Health Information Compliance Alert

It's More Than Just Chit Chat: 7 Things to Look For in a Texting App

We take texting for granted, often forgetting that SMS isn't secure. Frequently, we share usernames, passwords, contact lists, information, and phone numbers without thinking of the consequences.

Not every practice employee is a covered entity, but despite this fact, many groups forget about HIPAA rules on who can and cannot have access to PHI and ePHI. As a safeguard against unlawful access and common texting errors, it's wise to invest in apps for your practice portables that protect you, your staff, and your patients.

Here are seven things **Michael DeFranco**, founder and CEO of Lua suggests practices have set up before they add texting to their office dynamic:

- Eliminate the threat of sensitive data being compromised if a mobile device is stolen or lost with message recall, message lifespan, and remote wipe.
- Segregate healthcare texting from personal texting through a HIPAA-compliant, secure application.
- Encrypt message data in-network and in-transit on the device and the server.
- Look for a lockout feature that erases data remotely if devices are stolen.
- Require PIN authentication for all application users.
- Include configurable time-out periods.
- Block users after a number of unsuccessful authentication attempts.