Sutter Health GENESYS semafone
securing data · protecting reputations

Case study: Sutter Physician Services and Semafone

The Contact Center Cure: How Sutter Physician Services Improved Customer Care, Simplified PCI DSS Compliance & Strengthened Data Security

Background

Sutter Physician Services (SPS) is an affiliate of Sutter Health (now part of Sutter Shared Services, a division of Sutter Health), one of California's most comprehensive healthcare systems serving more than 3 million people in 100 Northern California cities and towns.

An industry leader in providing revenue cycle, patient access, and accountable care solutions to healthcare providers and payer organizations, SPS is passionate about improving the patient experience and contributing to happier, healthier lives.

Challenge

With contact centers located in Sacramento, California, and Salt Lake City, Utah, SPS was using an automated interactive voice response (IVR) system to take payments from patients over the phone. Payments are obtained either through inbound calls (a patient calls to pay for medical services or a doctor's visit) or outbound calls (a patient service representative (PSR) calls a patient to collect advance payments for procedures).

The solution was proving inefficient; it was often difficult deciphering the various dialects and accents of patients across diverse regions. The frustration caused by misheard or mis-keyed card numbers led to premature hang-ups and abandoned calls. SPS saw the opportunity to streamline the process providing a better, more personalized patient experience. This was especially important for servicing ill or recovering patients who do not want the hassle of inefficient processes.

For an interim solution, SPS introduced point of sale (POS) systems to PSRs' workstations. As patients read their credit or debit card numbers aloud, PSRs manually typed them into the POS device. Yet, the company still had numerous elements in scope for compliance with the Payment Card Industry Data Security Standard (PCI DSS), including the verbalized cardholder data (CHD) and the PSRs themselves.

To add to the compliance challenge, all calls are recorded. Because the PCI DSS prohibits the recording of sensitive authentication data (SAD) such as CVVs, PSRs had to manually pause the recording when credit card information was read out loud. While their software automatically resumed the recording once the data was captured, SPS did not want to take any risks – a PSR could forget to pause the recording and accidentally log sensitive data.

SPS sought a solution that would descope its entire contact center environment from the PCI DSS, remove the burden from agents for securely capturing payment information, and enable patients to take control of entering their card details which would result in a better patient experience.

The Solution

Already using the **Genesys Customer Experience platform**, SPS didn't have to look any further than Genesys' certified partner, Semafone, for a solution. Based in the U.K. with a fast-growing North American client base, Semafone provides data security and compliance solutions to enterprise contact centers around the world. SPS selected Semafone's award-winning, flagship product, **Cardprotect**, which enables callers to directly enter their payment card details through their telephone keypad.

Using dual-tone multi-frequency (DTMF) masking technology, Cardprotect shields card numbers from agents, call recording systems and even nearby eavesdroppers by replacing the keypad tones with flat tones. Card details are sent directly to the company's payment processor, never touching the contact center's IT infrastructure – thus descoping it from the PCI DSS. Meanwhile, agents can remain on the line with the caller in full voice communication, answering any questions, handling wrap-up tasks, ensuring a smooth customer journey and improved customer service.

Implementation

Semafone led a complex implementation with multiple vendors and technology integrations. This included a customized integration of Cardprotect with Genesys' solution and a third-party payment processing system. Together, the three solutions operate without a hitch: using the Genesys platform to control the call, agents select a "Secure Mode" button to screen pop Cardprotect into the payment processing system. The caller securely enters his or her payment card numbers into their keypad, which is sent directly to the third-party system for processing. Once the transaction is complete, the next call comes in and the process starts all over again.

"Semafone worked closely with our internal team and Genesys to quickly deploy a solution in a relatively short period of time," said Alicia Gee, Director, Unified Communications at SPS. "Their team was engaged and committed throughout the process, despite working across several different time zones. Plus, our PSRs found the solution easy-to-use and intuitive, making for an even simpler go-live."

Results

Today, SPS is using Cardprotect to securely collect payments in two contact centers with nearly 500 PSRs. The organization has experienced impressive results – they successfully de-scoped much of the contact center environment from PCI DSS compliance, and payment card data no longer touches or is exposed to agents, desktop applications or call recordings. With Semafone, SPS is avoiding hundreds of thousands of dollars in noncompliance fees and is meeting the requirements of the PCIDSS v 3.2.

Patients still have the capability to use an IVR if they prefer and that too is descoped from PCIDSS, as Cardprotect relays the entered card data directly to the payment processor. Infact, SPS was able to easily introduce a second IVR to accommodate higher call volumes, without sacrificing customer satisfaction.

Most importantly, SPS enhanced its ability to provide the best-possible patient care and customer experience through the combination of Semafone and Genesys' solutions. Callers have the option of speaking with a live agent or using an IVR – both of which provide a secure payment transaction.

According to SPS, the feedback from both patients and PSRs has been overwhelmingly positive regarding privacy and security, as card numbers are no longer verbalized. SPS and its patients have the peace of mind that their sensitive data is protected. Additionally, 96 percent of PSRs in a post-deployment survey said that Cardprotect was easy to use.

"Semafone enabled us to balance the best of both worlds – we are securing our data and simplifying compliance, while improving the patient experience," said Gee. "Our patients understand that their information is secure and enjoy the ease-of-use of Cardprotect. Our SPS team is delighted with the project results."

Alicia Gee – Director, Unified Communications at SPS

Results Overview:

- **Descoped much of its contact center environment from the PCI DSS, reducing risks and avoiding noncompliance penalties**
- **Improved the customer experience and patient care**
- **Strengthened overall data security and simplified PCI DSS compliance**