When you read this article’s title “Patient Information Sent Through Unencrypted Email,” the HIPAA policeman inside you probably yells “NO!” However, through the changes to HIPAA released in the HITECH OMNIBUS regulations, patients can now request that their patient information be sent via email, even if it is unencrypted.

Let’s review the HIPAA standards for encryption and email. The HIPAA Security Rule is: **ENCRYPTION AND DECRYPTION (A)**

- § 164.312(a)(2)(iv) Covered Entities must “Implement a mechanism to encrypt and decrypt electronic protected health information.” This includes personal health information (PHI) sent via email.

However, in the HIPAA Privacy Rule, it allows **Standard: Confidential communications requirements.**

(i) A covered health care provider must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of protected health information from the covered health care provider by alternative means or at alternative locations.

Based on recent guidance from the U.S. Department of Health & Human Services and the HIPAA OMNIBUS FINAL RULE - We clarify 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 ... If individuals are notified of the risks and still prefer unencrypted email, the individual has the right to receive protected health information in that way, and covered entities are not responsible for unauthorized access of protected health information while in transmission to the individual based on the individual’s request. Further, covered entities are not responsible for safeguarding information once delivered to the individual.

As long as the covered entity is using a secure email system, the HIPAA Omnibus Rule says that if a patient asks you to send them information at a Gmail, Yahoo! Mail, Hotmail (or similar) account, you should inform them that their system is not secure and ask if they still want the information sent to them. If they say yes, it is HIPAA compliant to do this. Be sure you document your conversation and their approval. An easy way to document this is to include a statement on the authorization to release patient information form.

OCR’s website has posted several questions and answers about using email with patients.
Does the HIPAA Privacy Rule permit health care providers to use email to discuss health issues and treatment with their patients?

Yes. The Privacy Rule allows covered health care providers to communicate electronically, such as through email, with their patients, provided they apply reasonable safeguards when doing so. See 45 C.F.R. § 164.530(c). For example, certain precautions may need to be taken when using email to avoid unintentional disclosures, such as checking the email address for accuracy before sending, or sending an email alert to the patient for address confirmation prior to sending the message. Further, while the Privacy Rule does not prohibit the use of unencrypted email for treatment-related communications between health care providers and patients, other safeguards should be applied to reasonably protect privacy, such as limiting the amount or type of information disclosed through the unencrypted email. In addition, covered entities will want to ensure that any transmission of electronic protected health information is in compliance with the HIPAA Security Rule requirements at 45 C.F.R. Part 164, Subpart C.

Note that an individual has the right under the Privacy Rule to request and have a covered health care provider communicate with him or her by alternative means or at alternative locations, if reasonable. See 45 C.F.R. § 164.522(b). For example, a health care provider should accommodate an individual’s request to receive appointment reminders via email, rather than on a postcard, if email is a reasonable, alternative means for that provider to communicate with the patient. By the same token, however, if the use of unencrypted email is unacceptable to a patient who requests confidential communications, other means of communicating with the patient, such as by more secure electronic methods, or by mail or telephone, should be offered and accommodated.

Patients may initiate communications with a provider using email. If this situation occurs, the health care provider can assume (unless the patient has explicitly stated otherwise) that email communications are acceptable to the individual. If the provider feels the patient may not be aware of the possible risks of using unencrypted email, or has concerns about potential liability, the provider can alert the patient of those risks, and let the patient decide whether to continue email communications.

Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the internet? If so, what protections must be applied?

The Security Rule does not expressly prohibit the use of email for sending e-PHI. However, the standards for access control (45 CFR § 164.312(a)), integrity (45 CFR § 164.312(c)(1)), and transmission security (45 CFR § 164.312(e)(1)) require covered entities to implement policies and procedures to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security(§ 164.312(e)) also includes addressable specifications for integrity controls and encryption. This means that the covered entity must assess its use of open networks, identify the available and appropriate means to protect e-PHI as it is transmitted, select a solution, and document the decision. The Security Rule allows e-PHI to be sent over an electronic open network as long as it is adequately protected.

For more information about this issue of AFMC HealthIT HIPAAwatch, please visit afmc.org/healthit, email healthit@afmc.org or call 501-212-8616.