


Vocera Communications:

HIPAA Data Security and Privacy Standards for
Voice Communications Over a Wireless LAN





Vocera Badge

[Actual Size]

❖ Introduction

This white paper will address compliance issues associated with voice communications over wireless networking technologies within the context of the Health Insurance Portability and Accountability ACT (HIPAA) and how the Vocera Communications System meets HIPAA data security and privacy standards. As a first step, this paper will briefly provide background on HIPAA regulations. Next, it will explain how the Vocera Communications System works in the healthcare setting, followed by a demonstration on how the Vocera Communications System fulfills HIPAA data security and privacy standards. It concludes with guidelines for “best care” practices for healthcare workers using Vocera communications badges.



•• The Health Insurance Portability & Accountability Act (HIPAA)

The Health Insurance Portability & Accountability Act (HIPAA) is a new federal law creating security standards to ensure the privacy of patients' medical records and personal health information. It affects primarily hospitals, healthcare providers, insurance companies, and anyone who has access to a patient's medical data. Because healthcare providers use the Vocera Communications System, which operates over wireless networks, to communicate the medical treatment of patients, the system must comply with HIPAA regulations.

The HIPAA rules are primarily for "covered entities," which are health plans, healthcare clearinghouses, and certain healthcare providers. But the laws also apply to a "business associate," which is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information it receives or creates on behalf of the covered entity." Under the law, Vocera Communications is considered a "business associate." Technically, the law only applies to companies, vendors, or professionals who have access to a patient's medical case file, but chances are high that any company who deals with the medical industry will have to be HIPAA compliant. To comply with HIPAA data-security standards, hospitals must meet five main requirements:

- Confidentiality. Keep all transfers of information private; ensure that information is not made available or disclosed to unauthorized individuals
- Integrity. Ensure that data has not been changed en route or in storage
- Authentication. Verify that the person sending the message is who he or she claims to be
- Non-repudiation. Once a transaction occurs, neither the sender nor the recipient can deny that it took place
- Authorization. Allow authenticated users access to network information and resources based on defined privileges

The main concept of the security principle is simple. Any company that has access to medical information must document the individuals who accessed the files, when they accessed it, and for what purpose they accessed it. The security standards apply to all individually identifiable health information in electronic form, which is being stored or covered by the HIPAA Transactions Standards Rule, including internal transmission. All healthcare providers, health plans, or clearinghouses that electronically store or transmit individual health information must comply.

❖ The Vocera Communications System

Ongoing, instant communications between mobile, dispersed hospital staff is critical to improved quality of care, effective operations, and productivity in hospitals. Many communications options in use in hospitals today, such as overhead paging, in-house pagers, and in-building phones, do not provide instant communications among staff. Rather, when these systems are used, there is a significant amount of time wasted as personnel spend time tracking down each other through paging or playing “telephone tag.” This inability to reach anyone instantly increases stress levels and reduces productivity.

The Vocera Communications System is a wireless platform that provides hands-free, voice-controlled communications throughout any 802.11b networked building or campus. Utilizing Voice Over IP (VoIP) and WLAN as its transport mechanism, the calls are managed and set up by the Vocera Server, but the actual call is between two badges on the data network, and does not involve the server for the duration of the call.

The system enables fluid, instant voice conversations among team members, across groups, and throughout an organization of mobile professionals.

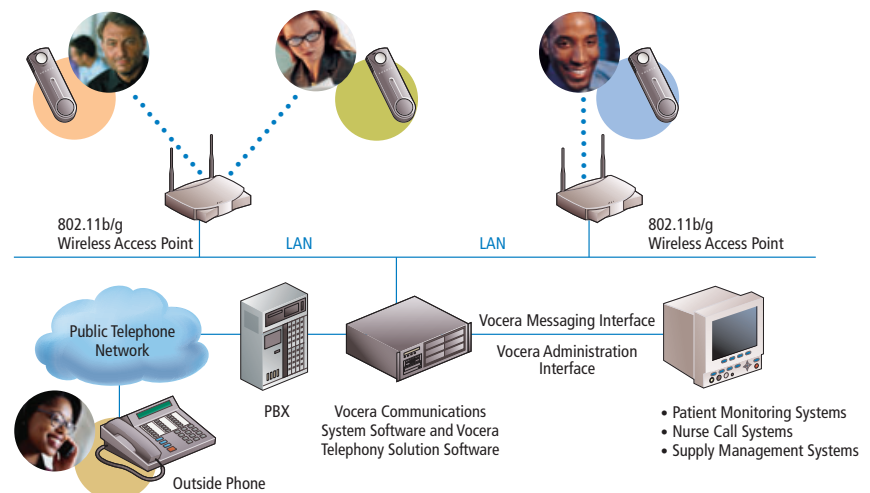
Vocera’s instant communications system keeps voice conversation active as mobile users change departments, change floors, and even change buildings within a campus. It delivers high-performance enterprise security, including user authentication, voiceprinting, encryption for an unlimited number of user groups, and audit logs. Vocera has the ability to interface with a PBX system with optional add-on server software and an analog line card. Being able to make a call offsite and be directed to a specific person or group is a key benefit. Because Vocera uses ISM (Industrial Scientific Medical) Wireless Band, it doesn’t affect any other electronic equipment used in hospitals.

The following diagram explains how the Vocera Communications System works:

❖ Vocera Server Software

The Vocera communications platform is made up of two elements: The Vocera Server software and the wearable Vocera Communications Badge. The Vocera Server software runs on a standard Windows 2000 server and houses the centralized system intelligence: the user database, call manager, connection manager, administration console, user console, and speech recognition engine. The Web-based administration console and user console enable system management and individual use settings, respectively. The software scalability enables literally thousands of users to be programmed into the system database. In addition, the optional telephone interface module allows the Vocera system to communicate with telephony systems.

Vocera Communications Network Diagram



[Figure 1: Vocera Network]



❖ Vocera Communications Badge ❖ Data Security for Voice Communications over a Wireless LAN

The Vocera Communications Badge is a wearable device that weighs less than 2 ounces and can easily be clipped to a shirt pocket or worn on a lanyard. It enables instant two-way voice conversation without the need to remember a phone number or manipulate a handset.

Features include:

- A voice user interface and one-button control to place calls with voice commands and that allows users to continue working without having to fuss with a handset or keypad
- Call by name, title, function, or group eliminates the need to know phone or extension numbers or even who is on duty
- Call blocking and call screening provide flexibility and privacy
- Conference calling and group messaging facilitates system-wide announcements

The ability to call to and from the badge through the PBX to telephones, such as desk extensions and cell phones, provides instant communication with contacts inside the building or outside the WLAN.

The Vocera Communications System provides wearable instant voice communications for healthcare staff, which results in many benefits:

- Save time by instantly connecting staff to each other to make decisions quickly
- Conserve scarce nursing resources and increase their productivity
- Reduce time spent tracking down necessary personnel, and increase time spent on patient care
- Increase healthcare staff morale and retention

Most important of all, it improves quality of patient care and safety.

In essence, data security for wireless applications consists of three main components: encryption, authentication, and data integrity.

Wireless LAN Security Requirements

Encryption

For secure through-the-air communications, wireless applications can take advantage of two standards; the Internet Protocol Security (IPSec) or Wired Equivalent Privacy (WEP.) IPSec is a security extension of the Internet protocol that governs land-line networks. Any communications that flow between these two end points are encrypted — data is scrambled and thus indecipherable without the proper decoding software.

WEP is a security protocol for wireless local area networks (WLANs) and is the most common approach used in 802.11b networks. WEP is designed to provide the same level of security as that of a wired LAN. WEP provides security by encrypting data over radio waves so that it is protected as it is transmitted from one end point to another.

Authentication

The HIPAA privacy regulation requires that the covered entity employ appropriate safeguards to ensure that the person sending the message is who he or she claims to be.

Data Integrity

HIPAA requires that data be protected from unauthorized changes while in storage or en route to authorized users.

The Vocera Communications Systems employs security features for all three components as outlined here:

Vocera Security Features

Vocera Communications System

The Vocera Communications System supports both 64-bit and 128-bit WEP (Wired Equivalent Privacy) encryption and system SSIDS. Additionally, Vocera utilizes a proprietary voice compression algorithm that both compresses and encrypts badge transmission. As security standards such as 802.11i IEEE initiative and WPA (Wi-Fi Protected Access) become better defined and adopted by the industry, Vocera will ensure its system is upgraded to the new standard. Vocera also encourages its customers to set up separate VLANs for voice traffic.

Voiceprinting is a significant security enhancement to the Vocera Communications System because it prevents imposters from logging in as someone else or gaining unauthorized access to sensitive information, such as voice mail, e-mail, and text messaging.

When employees log into the system, they say their name and repeat requested random digits. A pre-recorded voiceprint is compared to the user's voice to determine if there is a match. Each time the user logs into the system, the voiceprint is enriched and better captures the user's voice characteristics. The system captures the behavioral characteristics of the way the person speaks, as well as physical characteristics of the person's vocal tract. During voice authentication, the voice of the user is compared to the stored voiceprint to verify the claimed identity. This security feature is a biometric identification system, similar to a fingerprint, and even works if a person's voice changes slightly, such as when they have a cold.

The Vocera System does not record or store conversations between users. Once a call is connected voice communications over the system are as secure as a traditional phone conversation.

:: Safeguarding Patient Privacy While Using the Vocera Communications System

Treating patients requires that healthcare workers communicate with each other. Providers must have full discretion in determining what personal health information to include when sending or discussing patients' medical records with each other. That's where best practices for communicating patient information come into play.

Best Care Practices

Users of the Vocera Communications System should remain aware at all times that information shared via the system can be heard at the receiver's end, if a headset is not in use, and could be overheard by individuals other than the receiver. Therefore, reasonable precautions must be taken to minimize the potential for inadvertent or incidental disclosure of patients' protected health information (PHI) to bystanders who may not be authorized to receive such information.

PHI is broadly defined in the HIPAA Privacy Rule to mean any individually identifiable health information (information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual, and that identifies the individual or could be used to identify the individual) that is transmitted by or maintained in any form or medium (including electronic media). PHI may be more specifically defined in applicable hospital policies.

The reasonable precautions that users of the Vocera Communications System are expected to take shall include (but are not necessarily limited to):

If you are the provider of information:

1. Pay attention to your surroundings and keep an eye out for any bystanders who may overhear your conversations.
2. Always assume bystanders who are not authorized to receive PHI may be present on the receiver's end, unless the receiver specifically states otherwise. When appropriate, let the receiver know you need to transmit patient-specific information, and consider asking the receiver if he/she is clear to talk or if they need to move to a more private location.
3. Use your best judgment to limit the information you relay via the Vocera Communications System to only reasonably necessary items the receiver needs to make appropriate decisions and take appropriate actions within the context of his/her job.
4. Leave the patient's name out of the conversation whenever reasonably feasible, and if you can do so without risking confusion on the part of yourself and the receiver.
5. For voice mail messages, leave the patient's name out of the voice mail, if possible. Instead, use a patient number or private code to protect the patient's privacy. Alternatively when playing voice mail check your surroundings to ensure privacy.



•• Conclusions

If you are the receiver of information:

1. Pay attention to your surroundings and keep an eye out for any bystanders who may overhear your conversations.
2. Keep in mind that individuals who are not authorized to receive PHI may suddenly walk up on the other party's end. Leave the patient's name out of the conversation whenever reasonably feasible, and use your best judgment to limit your inquiries to only the information you believe is reasonably necessary for you to make appropriate decisions and take appropriate actions within the context of your job.
3. If you are in a location where bystanders are present who may not be authorized to receive PHI and someone begins to relay patient-specific information to you via the Vocera Communications System, quickly do one of the following:
 - Interrupt the other party and ask him/her to hold that information until you can move to a more private location, or
 - Use a headset with the Vocera Communications Badge to hold a private conversation.
 - Place your Vocera Communication Badge on "hold" until you are able to move to a more private location.

All users of the Vocera Communications System must be in-serviced on this policy and procedure initially upon becoming an authorized user of the system and at least annually thereafter. They must be able to demonstrate knowledge of and competency in the reasonable precautions described above. Evidence of the initial and annual in-services and competency demonstrations shall be documented in the employee's education file.

Healthcare institutions are facing a huge staffing crisis that is leading to an increased number of catastrophic events. This shortage places a huge burden on the healthcare staff to perform efficiently. Timely, precise communications can eliminate some of the wasted time staff spends searching the facility or playing phone tag. With instant voice communications over an 802.11b network staff can talk with the resources they need instantly. No waiting for a dial tone, ringing or waiting for the other side to answer the phone. With instant communication, the time spent tracking down necessary personnel is instead available to spend on patient care.

The Health Insurance Portability & Accountability Act (HIPAA) was designed to help protect patient information. It should not impede the quality of care. With responsible use of the Vocera Communications system healthcare workers can increase overall quality of care and add to patient safety while maintaining the integrity of the rules created by HIPAA.



525 Race Street
San Jose : CA 95126
tel :: 408.882.5100
fax :: 408.882.5101
www.vocera.com

