amtelco

White Paper

Protecting Clinical Data and Streamlining Workflows with Secure Messaging

What's Inside

- **The True Cost of Healthcare Data Breaches**
- **Moving Beyond Legacy Paging Technology**
- **Improving Clinical Workflows: Orderlies and Patient Transport**
- **Reducing Noise Pollution and Elevating Patient Care**

One customer pilot study demonstrated traditional paging took an average of **2.5 minutes** to send an alert and receive a phone response, but secure messaging took only **34 seconds**. This time savings could return hundreds of thousands of dollars in direct clinical labour back to the organization.

Nick Evans
Regional Sales Manager for Australia
Ph: +61 2 5017 9925

amtelco.com nevans@amtelco.com

As the Australian healthcare sector continues to move away from legacy paper-based workflows toward fully integrated, digital care models, protecting Electronic Personal Health Information (ePHI) has never been more critical. Patient privacy and data security sit at the absolute centre of the Privacy Act 1988 and the Australian Privacy Principles (APPs).

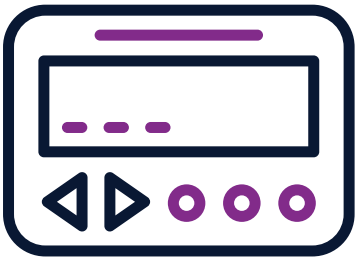
Traditional messaging methods among healthcare providers—such as standard SMS or unencrypted emails—frequently fail to meet these strict regulatory standards. This leaves highly sensitive patient data vulnerable and exposes healthcare networks to severe compliance violations, mandatory data breach reporting, and significant reputational damage. Under local regulations, digital health providers are expected to proactively safeguard against anticipated security threats, govern data access strictly, and ensure that their entire workforce complies with secure communication protocols.

The True Cost of Healthcare Data Breaches

Cybercriminals increasingly target the healthcare sector because a medical record contains permanent, high-value identity and clinical data that cannot simply be cancelled or replaced like a credit card number. Recent high-profile cyberattacks across Australia have highlighted how vulnerable the industry is. Beyond the immediate threat to patient trust, the financial fallout of an Australian healthcare data breach is staggering, often running into millions of dollars in containment, legal fees, regulatory penalties, and operational downtime.

To mitigate these risks, healthcare organizations require modern communication solutions that are secure, immediate, and fully auditable, ensuring total compliance while actively improving clinical outcomes.

> From a patient safety standpoint, Amtelco Secure Messages has been a very positive change. It plugs a hole in a common communication gap because you have documentation that the recipient did indeed receive your message. **Beth Wells, Executive Director of Patient Access and Information (Customer quote from an Amtelco case study with Jackson-Madison County General Hospital in Jackson, Tennessee)**



Moving Beyond Legacy Paging Technology

Many Australian hospitals still rely heavily on traditional pocket pagers to alert staff. While pagers were a staple of 20th-century medicine, they are inherently unsecure, one-way, and rapidly becoming obsolete in an era dominated by smart device technology. In response, some facilities have permitted the use of standard mobile SMS or commercial chat apps.

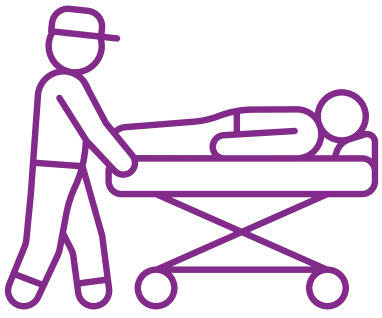
[Related White Paper: Modernizing On-Call Workflows with Integrated, Secure Messaging]

However, these consumer-grade methods introduce severe vulnerabilities:

- Pagers and personal mobiles can be left unattended or intercepted, allowing unauthorised parties to view clinical alerts.
- Standard SMS lacks end-to-end encryption, meaning data is stored vulnerably on telecom servers.
- A clinician accidentally exposing patient-specific text messages to a family member or third party on a personal device can trigger a reportable privacy breach.

To resolve this, forward-thinking health districts are consolidating communication infrastructure into a single, encrypted messaging platform, completely phasing out outdated pocket pagers.

Improving Clinical Workflows: Orderlies and Patient Transport



The operational benefits of secure messaging extend across the entire hospital enterprise. For instance, a prominent healthcare facility recently replaced pocket pagers with the Amtelco platform to optimise their patient transport and orderly workflows.

Previously, ward staff called a central dispatch desk to request an orderly. The dispatcher wrote down the details and sent a basic alert to a pager, requiring the

orderly to stop what they were doing and find a landline to call in for the full details.

Today, the entire job order is sent directly to the orderly's smart device. Ward staff enter specific patient notes directly into the system, making dispatch seamless. Orderlies can better coordinate tasks with colleagues via peer-to-peer messaging, and even use the device camera to instantly report broken ward equipment to maintenance.

Reducing Noise Pollution and Elevating Patient Care

Outdated communication infrastructure costs hospitals millions annually in lost productivity and administrative friction. Transitioning to secure messaging delivers immediate financial and clinical dividends:

1. Eliminating Pager Overheads
Phasing out wide-area pager rentals and complex two-way paging networks significantly reduces ongoing IT support costs. Amtelco Secure Messages offers superior two-way and group communication capabilities as a baseline, without the heavy infrastructure costs.

2. Reducing Hospital "Noise Pollution"
Because detailed, specific data is delivered directly to the appropriate clinician's pocket, hospitals can dramatically decrease the use of overhead public address paging. This creates a quieter, more therapeutic environment for healing and reduces alarm fatigue for clinical staff.

3. Accelerated Response Times
One customer pilot study demonstrated the sheer efficiency of Amtelco Secure Messages. While traditional paging took an average of **2.5 minutes** to send an alert and receive a phone response, Amtelco's secure messaging process took just **34 seconds**.

For a typical hospital dispatching 2,000 alerts a day, this workflow acceleration saves approximately **67 staff hours per day**—or more than **24,000 hours annually**. This returns hundreds of thousands of dollars in direct clinical labour back to the organization.

When factored alongside optimized patient discharge workflows (with doctors reducing discharge bottlenecks by nearly an hour through instant communication), the annual operational savings quickly scale.

Amtelco Secure Messages: Purpose-Built for Healthcare

Amtelco Secure Messages is a fully encrypted, secure communication application. It enables healthcare professionals to send secure, rich-media messages to smart devices and desktops, leveraging the technology that clinicians and staff already use every day.

By integrating this platform, hospitals can drive down IT costs, elevate patient care, and significantly enhance Clinical Decision Support Systems (CDSS).

Key Features of the Platform:

- **Rich-Media Capabilities**: Clinical teams can securely share texts, photos, clinical images, videos, and audio files without saving media to the device's local gallery.
- **Dynamic Care Team Communication**: Recipients receive customisable visual and audio alerts and can instantly reply to an entire care team, a specific rostered group, or an individual colleague.
- **Designed for Busy Wards**: Staff can send pre-configured quick phrases with a single touch or use advanced voice-to-text functionality to dictate messages on the move.
- **Clinical Governance**: The app maintains a fully auditable trail of all communications, aligning with national digital health standards for tracking clinical handovers.
- **Persistent Alerting and Status Controls**: Important alerts will persistently notify a user until read, capable of overriding silent device settings for high-priority clinical events. If a clinician is off-shift, they can toggle the app off, immediately indicating their unavailable status to the rest of the network.
- **Zero-Downtime Remote Security**: Access can require a passcode, fingerprint, or facial recognition. If a device is lost or stolen, administrators can remotely deactivate the app license. Because messages are hosted securely and never downloaded onto the physical hardware, patient data is protected without requiring a destructive remote wipe of the employee's personal phone.

The Future of Connected Care

The acceleration of digital health adoption across Australia shows no signs of slowing down. Ensuring that ePHI remains perfectly secure while keeping clinical workflows fluid is a major priority for hospital executives.

Contact Nick Evans at +61 2 5017 9925 or nevans@amtelco.com to learn how replacing expensive, obsolete paging systems with an intelligent, encrypted messaging application, healthcare networks can successfully bridge the gap between absolute data security and peak operational efficiency.

Please contact us with questions.

amtelco.com

nevans@amtelco.com

Nick Evans, Regional Sales Manager for Australia
Ph: +61 2 5017 9925

amtelco