Security Industry Insights for **Healthcare**

Tools to keep your healthcare institution secure

2.1M Dollars

for an average security breach of a hospital

As more customer journeys go online, new vulnerabilities emerge, and with each new vulnerability, fraudsters look for new ways to exploit for profit and personal gain. Their attacks are increasingly sophisticated and highly coordinated.

Mobile fraud continues to rise in 2023...

Cyberattacks against the healthcare industry have risen **55%** in the last 18 months.

firecehealthcare.com

sopranodesign.com

soprano

communication unleashed

Security & Fraud Product Suite for Healthcare

IP Access Control

Allows admins to restrict access to IP addresses that are pre-approved. Login requests from any other IP address is denied, even if the login credentials are valid.

Single Sign On (SSO)

SSO integration gives organisations a centralised control system of access and reduces password fatigue for users which enhances the security.

2 Factor Authentication

2FA is the second layer of added security which a user can select to protect the account or system from attacks using stolen login credentials.

Healthcare Use Cases

IP Access Control

Most breaches are due to compromised login credentials, so adding a layer of protection with IP Access Control could be the critical security layer that protects your patients' data if any of your internal staff logins are stolen.

Hi, Sam! Remember your appointment with Dr. Smith on June 24 at 10 am. Please, CONFIRM or CANCEL it.

Single Sign On

Security measures often add friction to the day-to-day lives of healthcare staff. When password fatigue and forced password updates increase, SSO can help you anchor your login security to a single source and close unnecessary vulnerabilities.

2 Factor Authentication

2FA is a critical element of online infrastructure security and often a requirement for protecting patient data.

Security & Fraud Product Suite for Healthcare

Simple Template Messaging

Admins can define standard templates to be used across an organization which creates brand consistency and added protection against undesirable messaging due to user error.

Authenticator

Enables secure access to online services via OTPs to authorize online virtual private network (VPN) access or financial transactions to reduce fraud and improve network security.

Content Masking

This allows the message content that is stored in the database to be "masked" so that it cannot be visually seen unless one has access to view.

Healthcare Use Cases

Simple Template Messaging

Scale consistent and secure messaging with template-based messages. Admins can control the look, feel, and content allowed for outgoing campaigns.

Authenticator

Establish a OTP standard across your software ecosystem with Authenticator. Your team will benefit from fast, reliable delivery and low-friction security.

Content Masking

Relive doctors' time administering communications by masking sensitive patient data in your portal. This will allow doctors to delegate communications without putting the patient data at risk.

Your code to register is 6707 944. It expires in 5 minutes.