

Health Information Compliance Alert

Security: Are You Taking The Right Steps To Protect Your E-mail PHI?

Document patient consent for e-mail messages and keep this on file, experts advise.

If your medical office uses e-mail as a form of communication with patients, you could be risking protected health information (PHI) violations if you're not taking all the right precautions.

E-mail does make your communications with patients much easier since a message shot through cyberspace reaches the intended recipient faster than phone calls and letters.

However, the convenience and speed of e-mail comes with a price: someone other than the patient could read the e-mail and spread the word about sensitive medical conditions, such as HIV test results or malignancies.

Our experts offer advice on putting controls in place to safeguard PHI before sending any e-mails to patients.

Reduce Risks With E-mail Routine

A medical office employee should follow a few simple rules for every single e-mail she sends, regardless of whether the recipient is a patient, vendor or insurance rep, advises **Gwen Hughes** with **Care Communications** in Chicago. That way, you will be sure to protect sensitive information whenever it pops up in an e-mail.

Before you send an e-mail from your medical office, Hughes recommends:

- checking for encryption software. You should protect each message with some sort of guard against hackers.
- putting a confidentiality disclaimer at the end of the office e-mail template. If you are stuck on how to begin your generic e-mail confidentiality disclaimer, see "Craft Your Own E-mail Disclaimer: Here's How" in this issue.
- asking the patient if he understands the concept of e-mail. Even some people with e-mail accounts (especially older patients) will have trouble with the intricacies of e-mail. Don't assume that patients know how e-mail works.
- be trained in e-mail PHI. If you don't know how to protect patient PHI in e-mails, you're better off having someone else send the message.
- forward patient-identifiable information to a third party **only if** you have the patient's authorization to do so.

You should never e-mail extra-sensitive PHI, warns Hughes. There are some things you should not print in an e-mail, such as the results of an HIV test, messages relating to psychiatric illness, substance abuse, and domestic violence.

Exactly what types of info are too sensitive to e-mail will depend on the practice. If you're unsure about a piece of info, it's worth checking with a doctor or nurse to see if you should be e-mailing it.

Hard Copies Provide Solid Evidence

Print a hard copy (or save a separate computer file) of each patient-office e-mail you send. That's the most practical method of protecting the office's interests when sending e-mails. Then, if there is any question about an email, you can easily reference it.

"E-mail that contains clinical information about patients should be stored (electronically or in hard copy) in the patient's medical record. This is extremely important and fairly easy to do with e-mail," says **Daniel Z. Sands, MD, MPH**, of **Beth Israel Deaconess Medical Center & Harvard Medical School**.

Patient Must Be Informed Of E-mail Risks

So what should a staffer do if a patient asks her to e-mail information that is considered PHI-sensitive? Before hitting "send" on the e-mail, the employee is obligated to explain the risks of sending the e-mail to patients.

"A staff member and/or physician needs to discuss risks of using insecure e-mail for communicating PHI to the patient," explains Sands. The risks include others reading the message, either intentionally or unintentionally, through misaddressing, interception, shared e-mail accounts, and employer-owned e-mail systems."

Also, the office must tell the patient that all e-mails between patient and office will become part of the patient's record.

Best practice: Once the patient agrees and consents to all the e-mail conditions, document this agreement and consent in the patient record.

You may choose to have a contract/consent form signed with a copy to the patient and copy for the record. "Patients should also be asked to save copies of all messages from the office," says Sands.