

Voice Documentation in HIPAA Compliance

An OAISYS[®] White Paper





Table of Contents

- The HIPAA Security Rule 1
- Electronic Medical Records 2
- Voice Documents and EMRs 3
- How Voice Documentation Works 3
- OASYS and HIPAA Compliance 4
- Training and Process Compliance 5
- Voice Documentation in Action 5
- Conclusion 6



Voice Documentation in HIPAA Compliance

When it passed into law in 1996, the Health Insurance Portability and Accountability Act (HIPAA) created a profound impact on how healthcare providers in the United States conducted business.

While Title I of the act protects workers' insurance coverage options when they change or lose their job, Title II creates and defines numerous new regulations and processes relating to patients' healthcare information and provides civil and criminal penalties for failing to adequately protect it.

This paper will examine Title II's "Security Rule" and discuss how OAISYS Tracer and Talkument™ voice documentation solutions address the rules requirements for records arising from telephone-based conversations.

The HIPAA Security Rule

Title II of HIPAA aims to reduce fraud and abuse while simultaneously simplifying administration of patient records.

The Act's Privacy Rule sets forth who can receive protected health information (PHI) from the care provider.

The Security Rule, also known as The Final Rule on Security Standards, complements the Privacy Rule by establishing administrative, physical and technical safeguards.

Administrative safeguards generally require organizations that must comply with HIPAA to establish a set of procedures to protect patient privacy, identify employees or types of employees who can access electronic protected health information, train employees in the process and ensure that outside vendors who may see patient information have their own processes in place. There must also be plans in place for information auditing and to deal with security breaches should they occur.

Physical safeguards are meant to protect against inappropriate access to patient data. These include how hardware and software changes and disposal are conducted, restricting access to electronic storage devices to authorized personnel only, creating security plans for maintenance records, protecting workstations from public view and training third-party vendors on physical access procedures and policies.

Technical safeguards require organizations to control access to their computer systems and protect data transmitted over computer networks. These safeguards include access protection, password protection, data integrity verification and documenting the security process and configuration settings.



Electronic Medical Records

The Security Rule applies explicitly to electronic medical records (EMRs). An EMR is any medical record stored in a digital format. These can include treatment records, notes on patient care, images, billing statements and insurance provider notifications, among others.

EMRs have proven significantly more accurate than traditional, handwritten patient notes and other records. They are more legible, as well as more easily stored and retrieved. However, there is a lack of established standards and a low degree of interoperability among EMR systems, and many organizations have been slow to adopt these solutions.

Among regulators and patient groups, the benefits of EMR solutions outweigh organizational concerns, and there has been a concerted push to implement EMRs in healthcare organizations for that reason.

The rate of adoption has been slow (25 percent of doctors' offices as of 2005), but it has been steadily increasing. As a result of patient and industry demand, all healthcare organizations should consider their EMR strategy and how to make it compliant with HIPAA safeguards.



Voice Documents and EMRs

The benefits to a healthcare organization of converting paper records to electronic formats are well-documented both in terms of operation efficiency and patient care. However, until now no effective solution has existed to port those same benefits to telephone-based interactions.

In a busy office, it is exceedingly difficult to create and maintain adequate paper notes on telephone conversations. Writing notes by hand or typing them on a keyboard by necessity leaves out content and creates a high potential for error.

Call centers in medical-related fields, such as insurance, have used call recording technology for years to reduce their liability, ensure accuracy and evaluate agent performance. These solutions have been of great benefit in charting call volumes, training agents, resolving disputes as to what was said by whom and, in general, maintaining efficiency on an organization-wide level. Unfortunately, this "top-down" approach does not make sense outside of call centers.

OAISYS offers an organization-wide voice documentation solution that represents a radical shift in both the approach to and execution of how call recording technology can be used by health care providers.

With Tracer and Talkument, individual users can refer to, play back and share phone conversations with other authorized users. They can highlight portions of the call, insert comments for supplemental information and share a link to the document with another healthcare worker, billing agent or facility to ensure that patient needs are fully met.

How Voice Documentation Works

Our voice documentation software solutions are deployed via a flexible, cost-effective OAISYS hardware platform, working in tandem with business telephone systems to capture calls and store them as searchable, playable electronic voice documents. Now, rather than merely inserting notes into a file, the call is documented and stored in its entirety and can be organized into an electronic folder, retrieved by a combination of any number of search criteria, commented upon and securely shared with others.

OAISYS and HIPAA Compliance

OAISYS voice documentation solutions can easily and immediately fit into an organization’s Security Rule compliance programs.

HIPPA-Required Safeguards

The table below illustrates components of each of the HIPPA-required safeguards and how OAISYS solutions may satisfy them.

Administrative Safeguards	
Procedures must identify employees or classes of employees who will have access to protected information. Access must be restricted only to those employees who need the information to complete their job functions.	OAISYS built-in access controls are easily configured to restrict access to only those individuals who are authorized to access voice documents. Access sharing can be restricted to specific employees or groups.
Covered entities must have a plan for data backup and disaster recovery.	Voice documents safely reside in a central location, which can easily be incorporated into existing backup and disaster recovery protocols.
Procedures must detail how to address security breaches should they occur.	Administrators can log into individual users’ accounts to review with whom users have shared voice documents.
Physical Safeguards	
Controls must be established to introduce and remove new equipment on the network.	OAISYS recording platforms interface with the business telephone system, utilizing established parameters without need for revision.
Equipment containing healthcare information must have controlled and regularly monitored access and hardware and software access must be limited to authorized users.	As a centralized solution with permissions-based access to content, OAISYS recording systems should meet these criteria.
Technical Safeguards	
Voice document sharing with outside entities is performed through a secure link sent via email, and a record is kept as to with whom the document was shared. As access to email is normally restricted to users logged in via password on a secure network, authentication is achieved.	The ability to permanently delete voice documents must be specifically assigned by an administrator. Voice documents cannot be changed except to add text-based annotations.
Covered entities are responsible for ensuring data on their systems cannot be changed or erased in unauthorized manners.	A covered entity must authenticate with whom it communicates.

Training and Process Compliance

The Security Rule requires that employees be trained in process compliance. Using voice documents, supervisors have an ideal training and monitoring tool that uses an employee's own conversations to point out what is done correctly and where process adherence can potentially be improved.

Supervisors with appropriate access permission can conduct spot reviews of voice documents to ensure process compliance. When errors are made, the supervisor can highlight them and include a reminder as a comment.

Voice Documentation in Action

Consider the following scenario. Monica Jones calls her primary physician's office complaining of fatigue, mood swings and thirst and asks to schedule an appointment as she fears she may be becoming diabetic.

The technician talks to her and schedules an appointment for the following Monday. After completing the call, the technician puts the voice document in a folder for Ms. Jones. He then brings up the voice document, highlights the portion where Ms. Jones describes her symptoms and shares it with the doctor. In this way, the doctor can review the patient's stated symptoms in advance for the appointment if his schedule permits.

After examining her on Monday, the doctor wants Ms. Jones to undergo a glucose tolerance test. Depending on the results, he may or may not refer her to an endocrinologist for further testing.

The office manager calls the testing lab and sets up an appointment for Wednesday afternoon. However, when Ms. Jones arrives for her appointment, the lab only has her scheduled for a routine battery of blood work. The scheduler had input the wrong code when talking with the office manager.

While still at the lab, Ms. Jones calls the doctor's office to make sure she was, in fact, supposed to have the glucose tolerance test that day. The office manager puts her on hold, retrieves the voice document of the call to the lab and plays it back. She confirms with Ms. Jones and asks her to wait at the lab while she attempts to resolve the mix up.

The office manager then calls the lab and talks to a supervisor. At first the supervisor is defensive and says the doctor's office must have made a mistake. The doctor's office manager offers to share a link to the voice document that proves the error was on the lab's end. The lab supervisor says that if the office manager can prove to his satisfaction that the error was committed by the lab, he will make sure Ms. Jones gets her test that day.



The office manager sends a secure, encrypted link to the lab supervisor's email address. He plays the conversation back, realizes it was his staff who scheduled the wrong test and gets Ms. Jones started with the correct test right away.

Using OAISYS voice documentation functionality to share patient information in a manner completely compliant with HIPAA regulations, the doctor's office has turned what could have been a delay of several days into a minor inconvenience.

Conclusion

OAISYS Tracer and Talkument software solutions ensure conversations between patients, healthcare providers, insurers and others related to their care are preserved with 100 percent accuracy and complete collaborative ability among authorized users.

Voice documents themselves never leave the central location on which they are stored, and access links to voice documents are securely transmitted between authorized parties only.

The HIPAA Security Rule requirements place stringent controls on how EMRs can be stored and shared. OAISYS voice documentation solutions satisfy these regulatory concerns while improving patient care and bridging potential gaps in recordkeeping.

Lastly, OAISYS solutions can be added to any healthcare organization regardless of where they may be in their transition to an EMR system, as they function separately and in parallel to whatever text- and image-based solution an organization may ultimately employ.

To find out more about Tracer, Talkument and OAISYS, please contact us at **888.496.9040** or visit us on the web at www.oaisys.com.

To find a reseller near you, go to www.oaisys.com, click "Support," then "Reseller Locator."