Achieving HIPAA and HITECH Act Compliance with Engage WFO™

Secure protected health information in call and screen recordings

HIPAA and HITECH Rules

The 1996 Health Insurance Portability and Accountability Act (HIPAA) sets forth rules for electronic data interchange in healthcare. These rules require healthcare organizations to maintain minimum privacy and security standards to protect patient health data. The Privacy Rule protects individually identifiable health information. The Patient Safety Rule provides patient confidentiality. The Security Rule sets national standards for securing electronic protected health information (PHI).

The 2009 Health Information Technology for Economic and Clinical Health Act (HITECH) expanded HIPAA rules to include electronic health records and healthcare organizations' business associates.

Organizations must reasonably secure PHI—voice and screen recordings—from use that violates HIPAA rules. Benefits for organizations who comply include:

- 100% reliable call and screen recording.
- Authorized user control of call and screen recordings.
- Recordings are easily retrieved on demand.
- Recordings are stored securely.
- Archived recordings are available for audits.
- Provide legal defense and minimize litigation risk.

Engage WFO is a compliance recording and workforce optimization system used for achieving optimal performance. Integrated screen capture, analytics, and quality management enable service excellence. Desktop analytics automates regulatory compliance and CRM integration to gain value from interactions. Call recording supports service quality, policy adherence, and regulatory compliance. Recordings enable monitoring of service quality, resolving issues quicker, supporting legal defense, and mining fresh intelligence.

Securing protected information

Engage WFO enables healthcare organizations that record patient interactions to manage and secure access to PHI. With role-based access security, Engage WFO provides file-level encryption and audit trail reporting for monitoring compliance.

Recording encryption

Engage WFO stores patient interaction records with AES 256-bit encryption. The records are unreadable without unique decryption keys.

Network encryption
Engage WFO uses Secure Sockets Layer encryption for network communication during recording and playback. Data is encrypted prior to and during recording, including the video streamed from agent workstations and audio transmitted from remote servers to central storage.

Role-based permission
Engage WFO security features include hierarchical role-based user permissions. The system administrator can set granular controls, allowing only authorized users to access or export audio and video recordings. Access permissions may be tailored job responsibilities.

Password security
Engage WFO security forces password adherence to assist with HIPAA compliance. Passwords are required to be at least seven characters and contain numeric and alphabetic (both upper and lower case) characters. Users must change passwords every 90 days and not re-use the four most recent passwords. Users must re-authenticate after 15 minutes of idle time. And, access is blocked after six incorrect login attempts.

Data access monitoring
Engage WFO includes activity tracking of all system activity. Administrators conduct audits to determine who accessed any recording for playback, export, or other functions. System logs enable forensic investigation in case of compromise.

Data archiving and purging
Engage WFO users may customize archiving rules so records are automatically archived and purged in compliance with their organizational, HIPAA, and HITECH rules.