# Keeping Patient Health Information Safe with Secure Messaging

A Whitepaper by 1CALL

A Division of AMTELCO

Protecting electronic patient health information (ePHI) has become even more critical as the healthcare industry slowly transitions away from paper-based processes and into a more connected, electronic delivery model. Patient privacy and security is front and center in the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH).

That includes the transmission of patient information commonly shared via e-mail, text messages, and pagers at hospitals, clinics, and physician practices. Traditional approaches to messaging among healthcare providers often fail to meet the requirements of the current laws, leaving patient data vulnerable and providers liable for potential HIPAA violations. Healthcare providers need a messaging solution that is secure, accurate, reliable, and immediate, ensuring compliance and improving patient satisfaction.

The HIPAA Privacy Rule and HIPAA Security Rule address the technical and nontechnical safeguards that providers must have in place to secure ePHI, including the administrative, technical, and physical security procedures for ensuring the confidentiality, integrity, and availability of the data.

HITECH, which was passed in 2009 as part of the American Recovery and Reinvestment Act, contains specific incentives for information technology to be used in healthcare, widens the scope of privacy and security protections available under HIPAA, and increases the potential legal liability for noncompliance. Covered Entities (providers) and their Business Associates must comply with both sets of regulations and ensure that ePHI is protected in transit and at rest. Providers are expected to protect against reasonably anticipated threats to security and impermissible uses and disclosures. They also must ensure compliance with these procedures by their workforce. Failure to protect ePHI can result in extremely costly fines levied by the Office of Civil Rights (OCR). The OCR performs random audits of healthcare organizations and their business associates, and breaches can also be reported to them. According to a recent whitepaper from Protenus, a healthcare IT company specializing in protecting patient health data, breaches in the U.S. healthcare field cost $6.2 billion annually. The average HIPAA settlement fine is approximately $1.1 million and is increasing.

## Secure Messaging and the Clinical Decision Support System

Currently, many healthcare providers still rely on paging systems to send messages to staff members. But pagers are a 1950s technology that is quickly being phased out and rendered obsolete by smart device technology. That's why some hospitals have transitioned to SMS text messaging and e-mail, which staff members access on their mobile devices.

None of these communications methods are intrinsically secure. Pagers and mobile devices can be lost or left unattended, allowing unauthorized parties to access messages or e-mails. Even a doctor handing his phone to his son to play a game can potentially create a HIPAA violation if a patient-specific text is accessible on the device.

Providers are moving to consolidate devices to use a single, consistent messaging platform, and shifting away from pagers and other outdated technology and using secure, encrypted messaging solutions. An example of a secure messaging platform is miSecureMessages by AMTELCO's 1Call Division. miSecureMessages is a HIPAA and HITECH-compliant messaging application, which enables healthcare professionals to send fully encrypted messages to smart devices, ensuring privacy while leveraging technology that most physicians and staff already use. This technology can reduce costs, enhance service to patients, and improve the clinical decision support system (CDSS) in the process.

miSecureMessages sends and receives encrypted messages via smart devices and desktops. Clinical staff can send texts, photos, videos, and audio files securely. Recipients are notified about incoming messages via customizable, visual and audio alerts and can reply to an entire group or care team, just the person who sent the message, or someone else within the group. Busy staff can send quick phrases with a single touch or use the voice-to-text mode to speak a message into their device, which is then automatically converted into text. The app also provides a fully auditable record of all messages, as required by the Joint Commission.

The application issues a specific and persistent alert until the message is read, and can override the device's settings with custom visual and audio alerts so important messages are immediately recognized and responded to. If a user is unavailable, they can turn the app off in order to stop receipt of new notifications and their "off" status is indicated to anyone attempting to send them a message.

A passcode or fingerprint scan can be set as a requirement to open the app. If a mobile device is lost or stolen, a network administrator can deactivate the individual miSecureMessages license remotely. Messages themselves are never actually downloaded onto the device - ensuring they are secure. This protects patient data without requiring a complete remote wipe of the mobile device. This way, once the device is recovered, users still have access to all of their personal data and contacts and can begin using the secure messaging solution again.

The solution works on both cellular data and WiFi-based wireless networks, and provides an unlimited alphanumeric character display for messages, as well as an unlimited number of messages per user. Users can message colleagues directly (device to device), and even send messages to entire care teams.

## Improving Workflows

Secure messaging can improve hospital operations. For example, Capital Health in Halifax, Nova Scotia, is using the miSecureMessages app to enable a porter services application that has improved the efficiency of the hospital porters. Before, porters carried pagers. If someone needed a porter, they would call a central dispatch number to place an order. The dispatcher would write down the details and send a message to the pager. The porter would then call in to get those details.

Now, all of the details of the order can be sent directly to smart devices that have been issued to the porters. Those placing orders can enter their own notes, which has made the dispatch process more efficient. Porters can better organize their calls since they can see all the details of each order at once. The porters also are leveraging their devices to send messages to each other to better coordinate their activities. They are even using the built-in cameras to take photos of broken equipment.

Unlike traditional phone-based messaging solutions, the system does not send SMS text messages. The messages do not pass through a third-party cellular provider (which is the case with SMS texts), and there are no associated messaging fees. The solution simply pushes out notifications that messages have been received. The messages themselves live only on the server and never pass onto the device.

miSecureMessages can be installed behind the corporate firewall, an option that is appealing to those organizations that want to maintain more control over data transmission and storage. It also can be deployed as a 100 percent cloud-based solution. The latter option can save time, cost, and labor hours that would otherwise be dedicated to deployment and support of the solution and its associated server.

## Reduce Costs and Improve Patient Care

Hospitals lose on average $8.3 billion each year due to using pagers and other outdated technologies (Ponemon Institute). Secure messaging can reduce the cost of hospital communications. Clinicians can get rid of their pagers and use their smart phones and tablets (devices they likely already carry) to manage work-related communications, which further reduces the cost of IT and administrative support for multiple devices. The average cost of a wide-area pager is approximately $9/month per user, and if an organization is using a two-way paging system, the cost is even higher. Compare that to the lower cost of

miSecureMessages, which not only provides two-way messaging as part of the base solution but also allows users to message more than 100 recipients simultaneously.

Because detailed information is available in the secure messages, hospitals can even reduce the amount of overhead paging in the care environment, reducing "noise pollution" levels and improving conditions for both patients and staff.

Secure messaging also improves messaging response times. One customer pilot study found that with traditional paging, it took an average of 2.5 minutes to send a message and obtain a response from the recipient. Using miSecureMessages, the same process took just 34 seconds. If a typical hospital sends out 2,000 pages per day, that would be nearly 67 staff hours per day in saved time, or more than 24,000 hours per year. At an average hospital wage of $20/hour, that could lead to nearly $0.5 million dollars per year in labor savings. That total increases to over $1 million of savings annually when the result of reduced patient discharge times is also factored in.

Faster responses also mean that patient-related issues are handled more efficiently, without the need for time-consuming phone calls and

note taking. Doctors can spend more time with their patients and reduce patient discharge time by 50 minutes (Ponemon Institute). The miSecureMessages app can be integrated with existing database solutions to improve access to EMR, decision support tools, and medical references.

## The Future of Secure Messaging

The adoption of new healthcare technology is only going to accelerate. Ensuring that ePHI is secure and private will be an increasingly important and challenging task. Hospitals and other healthcare providers that want to move away from outdated and costly paging solutions have had limited alternative options. Many rely on SMS text messaging or e-mail solutions that are unencrypted, vulnerable to data breaches, and don't really provide efficiency or operational improvements over the paging systems they are replacing.

Secure messaging provides a secure, fully encrypted replacement for traditional paging and enables new functionality that can improve patient care, streamline messaging procedures, improve productivity, and reduce costs.

## About 1Call

The 1Call Division of AMTELCO specializes in offering enterprise-wide communication solutions for healthcare organizations. AMTELCO, 1Call's parent company, has been a leading provider of innovative communication applications since 1976. AMTELCO has its roots in the early 1950s when its founder, William J. Curtin, invented and patented solutions for his call center. With AMTELCO systems currently in operation in all 50 of the United States, and in more than 20 foreign countries, AMTELCO customers process millions of calls each month. AMTELCO is well-known in various industries for continually developing innovative solutions designed to streamline communications, all backed by AMTELCO's superior 5-star service and support.

For more information on miSecureMessages, call **800.225.6035**, send an e-mail to **info@1call.com**, or visit **1call.com**.