Sycurio.

Curing your contact center data security epidemic.

Six prescriptions for the healthcare industry

Contents.

There is a crisis in the healthcare industry, and it involves neither illness nor injury.

From hospitals to insurance networks, pharmacy chains to collections agencies, organizations operating in the healthcare industry handle, process and store vast amounts of sensitive personal data. This Protected Health Information (PHI) includes medical histories, lab results and vital signs, as well as addresses, social security numbers, birth dates, billing and payment card data, and other personally identifiable information (PII). It is no wonder the healthcare industry has become a favorite target for hackers, fraudsters and cybercriminals. In fact, healthcare data breaches are reported at a rate of more than **one per day** in the United States, with 45 million individuals affected by **healthcare attacks in 2021** alone.

Further, complete medical records sell for as much as **$1,000** a piece on the Dark Web, jeopardizing patient safety and privacy and putting them at risk for life-altering identity theft. If the modern Hippocratic Oath states, "I will respect the privacy of my patients," shouldn't that extend to include the privacy and security of their sensitive, personal data? Shouldn't healthcare professionals care for their patients' data, just as they would their health and well-being?

While strides have been made in regulating data privacy and security, with legislation like the Health Insurance Portability and Accountability Act (HIPAA), the EU's General Data Protection Regulation (GDPR) and of course, the Payment Card Industry Data Security Standard (PCI DSS), the healthcare sector has its work cut out for it. Just one high-profile breach can compromise patient trust and safety, while tarnishing an organization's brand reputation forever.

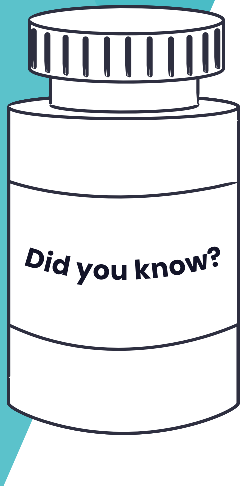
According to IBM and the Ponemon Institute, **healthcare data breaches** are the most expensive by industry with a $2M increase from the previous year—now averaging $9.23M per incident.

Is there a cure framework in the contact center?

There's no cure-all treatment for healthcare data security (just yet, at least). However, there is one area of the business that makes a great starting point: the call and contact center.

When a customer or patient needs to make an appointment, check test results or pay a bill, the contact center is often the first point of interaction. In fact, our 2021 State of Healthcare Payment Experience and Security Survey uncovered that many of today's consumers have changed the way they pay medical expenses and bills, transitioning away from in-person (28% decrease) and mail payments (17% decrease) to alternatives like mobile apps (23% increase) and phone (8% increase).

Having solutions in place that support payment compliance regulations, like the Payment Card Industry Data Security Standard (PCI DSS), in accordance with privacy measures put in place to protect other sensitive data, is imperative to implementing secure frameworks—especially for the contact center's infrastructure that are prime for hackers and fraudsters.



Did you know that **70 percent** of contact center agents **still require customers to read their payment card numbers aloud?**

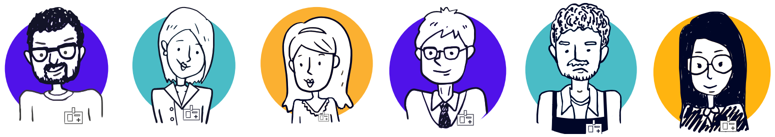
Is your contact center at risk?

Many healthcare organizations have been slow updating outdated technology; making their contact centers even more vulnerable, as legacy systems and non-segmented (or "flat") networks are prime breeding grounds for devastating cyberattacks. By breaching a single system in the contact center (such as a call recording database or CRM system), a cybercriminal can swiftly move from one area of the network infrastructure to the next, jeopardizing the entire organization and putting patient data at risk.

But not all healthcare breaches are a result of outside hackers and other external threats – 58 percent are caused by people *inside* the company. This includes patient service representatives (PSRs), agents, doctors and nurses, and even third-party partners like IT support teams and cleaning crews who work in the contact center. In other words, anyone who has access to PII is a threat, whether they maliciously access information, or accidentally expose patient data (for example, by clicking on a link in a phishing email containing a virus).

Who's threatening your patients' data?

Meet six fraudsters who may be putting your contact center at risk



SSM Health, a St. Louis-based healthcare system, revealed that a customer service representative previously employed in their contact center accessed the records of **29,000 patients** who were prescribed a controlled substance. Although SSM Health did not specify which "illegal activities" this individual performed, this incident showcases the dangers that come with easily accessible patient data.

Prescriptions for curing your contact center's data security epidemic.

The good news is that healthcare contact centers are beginning to take data security and privacy more seriously and are increasingly adopting best practices and strategies for securing PII. As with any medical treatment plan, you need to find the right combination of remedies that address your contact center's cybersecurity and compliance challenges.

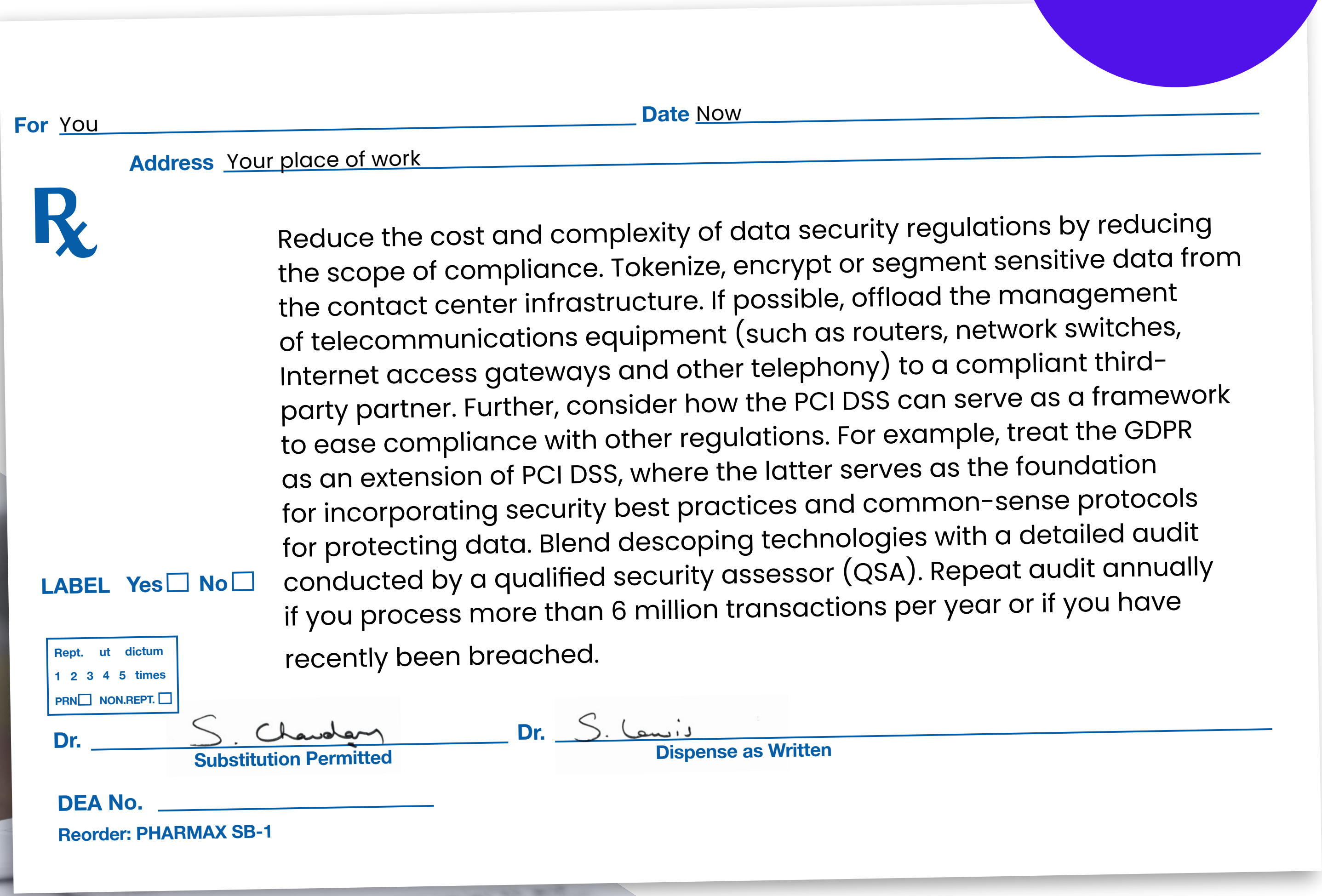
We'll help you get started by diagnosing six of the most pressing healthcare ailments in the contact center and prescribing their cures...

Ailment 1: PCI DSS Compliance is too complex and costly

Any healthcare organization that handles cardholder data must comply with the PCI DSS. For large organizations that process more than 6 million transactions a year, PCI DSS compliance can cost hundreds of thousands – if not millions – of dollars annually, while audits are an enduring nightmare.

Healthcare providers must also comply with a laundry list of data security and privacy regulations from HIPAA to GDPR and varying state laws on breach notifications. All of these various regulations and requirements can add up to a complex and costly compliance program.

The prescription



For You Date Now

Address Your place of work

℞

Reduce the cost and complexity of data security regulations by reducing the scope of compliance. Tokenize, encrypt or segment sensitive data from the contact center infrastructure. If possible, offload the management of telecommunications equipment (such as routers, network switches, Internet access gateways and other telephony) to a compliant third-party partner. Further, consider how the PCI DSS can serve as a framework to ease compliance with other regulations. For example, treat the GDPR as an extension of PCI DSS, where the latter serves as the foundation for incorporating security best practices and common-sense protocols for protecting data. Blend descoping technologies with a detailed audit conducted by a qualified security assessor (QSA). Repeat audit annually if you process more than 6 million transactions per year or if you have recently been breached.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chaudary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

DEA No. __________

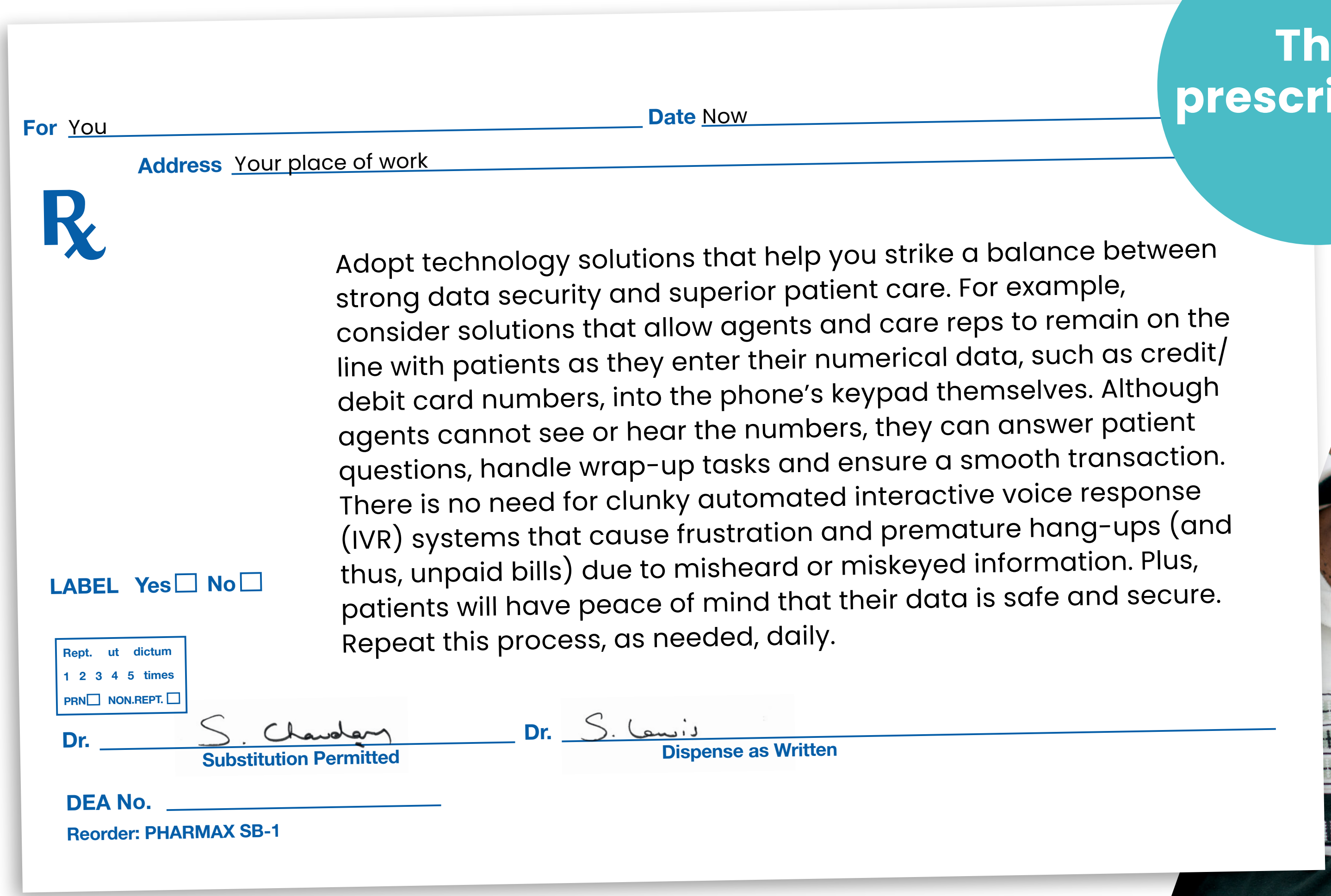
Reorder: PHARMAX SB-1

Ailment 2: It’s difficult to balance patient care with strong data security

With data breaches occurring daily and the regulatory compliance landscape changing rapidly, healthcare providers must remain hyper-focused on securing data, keeping their names out of headlines and avoiding costly noncompliance fines (HIPAA violation fines range from **$100 to $50,000** per violation or per record).

But, they can’t afford to lose sight of what matters most: the patient. While data privacy is an important element of a positive experience, your security controls and processes should not hinder the customer, patient nor member journey.

The prescription



For You Date Now

Address Your place of work

℞

Adopt technology solutions that help you strike a balance between strong data security and superior patient care. For example, consider solutions that allow agents and care reps to remain on the line with patients as they enter their numerical data, such as credit/debit card numbers, into the phone’s keypad themselves. Although agents cannot see or hear the numbers, they can answer patient questions, handle wrap-up tasks and ensure a smooth transaction. There is no need for clunky automated interactive voice response (IVR) systems that cause frustration and premature hang-ups (and thus, unpaid bills) due to misheard or miskeyed information. Plus, patients will have peace of mind that their data is safe and secure. Repeat this process, as needed, daily.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chawdary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

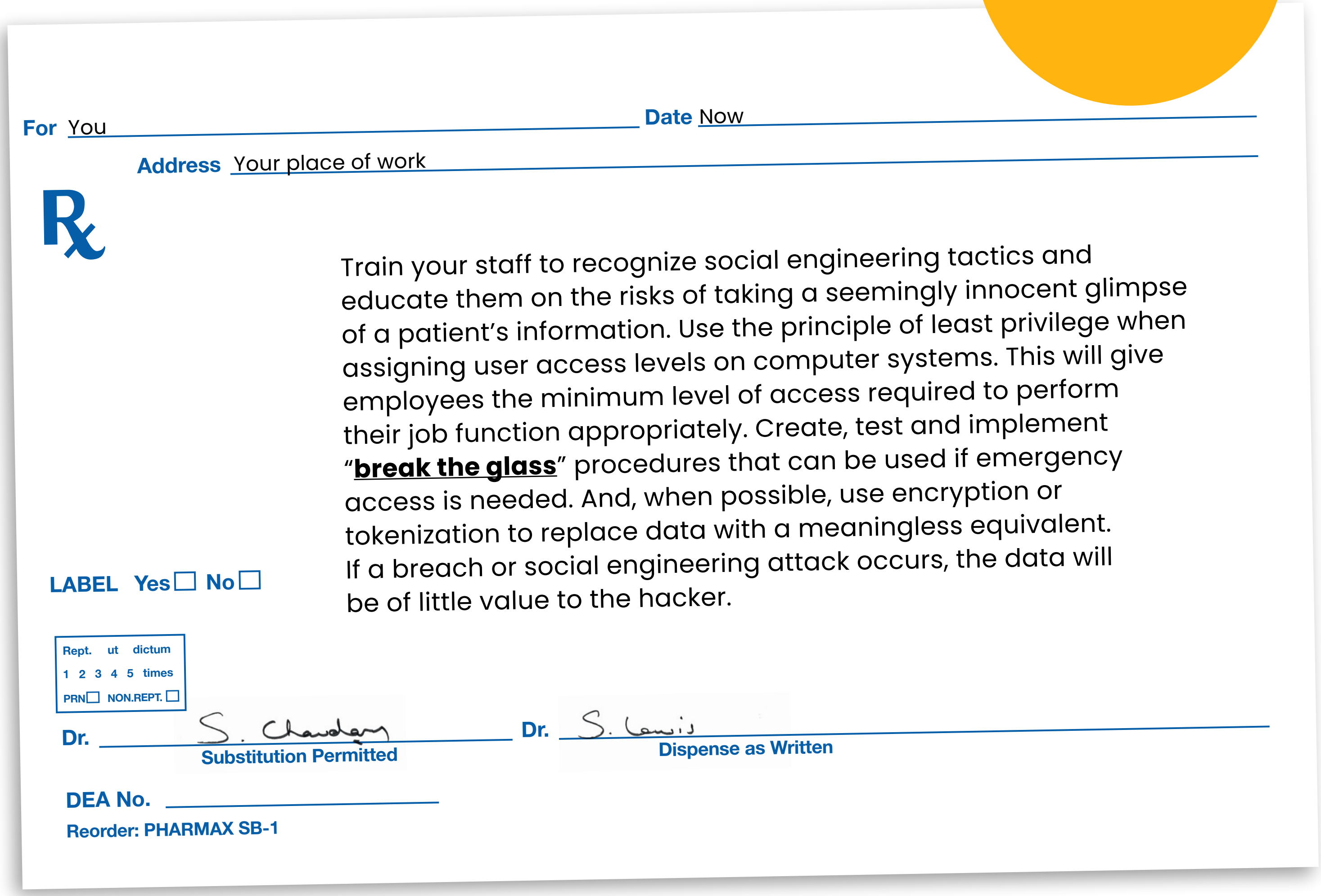
DEA No. __________

Reorder: PHARMAX SB-1

Ailment 3: Agents have too much patient data at their disposal

Although your agents, PSRs and other contact center employees may not be out to steal PII for fraudulent purposes, they might still illicitly access it – often to satisfy their curiosity. Simply viewing medical information without a legitimate reason to, violates HIPAA and can lead to legal action and fines. Indeed, over-access to information is a critical issue for the contact center and creates a slippery slope. Even an honest and well-meaning agent can fall victim to a phishing email or a sophisticated social engineering scam where a fraudster poses as the patient to get their hands on sensitive data – and there is no telling how much information the service rep may accidentally disclose.

The prescription



For You Date Now

Address Your place of work

℞

Train your staff to recognize social engineering tactics and educate them on the risks of taking a seemingly innocent glimpse of a patient's information. Use the principle of least privilege when assigning user access levels on computer systems. This will give employees the minimum level of access required to perform their job function appropriately. Create, test and implement "**break the glass**" procedures that can be used if emergency access is needed. And, when possible, use encryption or tokenization to replace data with a meaningless equivalent. If a breach or social engineering attack occurs, the data will be of little value to the hacker.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chawdary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

DEA No. ____________

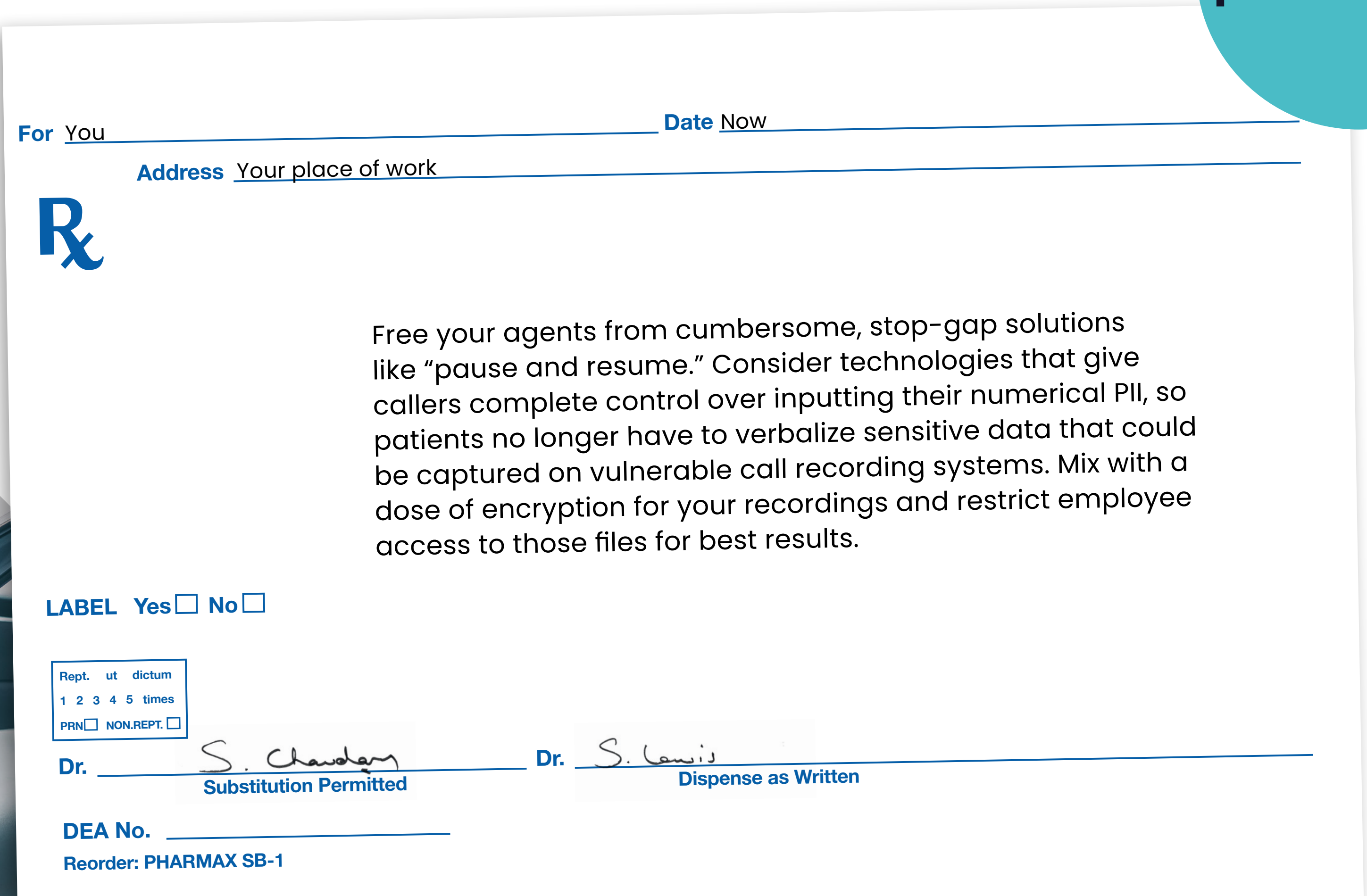
Reorder: PHARMAX SB-1

Unauthorized data access is the second most common cause of healthcare breaches, next to hacking incidents, according to **HIPPA Journal**.

Ailment 4: Patient data is captured on call recording systems

Call recording is a standard practice in healthcare contact centers, as it helps with quality control, provides an audit trail for compliance purposes and creates a source of truth in the case of a transactional dispute. However, it also comes with a few weighty risks. Contact centers typically rely on “pause and resume” or “stop/start” systems to avoid capturing sensitive data, such as payment card numbers or on-call recordings that could be breached or illicitly accessed by company insiders. Such solutions allow agents and PSRs to manually or automatically pause when sensitive data is spoken aloud, and then resume the recording after the data is captured. But, an agent could forget to pause the recording and accidentally log PHI, or fail to resume the recording, accidentally leaving out important information for an audit. Further, if sensitive authentication data (SAD) like CVVs from payment cards are captured on the recording, the contact center is in violation of the PCI DSS – for which the noncompliance fines can hover around **$50,000 monthly**.

The prescription



For You

Date Now

Address Your place of work

℞

Free your agents from cumbersome, stop-gap solutions like “pause and resume.” Consider technologies that give callers complete control over inputting their numerical PII, so patients no longer have to verbalize sensitive data that could be captured on vulnerable call recording systems. Mix with a dose of encryption for your recordings and restrict employee access to those files for best results.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chaudary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

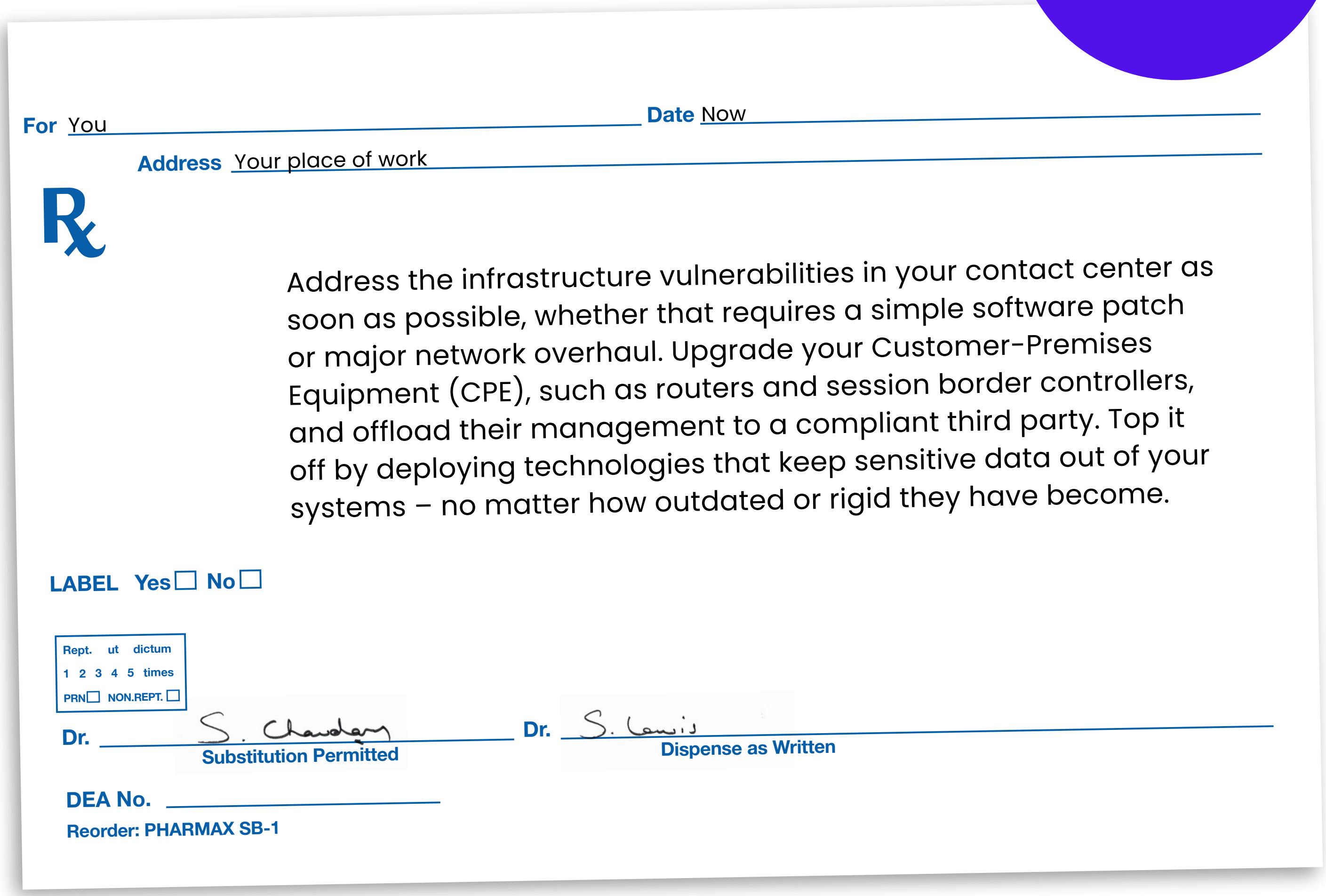
DEA No.

Reorder: PHARMAX SB-1

Ailment 5: The company relies on legacy, non-interoperable systems

The digitization of healthcare is changing the face of fraud. With patient portals, electronic health records (EHRs) and virtual clinics, a wealth of PII is available, especially in the contact center. However, many IT systems (software and hardware alike) are outdated and vulnerable to breaches. Legacy systems (such as CRMs and old telephony) can become easy entry points for cybercriminals in the contact center. Once in one system, hackers can move to another and eventually take hold of the entire organization's network. For example, the Accellion attack experienced far-reaching implications for healthcare, where the sector had the largest number of victims like Centene Corporation, a managed care solutions provider. In total, over **3.51 million** individuals were impacted as a result of legacy technology and improper security patch fixes.

The prescription



For You

Date Now

Address Your place of work

℞

Address the infrastructure vulnerabilities in your contact center as soon as possible, whether that requires a simple software patch or major network overhaul. Upgrade your Customer-Premises Equipment (CPE), such as routers and session border controllers, and offload their management to a compliant third party. Top it off by deploying technologies that keep sensitive data out of your systems – no matter how outdated or rigid they have become.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chaudary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

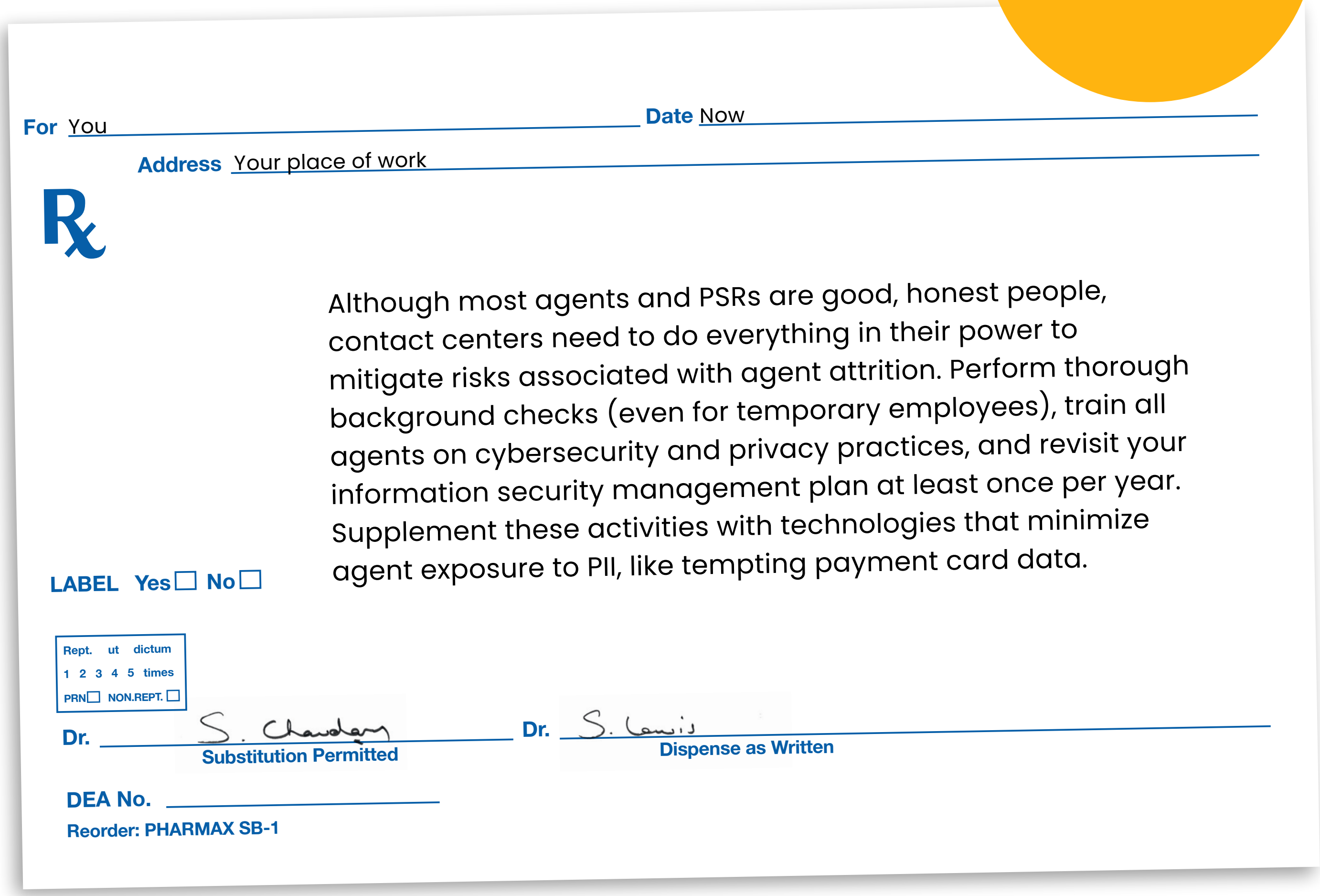
DEA No. __________

Reorder: PHARMAX SB-1

Ailment 6: The agent population is too cyclical

By its very nature, the healthcare industry employs a cyclical population of agents. Whether agents, PSRs and care reps are temporary, seasonal or outsourced, the industry requires ample staff to accommodate high call volumes, such as open enrollment periods and flu seasons. At the same time, the healthcare sector has the fourth-highest agent attrition rate (**28 percent**) of any sector. With a combination of temporary, seasonal and permanent agents moving in and out of the contact center, it is challenging to ensure sensitive data doesn't fall into the wrong hands. With little loyalty to the organization, a temporary agent could maliciously access and steal patient information, or a newly hired PSR – unaware of important data security standards and company policies – could expose PII.

The prescription



For You Date Now

Address Your place of work

℞

Although most agents and PSRs are good, honest people, contact centers need to do everything in their power to mitigate risks associated with agent attrition. Perform thorough background checks (even for temporary employees), train all agents on cybersecurity and privacy practices, and revisit your information security management plan at least once per year. Supplement these activities with technologies that minimize agent exposure to PII, like tempting payment card data.

LABEL Yes □ No □

Rept. ut dictum
1 2 3 4 5 times
PRN □ NON.REPT. □

Dr. S. Chaudary
Substitution Permitted

Dr. S. Lewis
Dispense as Written

DEA No. ______________

Reorder: PHARMAX SB-1

The contact center cure

Find out how Sycurio helped Sutter Physician Services (SPS) – an affiliate of one of California's most comprehensive healthcare systems serving 3 million people – improved customer care, simplified PCI DSS compliance and strengthened data security in its contact centers: **See case study.**

Doctor’s orders:

Descope the contact center with DTMF masking solutions

While every organization requires a personalized treatment plan consisting of a unique blend of security controls for people, processes and technologies, descoping solutions are emerging as viable “cures” for contact centers in the healthcare industry and beyond. One of the most impactful descoping technologies we’ve prescribed involves Dual-Tone Multi-Frequency (DTMF) masking. Such solutions make it dramatically easier for contact centers to comply with the PCI DSS and other complex regulations by keeping sensitive data, like payment card information or numerical patient data, out of the contact center infrastructure in the first place.

How DTMF masking technology works.

1

Callers enter numerical details (i.e., payment card numbers, birth dates, account or social security numbers) directly into their telephone's keypad.

2

The keypad (DTMF) tones are replaced with flat tones, so they are indecipherable to the agent on the line as well as to call recording systems and even potential eavesdroppers with fraudulent intentions.

3

The data is automatically encrypted and sent directly to the appropriate third party, such as a payment processor. In this way, it remains safely segregated from the contact center infrastructure.

4

Unlike with automated interactive voice response (IVR) systems, a live agent remains on the line with the customer or patient to answer any questions and carry out wrap-up tasks. This vastly improves the patient experience and customer journey.

5

Captured data is offloaded to a compliant intermediator, so compliance with data security and privacy regulations is much simpler and less costly.

How can DTMF masking help cure your contact center?

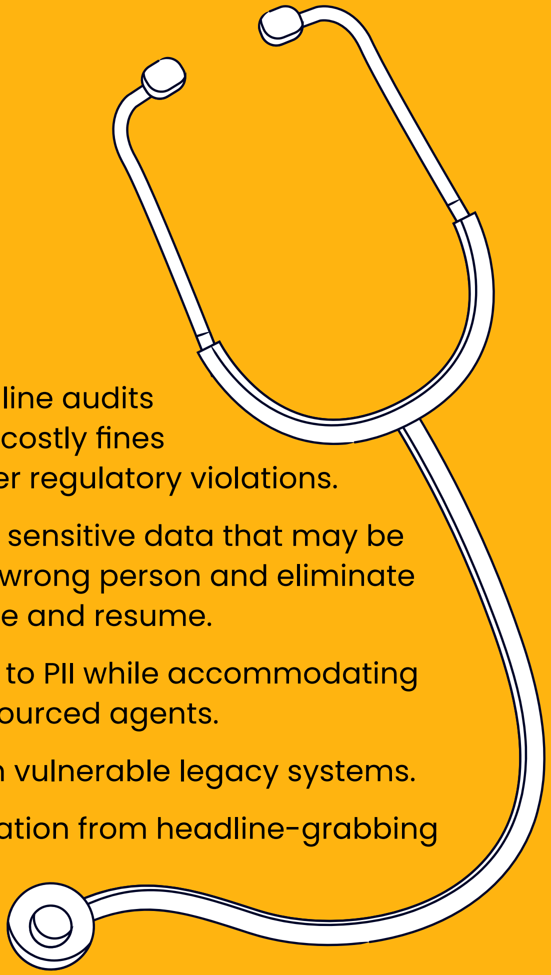
To learn more and schedule a demo of **Sycurio.Voice**, our award winning, flagship data security solution, visit: **sycurio.com**

No one is immune to a breach, but no one can hack the data you don’t hold.

No matter how many best practices you follow, controls you have in place or training you provide your staff, cybercriminals and fraudsters will still find a way to get their hands on sensitive data. The best way to make your contact center less of a target is to *treat all PII as toxic*. In other words, remove as much sensitive data from your environment as possible. Descoping technologies, like DTMF masking solutions, are a great place to start.

With these solutions, you will:

- Protect patient data without compromising on care.
- Simplify compliance, streamline audits and reduce the likelihood of costly fines from PCI DSS, HIPAA and other regulatory violations.
- Record calls without logging sensitive data that may be breached or exposed to the wrong person and eliminate stop-gap solutions like pause and resume.
- Prevent illicit or over-access to PII while accommodating temporary, seasonal or outsourced agents.
- Reduce risks associated with vulnerable legacy systems.
- Safeguard your brand reputation from headline-grabbing data breaches.



These efforts in securing your contact center will serve as a shining example for protecting data across every other part of your business. The more data you can offload, encrypt or tokenize, the less of a target you – and your patients – will be.

As we say at Sycurio...

“No one can hack the data you don’t hold!”

About Sycurio.

Sycurio is your contact center data security and compliance expert.

We work closely with enterprises around the world, including healthcare organizations and insurers, to remove sensitive data from IT and business networks – protecting your customers and your company's reputation from fraudsters and cybercriminals.

Our award-winning, patented data capture method enables organizations to securely capture personal information including payment card data, bank account details and social security numbers over the phone using Dual-Tone Multi-Frequency (DTMF) masking technology. Unlike interactive voice response (IVR) systems, agents remain in full voice communication with the caller as they enter their information into the telephone keypad, ensuring a positive customer (or patient) experience.

In addition to reducing risk and deterring fraud, Sycurio's solutions help simplify compliance with regulations like the Payment Card Industry Data Security Standard (PCI DSS) so you can focus on business as usual.

Sycurio.

nasales@sycurio.com

+1 888-267-5723