DATA SHEET

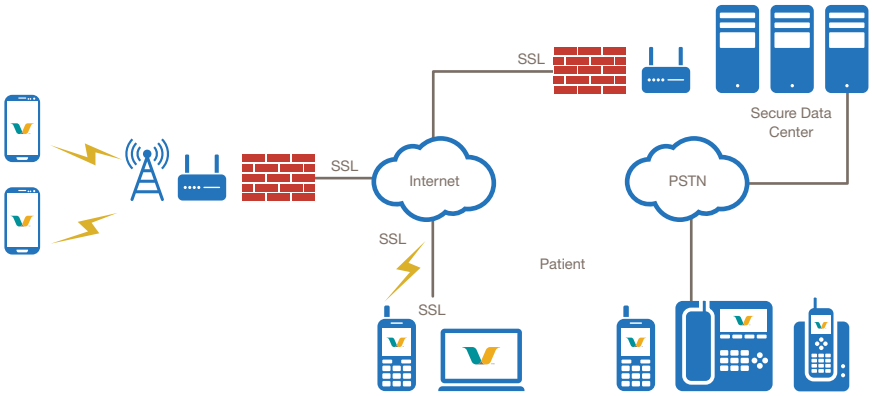
Vocera Care Experience Security Protocols

This document sets forth the Security Protocols found within the Vocera Care Experience solution suite.

Recognizing the obligations set forth by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), P.L. 104-191, as amended, and the Health Information Technology for Economic and Clinical Health Act (“HITECH”), Vocera has developed a secure solution architecture designed to protect the integrity, confidentiality and availability of a facility’s Protected Health Information (“PHI”). Additionally, some of the Vocera® Care Experience solution features may be configured for our clients to comply with varying state and facility regulations, policies and procedures.

Architecture

The solution architecture is designed to permit a secure flow of information whether as an upload from the user to the servers or as a response to a query from a user. The solution utilizes end to end encryption to ensure that any PHI is secured during transit or at rest. The solution does not permit the end user to actively manipulate any data stored on the server. The following diagram sets forth the basic solution architecture.



Access

The solution and the associated website may be accessed only by those end users (including patients) and product technicians issued appropriate credentials in the form of a password, PIN, or a combination of both.

- End users are identified by the facility and assigned a unique password. Upon successful entry of a password, a user may then complete a variety of user functions, including uploading patient information or querying the system.
- Patients are issued PINs by the facility upon discharge permitting access to their individual records. Lost PINs may be reissued by the facility.
- Vocera personnel are assigned access privileges based upon their individual roles within the company. Personnel with access privileges must use their unique passwords to gain system access.

All access, whether by end user, patient or Vocera personnel, is logged by the system and appropriate audit logs may be generated upon request.

Server Security

Servers are located at an offsite data center featuring 2N+1 redundancy in Internet, power and telecommunications.

- Audit discharge instructions and other patient communication
- Ensure care instructions are handled consistently throughout the organization
- Stratify patients most at risk to be readmitted
- Monitor staff compliance and competency
- Identify staff recognition and teaching opportunities

Additional security features include:

- Biometric scanners
- Mechanical security
- Alarms
- Video monitoring
- 24/7 human monitoring
- Data storage on encrypted drives across large arrays for additional redundancy

Please note that only certain Vocera personnel are credentialed to access the offsite data center for specific solution support requirements.

Encryption/Secure Transmission

The Vocera Care Experience solution ensures the security of PHI from its inception to its destruction by providing an end to end encryption scheme.

"Data in Transit"—The Vocera Care Experience solution permits the transmission of PHI both between the facility and the server and the patient and the server depending upon the individual query.

From the facility side, the solution may query the server as either the user is uploading information on a particular patient or as part of an automated process. Dependent upon the query either an IPSEC tunnel or an SSL tunnel is used for PHI transmission between the solution and the facility. Both IPSEC tunnels and SSL tunnels are deployed in accordance with the NIST Special Publications 800-77, Guide to IPSEC VPNs and 800-113, Guide to SSL VPNs respectively. Transmission of PHI resulting from a patient query also travels through SSL tunnels similarly deployed.

"Data at Rest" – Data may "rest" in one of three locations within the Vocera Care Experience solution: within the mobile application during creation or retrieval, on the website or on the servers.

The mobile application encryption scheme is designed to rely in part upon the hardware encryption and in part on the application itself. The Good to Go® application within the Vocera Care Experience suite operates on iOS® devices, including iPhone® 3GS, iPod® Touch 4th gen (also 3rd gen 32gb), and iPad® 1. Older versions of iOS devices do not support encryption and will not run the application. To utilize the hardware encryption, Vocera suggests requiring a device lock after a period of inactivity. In addition the application logs users out after a period of inactivity (configurable to facility) and any information not uploaded to the server at the time of log out will automatically be deleted by the application from the mobile device.

PHI at rest on servers is encrypted consistent with the NIST Special Publication 800-11, Guide Storage Encryption Technologies for End User Devices.

For More Information

Visit www.vocera.com, email info@vocera.com, or telephone 1-888-9-VOCERA (1-888-962-2372).

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

Vocera Communications UK Ltd.
100 Longwater Avenue
Green Park
Reading, Berkshire
RG2 6GP
United Kingdom
tel : +44 0 844 335 1237
fax : +44 0 118 945 0493
www.vocera.co.uk

Vocera Canada
8 Market Street, Suite 300
Toronto, Ontario
M5E 1M6
Canada
tel : +1 416 923 2900
fax : +1 416 923 2981

VOC_7353_DS_Product_Security_USA_021714_v1