

Legal Q/A

Bruce E. Wood, Esquire

Q: *What are the HIPAA requirements if I want to communicate with my patients via e-mail?*

A: E-mail communication between physicians and patients is moving into the mainstream of the practice of medicine. A recent survey shows that almost 40% of patients would pay for this access if security and privacy were guaranteed, and would change doctors to be able to send secure e-mail to their own doctor. But concern about the legal risks of transmitting confidential patient information through cyberspace has made many physicians wary of using the new technology.

Online communications can be used for routine matters, such as scheduling appointments and renewing prescriptions, to more clinically related matters such as treatment progress notes from patients.

Contrary to popular belief, interception of e-mail messages is not the greatest concern. It is the risk that unauthorized persons will read sensitive messages at home or work, or that the physician will send the message to the wrong patient by mistake.

The fundamental tenets of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are informed patient consent and the privacy of protected health information (PHI). Physicians are used to having patients sign consent forms for the release of PHI as a matter of course. The standard consent forms, however, may not be adequate to address the unique risks of e-mail communications.

We recommend the use of a separate written consent form that specifically deals with e-mail communications. The form should clearly spell out the appropriate use and limitations of e-mail and the potential privacy risks associated with the online communication of sensitive medical subjects, including the difficulty of validating the identity of parties and delays in responses. The physician bears responsibility for the proper sending of the e-mail communication (e.g., correct name and e-mail address of the patient), but the patient should take responsibility for who may ultimately read those messages and absolve the physician from liability if they are read by anyone other than the patient. The physician should refuse to communicate electronically with any patient that is unwilling to sign an appropriate consent form.

The HIPAA Security and Privacy Rules require that covered health care providers apply reasonable safeguards when making these communications to protect the information from inappropriate use or disclosure. Covered entities must perform a risk analysis and then determine the level of e-mail security that is needed. HIPAA doesn't technically mandate the use of encryption for electronically transmitted PHI, allowing the use of reasonable and appropriate alternatives, but since most experts feel there are no practical alternatives for open systems such as the Internet, for all intents and purposes encryption and authentication are required. Encryption is also recommended by the eRisk Working Group for Healthcare and Medem, an Internet company founded by the AMA and medical specialty societies to address issues surrounding electronic communications.

There are essentially two alternatives for encrypting e-mail messages -

encryption software or a secure web based messaging service. Encryption software, such as Pretty Good Privacy (only pretty good?) is available by download, but suffers from the drawback that both the physician and patient must have the same encryption software.

Companies such as Healinx, MDhub Medem, and Medscape offer subscription services that enable physicians and patients to exchange messages on a secure Web site. The message is encrypted when it's sent and the recipient needs a log on and password to decrypt it. Since the message never leaves the server of the Web site, it cannot be intercepted.

Bruce E. Wood is a corporate and health care attorney with the Syracuse-based law firm of Wood & Smith, P.C. and can be contacted at (315) 423-0400 or at bwood@woodsmithlaw.com.