



215 Ridgedale Ave
Florham Park, NJ 07932
Email: sales@trisys.com
www.trisys.com
Tel: 973-360-2300
Fax: 973-360-2222

Replay Call Recording for HIPAA

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, 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 Recordings 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.

With Replay call recording solution, individual users can refer to, play back and share phone conversations with other authorized users. They can also insert notes for supplemental information.

How Replay Call Recording Works

Our call recording software solutions works together in partnership with our Tapit call accounting to capture calls and store them as searchable, playable electronic voice recordings. Now the call is documented and stored in its entirety and can be retrieved by Tapit, acting as the search engine, and by a combination of any number of search criteria, commented upon and securely shared with others.

Trisys and HIPAA Compliance

Trisys Replay call recording solutions can easily and immediately fit into an organization's Security Rule compliance programs.

HIPPA Required Safeguards

This table illustrates how Replay call recording satisfies HIPPA required safeguards.

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.	Trisys built-in access controls are easily configured to restrict access to only those individuals who are authorized to access voice documents. Optional data encryption is also available.
Covered entities must have a plan for data backup and disaster recovery.	Voice recordings 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.	Trisys products will adhere to client's network security procedures.
Physical Safeguards	
Controls must be established to introduce and remove new equipment on the network.	Replay call recording interfaces with the business telephone system on the trunk side or station side, 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, Replay 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 recordings must be specifically assigned by an Administrator. Voice recordings 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 Replay's voice recordings, 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 call recordings to ensure process compliance. When errors are made, the supervisor can highlight them by adding a call note to the call record in Tapit.

Conclusion

Trisys Replay and Tapit 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. Trisys call recording solutions satisfy these regulatory concerns while improving patient care and bridging potential gaps in record keeping.

Lastly, Trisys 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 Replay, Tapit and Trisys, please contact us at **973.360.2300** or visit us on the web at **www.trisys.com**.