DATA SHEET

Vocera Leads the Way in Healthcare Information Security

The security of patient health information is of vital importance to healthcare providers. The healthcare industry, valued at three trillion, has become an increasingly valuable target for cyber criminals. Medical records sell at a premium because they contain personal data such as names, addresses, medical information, social security numbers, birth dates, and billing information.

Vocera provides the industry leading communications platform allowing physicians and other health care professionals to communicate critical patient information in real-time. Timely exchange of patient health information (PHI) facilitates the best care possible and saves critical time for health care professionals to collaborate on patient care.

Going Beyond Enabling HIPAA-Compliant Communication

Vocera's Secure Messaging solution enables HIPAA-compliant text messages, alerts, and other information, directly to and from smartphones. Not only does Vocera enable HIPAA-compliant messaging, we have implemented additional security features in place to ward off any further security threats.

Vocera's Best-in-Class Security Features

Security Feature	Description	Benefit
AES 256 bit encryption	The Vocera® Collaboration Suite secure messaging App uses AES-256 encryption for its data on the smartphone (known as "at rest").	Ensures data security. AES 256 encryption is considered among the top ciphers approved by the US Government to protect Top Secret data.
Active Directory Integration	During registration active directory integration provides another level of security prompting the user for their credentials to open the Secure Messaging App on their smartphone.	Adds additional level of security and user access verification.
PIN Code	Both a device level password profile or an application level PIN can be used for security. Either or both can be used. Vocera Collaboration Suite solution can also enforce device level PIN and also supports the use of device certificates to ensure only authorized devices can connect.	Adds additional level of security and user access verification.
Remote Wipe	Administrators also have the option to wipe all data stored in the user's smartphone application. This will not wipe the entire phone, but just the data inside the Secure Messaging App.	PHI data can be wiped remotely from phones that are lost, stolen, or transferred to new user.
SOC2 Audit	One of the nation's leading registered CPA firms performing SSAE 16 and SOC 2 audits has completed an in-depth security audit of the Vocera Secure Texting solution. SSAE 16 Professionals have issued an unqualified opinion that Vocera Secure Texting meets the American Institute of Certified Public Accountants criteria for SOC 2 Type 1 report.	A SOC 2 Type 1 report provides Vocera Secure Texting customers an independent verification that the Vocera Communication Platform meets the criteria defined by the AICPA Trust Services Principles, which confirms that highly secure and effective control systems are in place to protect data transmitted through the software platform and secure messaging solutions.

Vocera Solutions Meet Stringent Federal and US Department of Defense Standards

Vocera's security validations firmly establish our position as the leader in secure healthcare communications and go beyond to meet the specific needs of the US Department of Defense.

Security Feature	Description	Benefit
Joint Interoperability Test Command (JITC)	Vocera's core communications systems have been approved by the Department of Defense for use on its secure networks. To attain this certification Vocera had to complete rigorous interoperability (IO) and information assurance (IA) certification.	Provides confidence Vocera solution's security has been certified to the most rigorous US Government standards.
DoD Information Assurance Certification and Accreditation Process (DIACAP)	Vocera's core voice solution received an Authority to Operate (ATO). To achieve an ATO, Vocera completed the DoD Information Assurance Certification and Accreditation Process (DIACAP). DIACAP defines a DoD-wide formal and standard set of activities, general tasks and a management structure process for the certification and accreditation of a DoD IS that will maintain the information assurance posture throughout the system's life cycle.	Ensures that risk management is applied on information systems (IS) to comply with DIACAP United States Department of Defense (DoD) processes.
Federal Information Processing Standard (FIPS 140-2)	The Vocera B2000, B3000, and B3000n Badges have been validated as meeting the strict requirements for the U.S. government.	Ensures cryptographic modules used in Vocera Badges meet US Government security standard accreditation.

Ensuring a safe, secure, and compliant communication system for healthcare institutions goes beyond simply enabling HIPAA-compliant communication. When partnering with the US Department of Defense and other Federal agencies, the demands multiply. Vocera leads the market in meeting and exceeding security and compliance standards ensuring sensitive patient health information is protected.

For More Information
Visit www.vocera.com,
email info@vocera.com,
or telephone 1-888-9-VOCERA.

Vocera Communications, Inc.
525 Race Street
San Jose, CA 95126
tel : +1 408 882 5100
fax : +1 408 882 5101
toll free : +1 888 9VOCERA
www.vocera.com

DS_SecurityCompliance_032017_V2