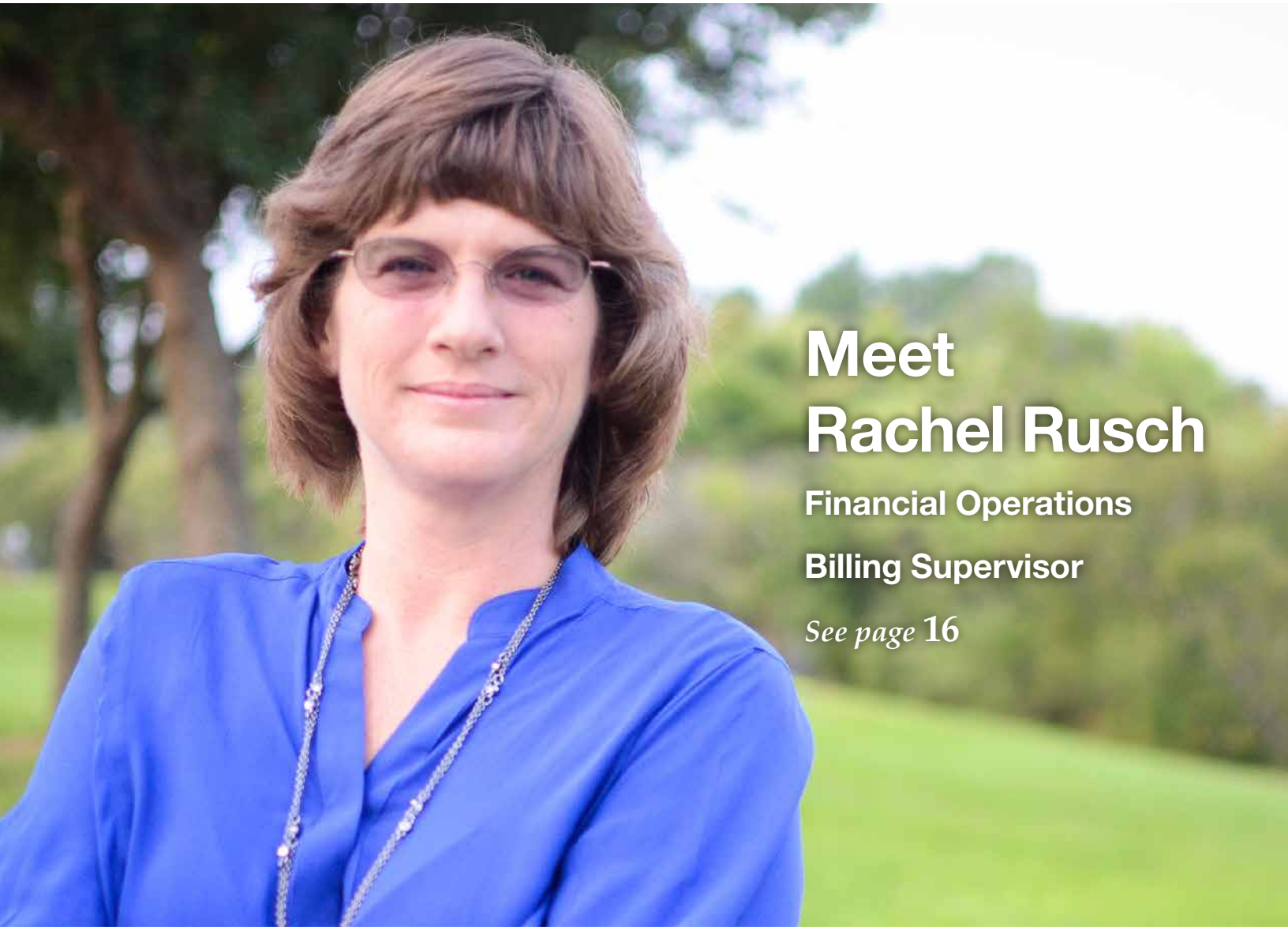
HCCA
HEALTH CARE COMPLIANCE ASSOCIATION

Compliance TODAY

August 2012

A PUBLICATION OF THE HEALTH CARE COMPLIANCE ASSOCIATION

WWW.HCCA-INFO.ORG



Meet Rachel Rusch

Financial Operations

Billing Supervisor

See page 16

by Adam H. Greene, JD, MPH

Electronically communicating with patients without running afoul of HIPAA

» Include all forms of electronic communications in your risk analysis.
» Implement systems to track patient preferences regarding electronic communications.
» Plan for human error, such as typos when entering emails.
» Obtain business associate contracts with hosts of your electronic messages.
» Consider that treatment-specific messages may have greater risk.

Adam H. Greene *(adamgreene@dwt.com) is a Partner in the Health IT/HIPAA practice of Davis Wright Tremaine in Washington DC.*

As a health care provider, your success in treating patients depends on your ability to communicate with them. As technology advances, this may mean electronically communicating with your patients in ways that are convenient for them, whether it be through email, text message, or even social media. The use of these technologies can facilitate better assistance to your patients on the days that they are not sitting in your office or facility. It is important, however, to understand how the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy, security, and breach notification rules apply to these forms of communications. (For purposes of this article, it is assumed that the health care provider is a HIPAA covered entity.)


Greene

Email—applying reasonable safeguards

Let's get something out of the way immediately—the HIPAA rules do allow health care providers to email patients.[1] In fact, in some circumstances, a health care provider actually may be expected to communicate with a patient through email, such as when a patient requests that certain communications (e.g., appointment reminders) be communicated through email and it would be reasonable to do so.

The key is that a provider should use email reasonably and in accordance with patient preferences. This means that when communicating through electronic media, the health care provider must employ reasonable and appropriate administrative, physical, and technical safeguards,[2] and should accommodate any reasonable request for confidential communications.

Administrative safeguards governing the emailing of patients include policies, procedures, and training, and may include safeguards against potential human error. For example, what safeguards are in place to guard against typos when entering email addresses? You may want to have a policy or procedure that requires staff to double-check email addresses. An alternative (or additional policy) may be that you require the use of a patient address book, which has entries that have been confirmed by sending a verification email to

each patient, to minimize the risk of a typo. It is worth remembering that for any patient who uses a public email service, there may be dozens of email addresses that only differ by a single letter, digit, or punctuation mark.

Administrative safeguards also include having a business associate contract in place with any entity that uses or discloses electronic protected health information (ePHI) on your behalf,[3] which may include an entity that hosts your email server. A physician practice in Phoenix had to enter into a $100,000 settlement with the U.S. Department of Health and Human Services for, among other things, not having a business associate agreement in place with an Internet-based email provider.[4] A business associate contract is not required for an entity that merely acts as a conduit, rather than using and disclosing PHI as part of its services.[5]

Physical safeguards for emails may include reasonable physical security for email servers, as well as any device that retains a copy of the email. For example, does a copy of each sent email remain on a workstation? If so, is the workstation kept physically secure? To the extent that you email patients from laptops, smartphones, and other portable devices, physical security always will be a challenge, and you may be best served by employing technical safeguards, such as ensuring that the devices are encrypted or that no copies of emails are left on the devices.

Technical safeguards for patient emails may include encryption of the information in transit, the use of secure messaging (such as where the patient receives notification that a message is waiting and must login to a website to view the message), and encryption of copies of emails at rest. HIPAA does not require you to safeguard information once it is on the patient's device. As a best practice, however, you may want to consider whether there are safeguards that you can employ to assist the patient with keeping the information secure, such as by using a secure messaging system that does not leave a copy behind on the patient's device.

When employing the above safeguards, what is reasonable and appropriate will differ, based on how you use email. For example, you may send general preventative tips to all patients. Although the contents of such messages are generic to all patients, the emails still may be PHI, because they include demographic information about each patient (e.g., name and email address) and indicate that the recipients likely are or have been your patients. These emails generally pose a lower risk than patient-specific emails that do not include condition-specific information (e.g., appointment reminders), which in turn pose a lower risk than patient-specific emails that do include condition-specific information (e.g., an email used for the purpose of treatment). You should adjust your controls, based on the risk of each type of email, and document your decisions (e.g., less sensitive data may represent a lower risk, because it may cause less harm if intercepted by third parties). For example, you may

You should adjust your controls, based on the risk of each type of email, and document your decisions (e.g., less sensitive data may represent a lower risk, because it may cause less harm if intercepted by third parties).

decide that it is reasonable to send out preventative tips and appointment reminders via unencrypted email. You should document this decision in a manner that demonstrates that you considered the potential threats and vulnerabilities to such emails and concluded that the associated risks were reasonable (i.e., low).

You may want to conduct the above analysis prior to communicating with your patients via email (or do so now if you are already emailing patients), and you should craft reasonable policies and employ them uniformly. In practice, however, you then can make adjustments as necessary, based on each patient's communication preferences. For example, if you conclude that treatment-related emails should be sent encrypted, but the patient indicates a preference to receive them unencrypted, then you may document the patient's request, make sure that the patient understands that there is some degree of risk of interception by third parties, and then accommodate the patient's preference.[1] Conversely, if you determine that emailing certain information to your patients is reasonable (e.g., appointment reminders), but a patient would prefer not to receive the information through email, you should accommodate the request. The use of a written form that document's the patient's communications preference and warns of the possible risk of interception may be helpful.

In short, you can implement reasonable and appropriate safeguards to protect a patient's information, but these safeguards need not not trump the patient's privacy rights.

To text or not to text

Email is not the only means of electronically communicating with patients. Health care providers also may send text messages to their patients. As with emails, different types of texts may raise different levels of risks. For example, you may conclude that it is reasonable to text general preventative tips to all of your patient population. In contrast, you may determine that the texting of treatment-specific messages to individual patients would be unreasonable, based on heightened risks.

Unless and until further research is conducted and further Health and Human Services guidance is issued, there are simply no hard-and-fast rules as to when it is reasonable to text PHI.

A challenge with text messaging is the dearth of information regarding the threats, vulnerabilities, and potential risks. The interception of text messages is rare, but not unprecedented.[6] Additionally, the means to safeguard against such risks may be limited, other than by avoiding true texting (e.g., the use of the SMS protocol) and instead using an alternative means, such as secure messaging software for cellular phones. Unless and until further research is conducted and further Health and Human Services guidance is issued, there are simply no hard-and-fast rules as to when it is reasonable to text PHI. In the absence of such guidance, documentation of a well-reasoned analysis may be key before texting.

As with emails, you also should consider employing appropriate administrative safeguards, such as steps to limit sending texts to the wrong destination and by obtaining a business associate contract with any entity that uses or discloses electronic PHI on your behalf other than a conduit (e.g., you may need to enter into a business associate contract with

a vendor that is hired to maintain and send texts to patients).

Despite the potential compliance challenges, communicating health care information through text messaging may offer substantial benefits to patients. For example, in its first year, approximately 135,000 women signed up for the text4baby program, in which timely health information is delivered to pregnant women and new mothers.[7] If you wish to communicate with patients via text messaging, you should analyze the potential risks and benefits and document your conclusion.

Pitfalls of "friending" patients

A third means of electronically communicating with patients is through social media websites, such as Facebook or Twitter. There is a growing pressure for all organizations, including health care providers, to maintain a high social media profile. As a health care provider, however, navigating these waters may be trickier because of HIPAA.

There are some challenges to communicating through social media that may make it a nonstarter with respect to HIPAA compliance. For example, if you communicate with a patient through a third party social media website, it is likely that the third party will be maintaining a copy of the message containing PHI on your behalf. Unless you can obtain a business associate contract with the social media provider, the government may view you as out of compliance with HIPAA.

Additionally, if you receive "friend" requests through social media, replying to such requests may represent a disclosure of PHI if you do not properly manage your privacy settings. You should consider keeping the fact that a patient is receiving services from you confidential, even in cases where the patient seems willing to shout it from the rooftops. This means ensuring that your list of friends or followers is kept private if the list is indicative of who your patients are (i.e., one patient should not be able to see that you are serving another patient).

Even if you do not voluntarily engage in the use of social media, your employees may. Consider training them that they may not post any information about patients on their own social media pages, even if they believe that they are not identifying the patient (a posting may be considered to identify a patient under HIPAA simply because the date of service is readily apparent).

Final thoughts

It is a brave new world out there, with patients spending more and more time online. Often, a text to a cell phone may be the best way to promote your patient's adherence to a medication regime or to initiate a follow-up appointment. Generally, HIPAA need not stop you from communicating with your patients in the most effective manner possible. Rather, HIPAA combined with ample amounts of common sense should be used to navigate around the potential privacy and security challenges that infest these waters.

1. HHS Office for Civil Rights: "Does the HIPAA Privacy Rule permit health care providers to use email to discuss health issues and treatment with their patients?" Dec. 15, 2008. Available at http://www.hhs.gov/ocr/privacy/hipaa/faq/health_information_technology/570.html.
2. 45 CFR §§ 164.308 to 164.312.
3. 45 CFR § 164.308(b).
4. Resolution Agreement between U.S. Department of Health and Human Services and Phoenix Cardiac Surgery, PC., April 13, 2012. Available at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf.
5. HHS Office for Civil Rights: "Are the following entities considered 'business associates' under the HIPAA Privacy Rule: US Postal Service, United Parcel Service, delivery truck line employees and/or their management?" March 14, 2006. Available at http://www.hhs.gov/ocr/privacy/hipaa/faq/business_associates/245.html.
6. Andrew Nusca: "Code that Encrypts World's GSM Mobile Phone Calls Is Cracked." *ZD Net*, December 28, 2009. Available at http://www.zdnet.com/blog/btl/code-that-encrypts-worlds-gsm-mobile-phone-calls-is-cracked/28942?tag=mncol;txt; Julie Criswell, "Wal-Mart Says Worker Taped Reporter's Calls," *New York Times*, March 6, 2007. Available at http://www.nytimes.com/2007/03/06/business/06walmart.html.
7. David Bornstein: "Mothers-To-Be Are Getting the Message." *New York Times*, February 7, 2011. Available at http://opinionator.blogs.nytimes.com/2011/02/07/pregnant-mothers-are-getting-the-message.