HIPAA and Digital Communication

Yes, you can text, email or communicate with your patients on social media. Here's what you need to do first:

- Warn your patients of the risk associated with transferring or storing their Electronic Protected Health Information (ePHI) through an unsecure means.
- Obtain consent either verbally, through Rhinogram, or in your HIPAA Policy & Authorization Form, and document the patient's consent decision in Rhinogram!
- Give them a choice! Your patients have the right to choose the means by which they communicate with your office.
- Allow patients to opt out of said communications and document their decision.
- Take reasonable measures to securely transmit and store ePHI like conversations in Rhinogram.

What if patients send me ePHI before I get their consent?

Patients can disclose ePHI in any way they choose. According to HIPAA law, it is how you return communications that could be a violation. As a provider, you must communicate with patients through whichever channel of communication they choose, but ensure you obtain consent before moving forward with a conversation after they've initiated it.

What about Appointment Reminders? Do they require consent?

No, according to HHS, you do not have to obtain consent to discuss appointments with patients via text message. They do not consider this a violation.

Is it okay for me to text my colleagues the same way I text my patients?

Providers are allowed to share PHI for treatment purposes without patient consent, as long as reasonable safeguards are in place to do so. That means you must store and transmit that ePHI safely via Rhinogram or another secure platform.

What measures does Rhinogram employ to secure patient data?

Rhinogram takes security and privacy seriously. Our Security, Risk, and Compliance Teams ensure our operating policies adhere to HIPAA and evolve with the constant change in technology. Our Production Operations and Engineering routinely monitor and perform penetration testing. We also employ NIST and OWASP standards for password protection, security, and encryption.

Do I need to encrypt any device I use to store or transmit ePHI?

Yes, you must ensure all devices you use to store or transmit ePHI are encrypted. Since Rhinogram can be used on any device that has access to the internet, you'll need to insure all devices connected to Rhinogram are protected. You can learn more about protecting mobile devices here.