



White Paper

Should Your Hospital Invest in a Secure Messaging App?

What's Inside

- ✓ **5 Reasons Hospitals Are Hesitant to Adopt a Secure Messaging Platform**
- ✓ **The ROI of Secure Messaging Apps**
- ✓ **Which Staff Benefit from Secure Messaging?**

Hospitals are often in a difficult spot when it comes to communication. While doctors and nurses desperately need the speed of instant messaging, the transition to secure messaging apps can be slowed by a combination of cost, technical hurdles, and human factors.

Amtelco launched its secure messaging app for healthcare in 2011. This white paper presents some helpful information for those who are considering an investment in a secure messaging platform.

There are five primary reasons hospitals are hesitant to adopt a secure messaging platform:

The "BYOD" (Bring Your Own Device) Dilemma

Some hospitals provide smartphones to staff members, and others have a BYOD policy. Asking clinicians to install a work app on their personal phones creates significant friction. Staff have privacy concerns and are often wary of "Big Brother" oversight or the hospital's ability to remotely wipe their personal devices if they are lost.

Staff are also concerned about the technical strains a secure messaging app could have on their personal data plan, or if the app quickly drains battery life due to backend processes such as encryption and syncing.

Hospital leadership may fear that using a secure messaging app introduces a new avenue of liability for the system should a doctor lose their personal phone containing the secure app. They want to avoid legal "HIPAA incident" investigations.

“

Our journey to Amtelco Secure Messages was driven by the HIPAA requirements for secured messaging. We started looking at all the tools that were available on the market and there were literally hundreds of them. We narrowed it down to what we thought looked like the five best for our organization. We created a vendor comparison grid and a team of people to look at all of the products. Amtelco's Secure Messages met all of our requirements.

”

Kathy Mealer, IS Manager for West Tennessee Healthcare

Integration and Data Silos

A secure messaging app is only useful if it integrates with other hospital systems. If the app doesn't sync with the electronic health record (EHR), clinicians must manually enter patient data, which is time-consuming and prone to error.

Hospitals have complex, shifting schedules. If the app isn't perfectly integrated with the hospital's on-call roster, critical messages might be sent to a doctor who is currently off-duty or in surgery.

Message Fatigue and Workflow Disruption

In a high-stress environment, more communication isn't always better communication. Constant alerts and non-urgent notification interruptions can lead to alarm fatigue and burnout among clinicians. Additionally, the expectation of immediacy creates real-time pressure. If a nurse sends a message and sees that it has been read, they expect an immediate response, which may not be possible if the doctor is attending to another patient.

Implementation Costs

While consumer apps like WhatsApp are free, a truly secure, HIPAA-compliant enterprise platform comes at a cost. There is usually a per-user subscription fee, and sometimes older hospital buildings require an upgrade to the facility's wireless network.

Strict Regulatory Compliance

An app must provide far more benefits than just encrypt messages. To be effective and genuinely compliant, it must also provide:

- **Audit trails** to ensure that every message is time-stamped, logged, and archived for years, supporting legal and medical record-keeping.
- **Remote disabling** in case a phone is lost or stolen.
- **Encrypted message storage** somewhere other than on the device.

A purpose-built secure messaging app for hospitals is designed to address these challenges and others commonly faced in the healthcare industry. Still, it's essential for systems to examine the return on investment (ROI) when considering a secure messaging app and be prepared to demonstrate why upgrading to secure messaging is a worthwhile investment.

“

We run reports using Amtelco Secure Messages fairly frequently, especially if somebody has a concern or expresses a need. For instance, our stroke program may request information about the Neuro alerts we've had in a particular month. We can run a report with that data, so it's very helpful.

Beth Wells, Executive Director of Patient Access and Information for Jackson-Madison County General Hospital in Jackson, Tennessee

”

The ROI of Secure Messaging Apps



There is substantial data on the ROI of secure messaging. For most hospitals, the investment is considered worth the cost. Software licenses remain an expense. However, the app's benefits often cover the system's installation cost within the first year. Afterwards, hospitals find that these benefits provide ongoing cost savings.

The ROI typically falls into three categories: Operational Efficiency, Risk Mitigation, and Revenue Recovery.

1. Reduced Length of Stay (LOS)

The most significant financial driver is how quickly patients can be discharged. When doctors, nurses, and transport staff communicate in real-time, the idle time between a doctor's discharge order and the patient actually leaving the building is slashed.

A [landmark study](#) at the University of Pennsylvania found that implementing secure text messaging for inpatient medical teams led to a significant reduction in the average length of stay (LOS) for patients (about 0.77 days or 14% relative decrease) but had no significant impact on 30-day readmission rates. This method of

communication helped streamline care, shortening hospital stays, without negatively affecting readmission rates, suggesting enhanced team coordination. This study demonstrates that when providers use smartphone-based secure messaging instead of older methods, such as paging, it reduces delays and improves patient flow and outcomes.

In the United States, the average cost of a day in the hospital is around \$3,025. This study demonstrates that a hospital with 10,000 annual admissions could save millions of dollars in capacity costs each year just by adopting a secure messaging platform.

2. Avoiding HIPAA Fines and Breaches

Hospitals are a primary target for cybercriminals, and human error is the leading cause of data leaks. The average cost of a healthcare data breach is now over \$10 million. A secure messaging app provides staff with an approved, HIPAA-compliant tool, helping healthcare organizations avoid falling into the shadow IT trap. Avoiding just one major HIPAA settlement for "unauthorized disclosure" could pay for a secure messaging platform for a decade.

3. Reducing Phone Tag

Clinicians spend a staggering amount of time simply trying to find each other. A study published in the Journal of Medical Internet Research found that nurses were the most frequent users of secure messaging (40 percent), followed by physicians (25 percent), and medical assistants (12 percent). Secure messaging reduced "response latency" (the time it takes for a person to reply) to a median of only 2.4 minutes, compared to much longer waits for paged call-backs.

For a nurse, saving time on phone tag allows them to focus on higher-value clinical tasks or handle a slightly higher patient load without increasing burnout.

4. Appointment "No-Shows"

Patient "no-shows" cost the U.S. healthcare system \$150 billion annually. Outpatient facilities and hospital-owned clinics will often use secure messaging for patient outreach. Secure SMS reminders have a 98% open rate, and most texts are read within minutes, making them an excellent way to send appointment reminders and engage with patients.

“

We were able to convince one site to start using Amtelco Secure Messages by just having one physician try out the app for a few days. This allowed them to see how easy it is to use and led to all of the physicians deciding to utilize it.

**Jamie Pineau, Owner of Debra's Medical Telemessaging
in Royal Oak, Michigan**

”

Secure messaging apps can pay for themselves. However, healthcare organizations need to avoid having tools that staff don't even use. If you're thinking about a secure messaging platform for your organization, consider how staff from various departments can use it to better manage workflows and patient flows.

Which Staff Benefit from Secure Messaging?



While almost everyone in a hospital benefits from faster communication, certain roles experience a dramatic shift in safety and efficiency when transitioning from traditional methods, such as pgers or sticky notes, to secure messaging apps.

The biggest winners are those in roles that require high-speed collaboration or the sharing of visual data. As stated earlier, **nurses** are the primary users of these apps, but secure messaging provides more than texting; they also send and receive encrypted audio, video, and photo files. In practice, a nurse may notice a patient's wound looks infected. Instead of describing it over the phone, they snap a secure photo and send it to the physician, who instantly sees it and can message back instructions to start IV antibiotics and provide an estimated time of when they will be there in person.

On-call physicians and specialists benefit most from role-based messaging, which routes texts to the person on-call rather than a specific name. It prevents messages from being sent to doctors who are off duty, and it allows specialists to review data (such as EKG strips) on their phones while moving between rooms.

For example, if an ER doctor needs a neurology consult for a potential stroke, instead of looking up the schedule and calling a cell number, they simply message the group labeled "@Neurology_On_Call." The app automatically alerts the right person on their preferred device.

“

Neuro alerts go out to every member of that team, including the CT staff and the Radiologists, using Amtelco Secure Messages.

Beth Wells, Executive Director of Patient Access and Information for Jackson-Madison County General Hospital in Jackson, Tennessee

”

Staff members, like **case managers and social workers**, handle complex logistics when getting a patient out of the hospital and into rehab or home care. They can coordinate with multiple departments (pharmacy, transport, physical therapy) in one group thread rather than making five separate phone calls.

In the real world, a social worker can start a group chat for a patient being discharged. They message the pharmacist for the home meds, the physical therapist for the walker, and the transport team for the ride home—all in one place to ensure nothing is forgotten.

Emergency response teams handle code situations, and every second counts. Secure messaging apps can broadcast STAT alerts that bypass do-not-disturb settings to ensure the entire response team is notified simultaneously.

If a "Code Blue" is triggered, the app sends a high-priority alert to the respiratory therapist, the ICU resident, and the crash-cart nurse. It provides critical links and information about the patient, so the team has the medical history before they even reach the room.

Non-physician staff working in ancillary services, such as the **lab, radiology, transport, and environmental services**, use these apps to clear bottlenecks that keep patients in hospital beds longer than necessary by automating the hand-off of critical results or tasks. When a patient is discharged, cleaning services can be alerted that a room needs to be cleaned to speed patient turnover.

A lab technician may perform a blood test that reveals a dangerously low potassium level. Instead of calling the unit and being put on hold, they send a critical result alert directly to the attending physician and receive a receipt verifying that the physician has seen the message.

Visit the Resources section of our website for more information about secure messaging. [Click here to learn about our Amtelco Secure Messages app.](#)

Please contact us with questions.

 800.356.9148

 amtelco.com

 info@amtelco.com

 4800 Curtin Drive
McFarland, WI 53558

amtelco