FEATURE

Electronic Communications: For Your (and Your Patients') Eyes Only

BY EMILIE T. PINKHAM, ESQ.

**This is the final article in a four-part series exploring social media and electronic communication challenges for health centers. The series previously covered general privacy and security risks, malpractice liability, and reputational threats related to social media use in health care settings*

Living in a digital age, consumers expect the ability to access personal accounts with the touch of a thumbprint on an iPhone. After all, sitting at my dining room table, I can view pictures from a friend's wedding in India, check my 401(k) balance, and pay my electricity bill. It's only logical that I should also be able to request an appointment with my primary care provider and find out when I had my last tetanus shot. In this final article, we'll go beyond social media to take a closer look at other forms of electronic communication in health care settings.

Text You Later, Alligator

Modern communication allows providers to text an appointment reminder, send a prescription to a pharmacy near your office, and send a record of immunizations to prepare for upcoming travel – all without leaving their desk. This capability is particularly helpful for patients in rural areas, enabling faster communication and lessening the impact of geographic barriers to care.

However, given the sensitive and confidential nature of electronic protected health information (ePHI), patient-provider communications must always be appropriately secure. Providers cannot use a personal email account like Gmail or yahoo to respond to a patient question.

Similarly, a patient shouldn't send pictures of symptoms or request medical advice via a standard text message ("SMS" or "short message service"). Doing so poses a privacy concern: SMS messages are stored on the cellular service carriers' servers as well as on both the sending and receiving devices, and more if you have linked devices. Plus, neither of these methods retain the information in the patient's record for future reference.

Providers face a delicate balancing act: a desire to meet patient

CONTINUED NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

communication preferences and leverage the benefits of technology coupled with an obligation to keep such communications appropriately documented and secure. As a solution, many electronic health record vendors have developed complementary or built-in "patient portals" to keep ePHI secure and maintain appropriate documentation in patient medical records.

What's a Patient Portal?

Patient portals are secure online websites that provide patients with convenient access to their personal health information from anywhere with a secure internet connection. Common features include document posting (e.g., test results and immunization history), appointment scheduling, prescription refill requests, and a secure line of communication.

No two portals are created equal. Some display a patient's entire medical record, while others have a summary view of recent records or a broad health history (e.g., immunization records, allergies, medication reactions, and previous hospitalizations). Still others serve mainly as a secure communication channel.

ePHI On Demand

A key benefit of patient portals is convenience. If TV shows are available to stream on-demand at any time, day or night, why not your personal health history? With 24/7 access, patients can send an

How do you know if your portal is appropriately secure? Talk to a qualified professional. Here is a quick guide to the key lingo to guide your conversations:

- **Audit Trail:** an electronic record of who accessed which accounts/information, when they accessed it, and if they made any changes.
- **Authentication:** the procedure of confirming the identity of a user trying to log in.
- **Authorization:** the process of recognizing that an authenticated user has permission to log into the account they are trying to access.
- **Encryption:** a method of saving files that converts data into ciphertext, making it difficult to "reassemble" without the right key (think of it like a program that turns your files into puzzles and mixes up all the pieces, and only an authorized user can see the big picture).
- **HTTPS:** the secure way to encrypt and transfer data between your browser and the website that you are connected to.
- **Multi-Factor Authentication:** a system that grants access only after the user successfully presents multiple pieces of evidence proving who they are (e.g., typing in a code texted to a cell phone while logging in on a computer, the last four digits of a social security number, and/or a unique code generated by the doctor's office).
- **PCI Compliance:** a set of standards set by the PCI Security Council to regulate customer payment data storage. Unless you meet these standards, patient credit card details and related payment data should not be stored in the portal or EHR system.
- **Role-Based Access Control:** a system controlling which information users can access based on their role (e.g., a patient can only see their account while a provider has broader access to all patient accounts).
- **SSL:** a method that encrypts network traffic from the web browser to a website.

appointment request while watching the nightly news instead of spending their lunch break on hold.

Providers can post required forms for patients to complete in advance of an upcoming appointment instead of spending time doing paperwork in the waiting room. Plus, an electronic form delivers better information: no longer does a staff member have to transcribe messy notes on a medical history or debate which allergen is checked with a haphazard "x" in between boxes

In addition to the convenience for patients, patient portals can also improve efficiency for staff. Front desk staff can make better use of phone calls if they can confirm appointments and send reminders through the portal. Similarly, providers can take time in between appointments to answer a quick question, approve a prescription refill request, or post a lab result that otherwise would be delayed until the patient's next appointment.

Portals may also improve accuracy. Given regular access to their health history, patients may identify inaccuracies or missing items. Once alerted to errors, a provider can make corrections at the next in-person visit. While research is mixed on the impact of patient portals on health outcomes, arming providers with more complete, accurate data, can only improve their ability to furnish higher quality care.

Further, increasing access to health information empowers patients, making them feel like a partner in their own care. The easier it is for a patient to communicate with and receive information from their provider, the more likely that patient is to actively engage in managing their health. This is particularly important for individuals with chronic diseases. Patient portals provide a quick way to log symptoms, send questions to a provider, and see an overview of key measurements over time.

It's not all good news — making ePHI available online from multiple access points increases its vulnerability. An unsecured patient portal is just one more place for hackers to access and mine sensitive information; however, taking the proper security precautions can mitigate major risks.

Beam me up to the Secure Patient Portal, Scotty

As with any ePHI (and PHI), health centers must comply with all relevant privacy laws and regulations. Given the complexity of patient portals and online security, it is especially important to consult with a qualified IT professional to keep ePHI secure. A patient portal must ensure access for authorized users while preventing unauthorized users from entering the system. Any ePHI captured in or linked to a patient portal must be stored safely (generally that means encrypted) and any messages with ePHI must be sent securely.

While you can limit staff to using secure devices and connections, patients will access information from a variety of devices (smartphones, tablets, laptops, and desktop computers) from many points of access (home, work, and maybe even public Wi-Fi networks). As a result, the security protections must be embedded in the digital access to the patient portal.

Other security measures to prevent fraud, identity theft, and data breaches remain relevant. Timed screensavers, strong passwords that are routinely changed, encrypted file-sharing programs to transfer ePHI, and regular staff training are all valuable. As with all technology, it's a moving target. The scope of required security precautions and the tools to execute them change regularly, making it critically important to review and implement new standards as they become available.

Addressing Patient Buy-In

Many people will be excited about the benefits of a patient portal; finding that the added convenience clearly outweighs any security risk. Others, however, will balk at setting up yet another username and password or may even refuse to participate, preferring the system they're accustomed to, regardless of added benefits.

Even the most user-friendly systems and well-planned roll-outs may result in low adoption rates. Communication on patient portals can be cumbersome. Instead of reading a message like any other email, users receive an email informing them of a new message or document posted

CONTINUED NEXT PAGE

CONTINUED FROM PREVIOUS PAGE

to the portal. Then, they have to log in to actually view the document or respond to the message. This is done to protect the ePHI, but it can cause frustration and impede user adoption.

Further, there may be financial or equipment barriers: some patients are less tech-savvy while others may not own a computer or smartphone, or lack regular internet access.

Provider reassurance can go a long way to encourage patient use of a portal as patients typically trust their providers' opinions and value their recommendations. The more patients know about the benefits of patient portals, the more likely they are to use them.

It may help to remind patients that portals:

- Offer a secure system to communicate quickly with their provider(s);
- Provide 24/7 access to their own medical records and health history; and
- Keep all messages and responses right in the patient record.

Providers can show more hesitant patients how to use the portal and reassure them that it's not mandatory — patients who don't like it, don't have to use it.

Strategies for a Successful Patient Portal

- **Know Your Audience.** Before spending resources on new programs or redesigning existing ones, understand how staff and patients currently communicate. Consider conducting an informal survey about patient comfort with technology and interest in electronic messaging.
- **Choose a simple product.** Maybe your EHR software already has secure messaging capabilities. If not, talk to experts and research options in order to choose a patient portal that integrates with your electronic records, has sufficient security measures, and is designed to be as simple and user-friendly as possible.
- **Set up a secure system.** Consult with a qualified IT professional to set up secure access ("https" and "SSL"), proper authentication and authorization procedures, and encrypted communication channels. If possible, provide each patient's initial user name and password in-person or over the phone. If account credentials must be sent electronically, require a password change on the first successful log-in and at regular intervals.
- **Review security measures regularly.** Regularly review security requirements and compare your system's capabilities (or pay an outside vendor to do so). Patient portals should meet all HIPAA standards for physical, administrative, and technical safeguards as well as all applicable federal, state, and local laws and regulations.
- **Educate employees and patients.** Make sure staff and patients know when to use the portal and when not to use the portal (e.g., send non-urgent questions over the portal and call 911 for emergencies). Provide clear examples that illustrate when a question can be resolved through a secure message and which common scenarios are more likely to require an in-person visit and/or physical exam.
- **Set Realistic Expectations.** Inform patients what type of information is available to them in the patient portal. Determine what constitutes a reasonable response time on a typical day and share these standards with your staff and patients. For example, is a provider expected to refill a prescription within four hours? Answer a non-urgent question within 24? Will the front desk confirm all appointments by the end of the next business day? Or, does the response time vary depending on the time of the request (e.g., during business hours or after)? ◆

Emilie Pinkham is an Associate at Feldesman Tucker Leifer Fidell LLP. For more information, contact her at: epinkham@ftlf.com.