HIPAA Email Compliance Cheat Sheet

This is an extra resource to go along with the original article:
Are Your Emails HIPAA Compliant? Here's How to Be Sure

Here is a quick guide to help you stay HIPAA compliant with your internal and external emails.

1. Get (Documented) Patient Consent to Use Email

HIPAA's Omnibus Rule states that "covered entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk, and the individual still prefers the unencrypted email."

In short, unencrypted emails are not encouraged, but they can still be used if you have the patient's documented consent to using email. According to HIPAA's privacy rules, if a patient contacts you via email first, consent is automatically given.

In all other situations, you must ask for consent to send emails to patients.

2. Double Check Your Email Provider's Security

Many leading email providers are becoming more HIPAA compliant, but it's never safe to assume that they're fully secure. You should always double check.

Gmail, for example, does use compliant technologies, but in some cases Gmail messages can't be encrypted (as stated in Google's safety report, which shows that 10% of all its emails are still vulnerable), in which case email messages are not compliant.

Unless you already know that your email provider is HIPAA compliant, assume they're not.

3. Use HIPAA Best Practices for Internal Emails

Just as staff shouldn't leave sensitive data lying around the office (open patient files on a computer or on a desk, passwords on sticky notes around computers, etc.), staff should also avoid sharing patient information via email to each other.

Communication through an electronic healthcare system (EHR/EMR) by leaving patient notes or through a private (encrypted) chat channel, or even via phone, is often preferable.

Consider how "office chat" can impact patient privacy when communicating between staff members, administrators and practitioners.

4. Understand How Third Party Vendors Fit Into HIPAA

HIPAA has its own coding system for any third party involved with patient data, called "business associates." A business associate is anyone who "creates, receives, maintains, or transmits" patient data.

It's essential that you have a written agreement with any business associate (called a "business associate agreement") to ensure that they do not use unsecured email to communicate with members of your staff or with the patients directly.

Signing an agreement isn't a guarantee that a third party is or will remain HIPAA compliant, so be sure to monitor any unusual behavior and to stay on top of your own HIPAA compliance best practices.

5. Use Alternative Communication Methods That are More Secure

It's important to understand that many of the technical safeguards specified in the HIPAA Security Rule are not required, but rather encouraged. In other words, there is flexibility with your communication preferences.

However, patient privacy is the most important component when it comes to communication. If you're not sure that your email provider or staff can't remain HIPAA compliant, use another form of communication.

Most electronic healthcare systems have secure communication options to use in place of email, which are already encrypted for patient privacy.

Having patients (who don't state a communication preference) call or communicate via a patient portal rather than using email is another way to maintain privacy without worrying about every single email being compliant.