AT&T Business

Enable highly secure patient-staff communications with solutions from AT&T Business Messaging

To get started, contact **888.318.1620**

Every day, sensitive healthcare information is exchanged. The alarming truth is that healthcare privacy breaches are more common than one may think. With costs on the rise and patient data at risk, the healthcare sector must look closely for ways to better transmit sensitive information using highly secure communications.

Did you know?

According to a recent survey, 9 in 10 health-care systems plan significant investments in smartphones and secure unified communications over the next 12 to 18 months.

Source: *Spyglass Consulting*

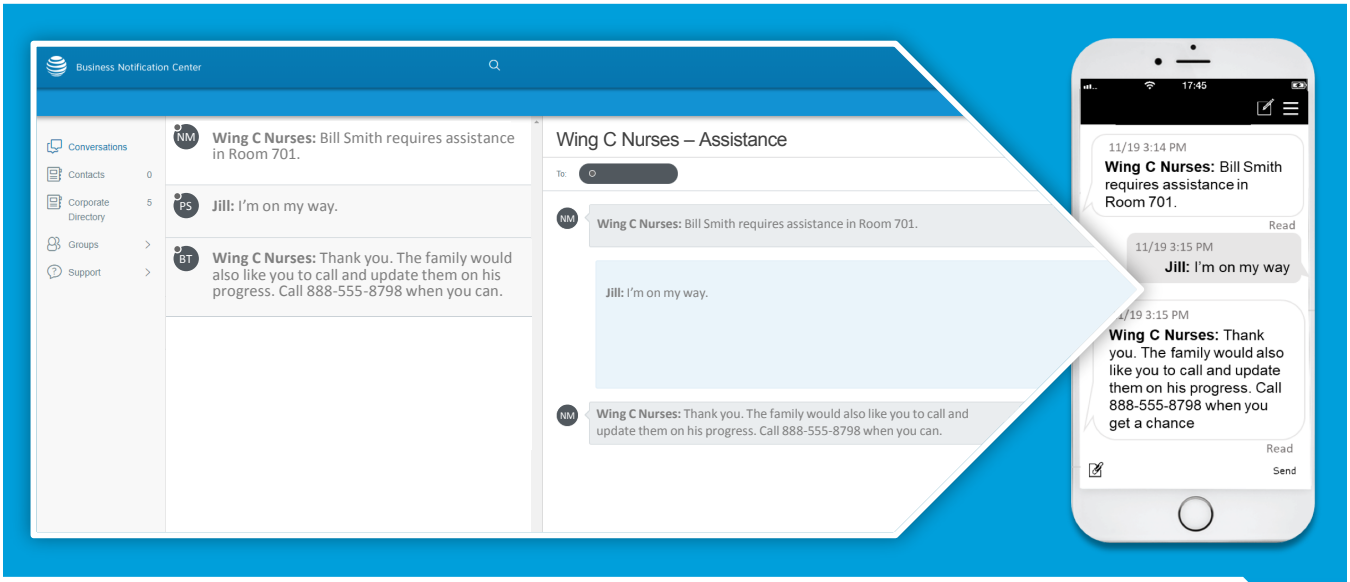
A highly secure, HIPAA-compliant, employee messaging solution*

- Wait time update
- Patient flows.
- Surgery scheduling
- Care management
- Medication management
- Hospital emergency alerts
- Mass employee notifications

*Users must apply HIPAA-compliant encryption and agree to the AT&T Business Associate Agreement at www.att.com/businessassociateagreement.

Key Benefits:

- **Gives users instant access to the organization's directory, allowing staff to communicate with individuals or groups via encrypted text, image, and video messages.**
- **Enables mobile clinicians to easily message the correct person.**
- **Replaces pagers to improve business processes.**



Product features

- Users can encrypt messages and file attachments for encryption at rest, in transit, and on mobile devices
- Message smaller work groups or broadcast company-wide messages
- Chat functionality for up to 20,000 contacts
- Message history storage
- File, photo, voice memo, and video attachments up to 5 MB
- Sent, delivered, and read confirmations
- Up to 100 custom group distribution lists
- Private or public distribution lists
- Location and contact sharing
- Push notifications enabled for near-real-time updates
- Apps for Android and iOS handsets and tablets

Additional security features

- **Security:** TLS encrypted data channel
- **Message content security:** AES – 256 encrypted unique keys for each message
- **Highly secure key management:** RSA 2048-bit encrypted keys provide asymmetric encryption with unique keys for each device

  4-digit PIN is required for mobile app access
- **Remote wipe:** Remotely wipe IP conversations
- **Message expiration:** Delete IP messages after pre-defined period of time
- **Prohibit copy/paste:** Cannot copy or paste to or from the app