HIPAA COMPLIANCE

A phone system or service is neither HIPAA compliant or not. Like all of your medical office equipment: Policy, procedure, and usage defines it's compliance. Ring-u's Hello Hub and Secure VoIP service is specifically designed and implemented to make HIPAA compliance practical.

Secure communications

All VoIP traffic is encoded and encrypted as far in and out of the call as possible. The other end of the call may not be. A call to standard “POTS” or mobile telephone will not be encrypted on it's end. Ring-u and it's upstream partner providers use the SRTP (Secure Real Time Protocol) and TLS (Transport Layer Security) protocols for all calls from the Hello Hub to the external networks.

Local Storage

Other than call detail records (CDR) used for billing, ring-u and it's upstream providers do not store any data. Ring-u and it's upstream providers do not record phone calls, store faxes, or store voicemail on their systems. **All confidential patient and business data is stored on the Hello Hub at your facility.** If a USB drive is attached, all recorded calls, voicemails, and faxes are stored on the USB drive. Ring-u staff does not have access to that data at your location.

Voicemail/fax to e-mail

If the Hello Hub is configured to convert voicemail and faxes to email, the Hello Hub will transport those emails using TLS (Transport Layer Security) v 1.2 to the receiving mail server. If your email server is considered HIPAA compliant, this function is also HIPAA compatible. **If your email server is not using TLS 1.2, or you are not sure, do not configure your Hello Hub to send voicemails or fax via email.** They can be retrieved locally via the phone or via the web interface.

Access/Audit Logs

The ring-u control interface logs all access and what a client does when logged in. These logs are available via the reporting interface. It is the clients responsibility to check those logs and make sure the system access is apropos to the clients policies and procedures. The current ring-u control interface only has one set of credentials, and is not typically used by office staff on a daily basis.

Addressing Lore

There is no reason VoIP is or is not HIPAA compliant. It is at least as secure as a “POTS” (Plain Old Telephone Service) or any digital (T1/PRI/ISDN) delivery method, and **in most cases VoIP is much more secure**. This is false lore spread by non-VoIP providers. In 2019+ almost all phone traffic is packetized, digitized and VoIP in transport over the public internet at some point.

Fax is not expressly HIPAA compliant. Fax is a 1920's analog protocol that on an analog phone line can be recorded, tapped and replayed. Doing Fax over VoIP using SRTP and TLS encrypted T38 digital transport makes it as secure as practical, as far as possible. The other end may be using plain old phone lines. Password controlled PDF's, encrypted emails and secure web interfaces are much more secure and practical.

If your location has a JCAHO, HHS or other audit, ring-u staff will gladly assist you with answering your auditors questions.

References

- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- https://www.hhs.gov/hipaa/for-professionals/faq/482/does-hipaa-permit-a-doctor-to-share-patient-information-for-treatment-over-the-phone/index.html