Many health systems overlook call centers when implementing a clinical collaboration platform. Instead, the focus is on nurses, physicians and other clinical services over "ancillary" departments such as dietary, physical therapy or call centers. But call centers, whether on premise or an after-hours service, are often the heart of communication with clinical staff, especially when passing important patient health information to physicians.

Call center policies will normally state that patient information cannot be sent via unsecured platforms, but it is widely known that this is still happening. Employees at health systems want to be efficient and expedite patient care, so they often work around these policies.

Traditionally, on-premise call centers receive a call from a physician, nurse, or a family member and after-hour services from a patient, and the operators would either contact the doctor or intended recipient by calling her phone and speaking to her directly, which is HIPAA-compliant, or by paging her. The correct page would simply read something like, "You have a message, please contact the call center," but many operators send patient names, conditions and questions through the page in an effort to provide information in real-time. This is not HIPAA-compliant and could cost a health system thousands of dollars in fines.

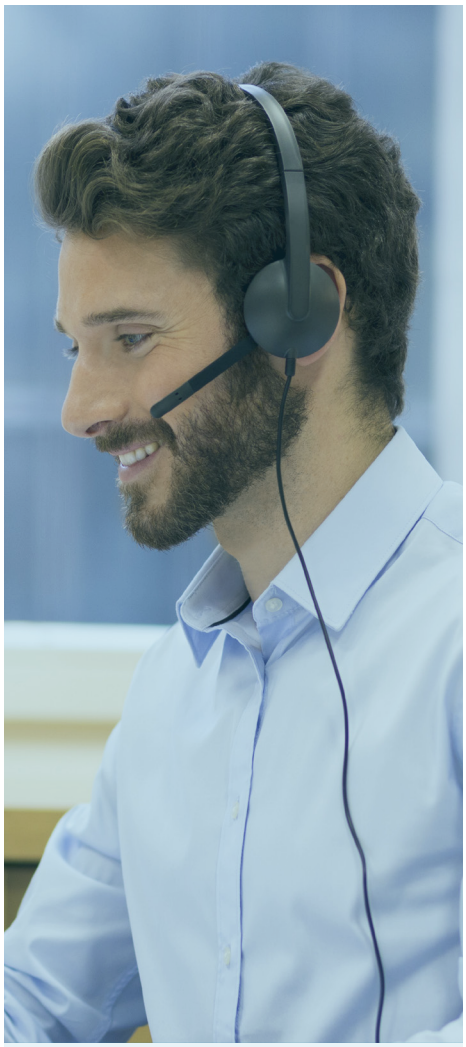
Why aren't pagers HIPAA-compliant? Paging messages are sent over specific radio frequencies, which can be easily intercepted and hacked. Because pagers were designed before the issue of cybersecurity, they were not set up to require encryption or authentication of any sort. As use of pagers begins to decrease in favor of smart devices – particularly with smartphones used by providers – texting has become the way to communicate. But unless physicians and call centers are using a secure clinical communication platform to facilitate these messages, they are out of compliance.

Why aren't pagers HIPAA-compliant? Paging messages are sent over specific radio frequencies, which can be easily intercepted and hacked.

Another consideration is that physician practices often choose their own after-hours call center services, which can result in the central health system dealing with many disparate call centers – some of whom are still using dial-up modems. One extreme example - a health system in Florida was using 40 separate call centers due to the number of provider offices working with them. The system was ultimately streamlined by placing all the call centers under the same clinical collaboration platform.

If your health system and clinicians want to convert from unsecured pagers to HIPAA-compliant messaging, look for a clinical collaboration platform that can address these kinds of issues by accepting pager information through legacy protocols and re-sending to a platform that encrypts and secures the messages.

Call centers know they are not HIPAA-compliant and are typically very receptive to using new technology to keep PHI safe. With the implementation of a system-wide clinical collaboration platform (including affiliated call centers), health systems have the opportunity to consolidate clinical communication vendors and ensure all of their communication is HIPAA-compliant.



Author

JON JANSEN
Chief Solutions Architect,
Halo Communications

Jon is responsible for integrating health system networks, particularly the critical areas of programming secure interfaces between hospitals, EMRs and clinician data. With more than two decades of experience in the secure healthcare communication arena, Jon is an important resource not only for the development of the platform, but for our Halo Customers as well.