attaching the user ID of the person who initiated the transaction to each payment processed for audit purposes.

Transaction Monitoring

Watches for irregularities that could be signs of fraud on your merchant account.

Card Data Encryption and Tokenization

Card data is encrypted in the payment terminals and readers before being sent for processing, with the response returning a token representing the card number for storage. The encrypted message cannot be decrypted without the decryption key stored securely with our processor, and the token cannot be used to initiate a payment at any other merchant other than the one that processed the original payment.

Nextech + stripe

WHY PARTNERING WITH STRIPE WAS THE RIGHT SOLUTION

Stripe Inc. was audited by a PCI-compliant auditor, has PCI DSS Service Provider Level 1 certification (assessed by Securisea, Inc.) and is validated to PCI-PIN (assessed by K3DES, LLC).

Stripe maintains the following PCI certifications for Terminal:

- PCI DSS for Stripe's payment infrastructure
- PCI PTS for the hardware (Verifone P400)
- PCI PA-DSS for the Stripe Terminal Client
- EMV Level 1 and 2 for the reader's firmware

For more information or to schedule a demo, contact us at www.nextech.com or (866) 857-8557.