Security and privacy overview

Stryker clinical communication and workflow products

Introduction

Stryker's clinical communication and workflow products help improve engagement, decision-making and operational efficiency in a range of settings such as healthcare, education and retail. Our technologies enhance communication and workflow efficiency with data-driven assistive capabilities, so your focus remains on high-value tasks. Recognizing the importance of cybersecurity, this overview outlines our key principles and approach to securing data, producing quality products and helping customers achieve their security assurance goals.

Organizational commitment to cybersecurity

Vocera Communications, Inc., a Stryker company ("Stryker") endorses a security framework aligned with the organization's mission and risk profile. Cybersecurity is integrated into the corporate culture, with executive leadership empowering the cybersecurity organization to implement security measures. Collaboration across functional areas helps to ensure effective security arrangements.

Security governance

A comprehensive security framework with technical and operational safeguards has been adopted. Cross-functional collaboration and risk-based decision-making are emphasized to support effective security practices across products and environments.

The family of products overview

Our clinical communication and workflow products fit naturally or are adaptive to various settings, whether for you "right sized" means a standalone communication system or an integrated platform to transform your business. Users can engage and respond to events in their work environment using their preferred media so they can call, text, video conference and transition between media without disrupting the flow and pace of work. Our enterprise communications, analytics applications and devices unlock your path to low friction, data-driven capabilities that assist your staff in identifying and tackling priority work.

Devices

Stryker's clinical and workflow devices are wearables that enable hands-free communication and simplify workflow to help improve staff safety, enhance facility compliance and impact patient care. Devices are built for the highly mobile worker who needs to stay connected while keeping their hands free to perform their regular job duties. Support your staff’s need for secure and mobile communication with:

- Sync Badge
- Smartbadge
- Minibadge

Security highlights

Our devices utilize wireless communication and are constructed to rigorous industry security standards. Refer to the product specific documentation for details. Below are examples that apply to some of our products:

- FIPS 140-2 compliant
- Secure wireless communication protocols
- Industry-vetted encryption

Software – on premise

Our enterprise collaboration software applications solve the challenges of communicating across interoperable interfaces and message formats within an environment you control. Users experience low-friction communication and workflow management in settings that require hands-free operation and familiar channels. Our software applications include:

- Vocera Voice Server
- Vocera Engage and EMDAN
- Vocera Analytics
- Vocera Messaging Platform
- Vocera Platform

Security highlights

- Built on a secure backbone and are scalable and can integrate with various communication channels
- Adaptable to your security policies/configurations
- Over 250 integrations with clinical and operational systems, using HL7 v2.x, v3.x, FHIR, RESTful APIs, XMPP, JSON and more
- Configurable role-based access control and multifactor authentication support
- Secure wireless communication protocols
- Industry standard encryption for data at rest
- Event logging
- Configurable data management

Software as a service

Our cloud-based solutions simplify workflows with a consumer-friendly mobile experience. Accelerate your care engagement experience across your various user communities such as care teams, patients and family members. A user-driven design means your teams can work in a way that is natural to them, whether that is receiving near-real time clinical information to inform care plans, priority events that trigger a time-sensitive response or compliance notifications to maintain your operational standards. Enterprise-class secure voice, text and video communication is designed to enhance patient experience and integrate with record management systems, so data flow is controlled and efficient.

Your teams can collaborate on care plans and keep abreast of real-time events, so care decisions and actions can be executed in a timely manner. Enhance decision-making with consolidated information to help support communication workflows, reduce clinician interruptions, identify root causes of sentinel events and performance of your assistive tools. Power seamless patient experience with:

- Vocera Edge
- Vocera Ease
- Vocera Collaboration Suite

Security highlights

Security is integrated into product design, its technical infrastructure and operating model that is suitable to the risks of cloud-based services.

Authentication standards

- Solutions support multifactor and single sign-on to enforce your enterprise policy and user experience.
- The password policy is configurable to your standard.
- Applications support customer-configurable auto log users off after inactivity period and lock account after failed login attempts threshold.

Data protection

- Sensitive data is encrypted in transit and at rest throughout its lifecycle within our systems.
- Systems are scanned to detect and classify data.
- Access to sensitive data is restricted by role using technical access controls.

Data management

- Customer data is physically and or logically segregated
- Data is backed up and integrity checked daily
- Cross-border safeguards

Continuous monitoring and auditing

System activity such as access, transactions, changes and errors is recorded to support integrity checks and incident response.

Compliance assurance
*Consult product specific documentation for details

Examples that may apply to our solutions:

- HIPAA-compliant application
- HITRUST certified solutions
- CSA certified
- ISO 27001 certified
- SOC 2 Type 2 certified

Professional and support services
Expert deployment helps ensure your solution is implemented to fit your unique needs, consistent with security best practices and continues to deliver at the highest level of service. Benefits include:

- Expert product and technology platform professionals lead your implementation
- A thorough onboarding plan to help train your staff to effectively use the product(s)
- 24 x 7 technical support integrated into a problem management system
- Access to systems and applications is limited by role and geographic conditions
- Sensitive data access is limited to its approved residence to limit cross-border transfer and conflicts of interest
- Third-party engagements are managed to limit access to sensitive data and governed by agreements with stringent confidentiality and security requirements

Data protection and privacy

Stryker collects and processes health-related and personal data with a focus on security-friendly processing and responsible handling. See Stryker's Privacy Statement, which governs data processing activities. Rigorous measures help ensure data is protected during its lifecycle, including ensure data is protected during its lifecycle, including:

- Engaging in sub-processing agreements when necessary.
- Scanning repositories to classify sensitive data, such as protected health information (PHI).
- Implementing the Principle of Least Privilege (PoLP) to restrict access to critical systems, accounts and data.
- Use of data encryption for data both at rest and in transit.
- Data anonymization: Anonymizing personal data, when possible, before analyzing it to protect individual privacy.
- Providing clear privacy notices that explain data collection and usage practices, allowing users to control their data.
- Secure data destruction and deletion when no longer needed.

Personnel security

Security is everyone's responsibility and is integrated into onboarding and development practices. Employees are trained to identify and report security threats and skilled security practitioners work to detect and respond to emerging threats.

- Conducting thorough background checks and vetting processes to identify any potential security risks.
- Requiring employees to sign agreements that outline their responsibilities for protecting sensitive information.
- Regular training sessions to educate employees on recognizing and responding to security threats.
- Providing ongoing education and professional development opportunities to keep employees updated on the latest security practices.

Secure infrastructure

Consistent security configurations across physical facilities and computing systems help ensure solutions are secure, available and resilient. Subservice relationships rely on partners with stringent security controls validated by industry standards.

- Implementing firewalls to regulate the flow of data between the network and the internet, blocking potential threats.
- Applying consistent security-friendly configurations across all systems and devices.
- Dividing the network into segments to limit the spread of potential threats.
- Deploying intrusion detection and prevention system to monitor network traffic for suspicious activities and protect against potential breaches.

- Using secure remote access channels such as VPNs and multifactor authentication systems.

Network and system defense

Systems are built with primary functions and safeguards in mind for compatibility and risk segregation. Layered technical threat detection and prevention capabilities protect network boundaries and support real-time threat response.

- Real-time alerts for suspicious access events, such as accessing accounts outside office hours or from unrecognized locations.
- Training staff on procedures for various emergency situations.
- Installing anti-malware software to detect and remove malicious software.
- Enforcing policies to control access to the network based on user roles and device compliance.
- Using security information and event management systems to collect, analyze and respond to security events in real-time.
- Protecting devices connected to the network with antivirus, anti-malware and encryption.

Business resilience

Stryker's solutions offer high availability, rapid scalability and data management capabilities. System survivability is tested for readiness in case of catastrophic events.

- Developing comprehensive plans to recover from natural disasters, cyber-attacks and other disruptions.
- Implementing regular data backups and disaster recovery plans for data availability and integrity.
- Implementing redundant systems and infrastructure to maintain operations in case of failure.
- Diversifying suppliers and logistics to mitigate risks from supply chain disruptions.
- Conducting regular tests and drills to prepare for various scenarios.
- Enabling remote work and flexible schedules to adapt to changing circumstances such as pandemic/absenteeism.

Third-party management

Business partners are carefully selected and onboarded through systematic due diligence to share risk accountability and security responsibilities. Partner engagements are monitored to assess their health and evolving risk landscape.

- Establishing specific criteria to assess vendors' professionalism, reputational risks and overall impact on the organization.
- Conducting thorough due diligence using questionnaires, security ratings and compliance checks to evaluate vendors' security posture.
- Tiering vendors based on risk criticality, setting expectations, establishing communication channels and creating service-level agreements (SLAs).
- Implementing strategies for continuous vendor risk assessment and monitoring throughout the vendor lifecycle.
- Requiring vendors comply with laws, regulations and internal requirements through regular reviews and audits.
- Optimizing contracts to manage compliance risks and document regulatory requirements.
- Maintaining ongoing work and attention to third-party relationships to help ensure alignment with organizational goals.
- Conducting periodic assessments to evaluate the effectiveness of third-party management measures.

Secure system development

Security is a product quality attribute, integrated into design, threat modeling and control gates throughout the system delivery pipeline. Products are tested for security flaws and remediated systematically.

- Defining security requirements as part of the software development lifecycle (SDLC).
- Adopting secure coding standards and guidelines to prevent common vulnerabilities such as SQL injection and cross-site scripting (XSS).
- Conducting design reviews with a focus on security so that security considerations are integrated into the architecture.
- Identifying potential threats and vulnerabilities during the design phase to mitigate risks early.
- Using tools to analyze source code for security vulnerabilities before deployment.
- Testing applications in runtime to identify security issues that may not be visible in static code analysis.
- Integrating automated security testing tools into the CI/CD pipeline for continuous security validation.
- Conducting regular penetration tests to simulate attacks and identify weaknesses.
- Providing ongoing training for developers on secure coding practices and emerging threats.

- Regularly updating and managing third-party libraries and dependencies to mitigate risks from known vulnerabilities.
- Using secure configurations for development, testing and production environments.
- Implementing strict access controls to limit who can modify code and deploy applications.
- Implementing continuous monitoring of applications and infrastructure to detect and respond to security incidents.

Security auditing and verification

Structured self-assessments and rigorous technical product testing feed into corrective actions and continuous improvement processes. Security intelligence is gathered to measure and improve security arrangements.

- Using comprehensive checklists to systematically identify areas of vulnerability, including asset inventories, patch levels, encryption settings, access controls and staff training processes.
- Regularly scanning systems and networks for known vulnerabilities and misconfigurations.
- Reviewing system configurations to meet security best practices and are free from vulnerabilities.
- Verifying that access controls are properly implemented and that permissions are appropriate for user roles.
- Analyzing incident logs to identify patterns and potential security breaches.
- Evaluating the security practices of third-party vendors and partners to validate they meet organizational standards.
- Assessing network security measures, including firewalls, intrusion detection and prevention system and network segmentation.
- Reviewing cloud security configurations and practices to protect sensitive data and comply with applicable laws and best industry standards.
- Continuously evaluating and updating security policies and procedures.
- Assessing the effectiveness of security awareness training programs for employees.
- Implementing continuous monitoring tools to detect and respond to security incidents in real-time.

Regulatory and standards compliance

Independent validation and certifications, such as HIPAA, SOC Type 2 and HITRUST, provide objective assertions of the quality of Stryker's solutions. Please see product specific documentation for applicability of such certifications.

- Implementing safeguards to protect patient health information and to help ensure compliance with HIPAA regulations.
- Adopting NIST cybersecurity framework to enhance security practices and to help ensure compliance with federal guidelines.

Conclusion

Protecting information assets is integral to Stryker's mission. Security arrangements align with the interests of customers, employees, regulators and partners. Stryker's commitment to security is relentless, aiming to earn confidence and trust continuously. To learn more about the security arrangements for specific products contact your customer success representative, email: vcsupport@stryker.com, or visit our support website. The Stryker Privacy Policy describes our commitment to data privacy.

Stryker Corporation or its divisions or other corporate affiliated entities own, use, or have applied for the following trademarks or service marks: Stryker, Vocera, Vocera Edge, Vocera Engage. All other trademarks are trademarks of their respective owners or holders.

10/2025. AC-GSNPS-COMM-2391136_REV-0_en_us

Copyright © 2025 Stryker