Electronic Protected Health Information and Patient Communications

By Beth Christian and Kurt Anderson

Giordano, Halleran & Ciesla, Attorneys at Law

Electronic recordkeeping and communication tools are a fact of life for every modern medical practice. You may be considering, or may already have implemented, electronic communications with your patients. This article will set forth some of the things that you should consider in implementing an electronic communication process for your practice that is compliant with HIPAA as well as some of the requirements for other electronic protected health information ('EPHI').

Question #1: Does HIPAA allow health care providers to use email with their patients?

Health care providers are permitted to communicate electronically (such as through email) with their patients, as long as they apply reasonable safeguards when doing so. If your practice will use email to transmit EPHI, it must ensure that the transmission is compliant with HIPAA technical safeguards, discussed below. Alternatively, you may limit email communications to out-bound communications only, such as practice announcements, general health education information, or appointment reminders.

Even if no EPHI is communicated by email, you should take measures to avoid unintended disclosures. You may want to send a test email to the patient for address confirmation. While HIPAA doesnit prohibit the use of unencrypted email with patients, safeguards should be applied to protect patient privacy, such as limiting the amount or type of information disclosed in the unencrypted email.

Patient preferences should also be respected. An individual has the right under HIPAA to request that you communicate by email if it would be reasonable for the health care provider to do so. Conversely, if a patient does not want information sent via unencrypted email, other means of communication must be used (e.g., phone, mail or encrypted email).

If you do not want patients to send e-mail messages to you, you should include a disclaimer at the bottom of each e-mail which states that the sending e-mail address is only used to send messages, that incoming e-mail is not regularly monitored at that e-mail address, and that patients should call your office if they have any questions or health concerns. Consider also whether you will use text messaging with patients or communicate with them via Facebook or Twitter. While, publicly posting EPHI to a social media platform is clearly problematic, as platforms like Facebook and Twitter add private messaging capability, they begin to function more like traditional email platforms (e.g., Gmail, Yahoo, AOL).

Question #2: What types of administrative safeguards should my practice implement in order to protect EPHI?

HIPAA requires that health care providers implement administrative safeguards in order to secure EPHI. Administrative safeguards are 'administrative actions, policies, and procedures to manage the selection, development, implementation and maintenance of security measures to protect EPHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.' A practice must conduct an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI. The practice must identify what EPHI it creates, receives, maintains and transmits. In addition to computer workstations, EPHI may also reside on servers, or on portable devices such as laptops and cell phones.

You should have security measures in place to reduce risks and vulnerabilities to a reasonable and appropriate level. E-mail access should only be granted to persons who have received HIPAA training, and electronic devices used to communicate via email should be password protected. Your employees shouldnit share passwords or leave them in open areas. Appropriate sanctions must be imposed against employees who failed to comply with security policies and procedures. You should implement a written sanction policy that covers both email and other forms of EPHI storage, security and communication, and should train your employees regarding the policy. You should also implement procedures for the authorization and/or supervision of employees who work with EPHI. You should maintain a record of every electronic device used by your workforce and implement a sign out procedure for electronic devices used to communicate with patients. Many well publicized HIPAA breach settlements have involved the assessment of fines and penalties against providers whose employees have lost laptops or cell phones containing EPHI.

A practice must also have a data backup plan to create and maintain retrievable copies of EPHI. A number of physician offices had devices used to send and receive email damaged by flooding during Hurricane Sandy. You should ensure that your practice is able to regularly backup all sources of EPHI (including email) on a regular basis.

The use of business associate agreements is an important component of the administrative safeguards required by HIPAA. You should have written contracts in place with all outside entities entrusted with EPHI.

Question #3: What types of physical safeguards should my practice implement in order to protect EPHI?

HIPAA also requires practices to comply with various physical safeguards. Physical safeguards relate to protecting the buildings where and equipment on which EPHI is kept from not only unauthorized intrusion, but also natural hazards. Practices must implement policies and procedures which limit physical access to buildings and equipment, specify proper use of equipment containing EPHI, and address the proper receipt, movement and removal of such equipment.

You probably already limit access to buildings and equipment by having physical locks on the doors to your building, requiring user IDs and passwords and requiring users to log off computer systems when not being used. You should also consider using video surveillance cameras and posting signs identifying restricted areas. There are also many ways to reduce unwanted exposure to EPHI on individual workstations. Monitors should be positioned so unauthorized users cannot view the screens. Privacy screens (which reduce the ability of persons not directly in front of the monitor to view the screen) are available at very low cost. Most operating systems come with screen saver functionality that, after a period of inactivity, displays a selected image on monitors thereby reducing unintended exposure of EPHI to unauthorized persons.

HIPAA also requires practices to implement safeguards with respect to the handling of storage media (e.g. internal and external hard drives, flash/thumb drives, discs). Practices must implement policies and procedures for the receipt, movement and removal of such devices, including having back-up retrievable exact copies of EPHI.

One frequently misunderstood issue is erasure of data. HIPAA requires that you erase any media that contained EPHI before you discard it. However, erasure is not the same as deletion. In a Windows environment, when you delete a file, it is simply moved into your recycle bin, not erased. Even when you empty your recycle bin, the data is not erased. Rather, the data remains on your hard drive and the computer merely marks that space as free space that can be written over. In order to truly erase such data, this free space must be overwritten. When data is overwritten, it is replaced with random data. Software that performs this function is readily available at low cost and many operating systems come equipped with this functionality. Windows XP Pro, Vista, 7 and 8 all include functionality that will overwrite free space.

Question #4: What types of technical safeguards should my practice implement in order to protect EPHI?

Many of the HIPAA technical safeguards are common place in even small practices (e.g., use of unique user names and passwords). HIPAA, however, also requires practices to be able to ìtracki user identity. Guidance from the Centers for Medicare & Medicaid Services suggests that you may have a duty not only to track user 'identity,' but also to track user 'activity.'

Practices should configure their systems to automatically terminate an electronic session after a predetermined time of inactivity. While this is not mandated by HIPAA, practices are required to implement it where it is reasonable and appropriate. There are likely few circumstances where the implementation of this specification would not be reasonable and appropriate, even for small practices.

Encryption has garnered much attention in this area. HIPAA does not require the encryption of EPHI, unless it is 'reasonable and appropriate.' Unfortunately, this does not provide bright line guidance. The US Department of Health and Human Services (HHS) has published unofficial guidance (in the form of FAQs) on the use of encryption in email transmissions via the Internet. According to the HHS, if a patient emails unencrypted EPHI to a provider, the provider may assume that the patient has consented to the use of unencrypted email, unless (a) the patient has explicitly stated otherwise, or (b) the provider feels that the patient may be unaware of the risks of using unencrypted email. Even with this guidance, however, practices should be very cautious about the unencrypted transmission of EPHI over public computer networks (e.g., the Internet) and should obtain express written and informed consent from the patient.