

Call Recording in Healthcare

The Easy Way to Protect and Safeguard Patient Data



Healthcare contact centers are fast-paced, high pressure operations where split-second decisions can mean the difference between life and death. Whether juggling critical tasks or handling a sentinel event, compliance with healthcare and financial regulations is the last thing a healthcare professional has on their mind. And yet, the steep fines and damaged reputations that come with violations is serious business.

In the healthcare contact center, patients often provide sensitive information over the telephone — from social security numbers and Protected Health Information (PHI) to credit card numbers and bank routing numbers. When personal information is captured and stored, it could potentially be accessed by unauthorized personnel or released to the wrong parties.

To protect the privacy of patient data, mandates such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS) provide strict guidelines to eliminate the risk of capturing and storing potentially compromising personal and financial information.

Eliminate the Risk

The manual, agent-initiated method of pausing and resuming recording leaves the door wide open for human error — and editing recordings manually after they are stored is unreliable and simply unfeasible at high volume call centers.



What is the best way to ensure sensitive personal information and payment data stays safe? Don't record it in the first place! HIPAA and PCI compliance can be implemented and adhered to within the healthcare contact center or other healthcare recorded environments without manual intervention by the agent or supervisor.



An effective interaction recording solution can selectively record based on agent workstation activity, ensuring that sensitive patient information is never captured, while the rest of the interaction remains completely intact.

Automated Triggers Pause and Resume

The HigherGround® Calibre™ interaction recording solution uses sophisticated API and screen diagnostic tools to automatically pause recordings when sensitive customer data is entered.

For instance, you can configure Calibre to pause recording every time credit card information is exchanged. When an agent navigates to an application screen used for credit card transactions, the recorder is automatically signaled to pause. Recording resumes only when the payment application window is closed — ensuring compliance without any direct interaction from the agent or supervisor on every call.

Ensure the Safety and Privacy of Patient Data

Restrict access of recordings and sensitive data to authorized personnel through the permissions tool in the HigherGround interface. Our recording solution incorporates extensive security measures to preserve the integrity of the interactions you record, capture and store, such as:

- **Encryption:** All recordings are encrypted as they are captured and stored on the server to prevent unauthorized access or alteration to the files.
- **Digital Signature:** Validate all recordings stored on the server to ensure they are 100% authentic with a cryptographically strong one-way function.
- **Digital Audit Trail:** Display all user activity in the system, detailing which calls were accessed or exported.