Going Live with a Patient Portal—Legal Risks and Operating Documents

William J. Roberts
Shipman & Goodwin LLP
Hartford, CT

Patients who have sought access to their medical records are familiar with the manner in which such requests typically are handled—submit a form requesting access, show identification, wait days or even weeks, pay a copy charge, and/or visit the medical records office during business hours (which often take place during the same time the patient is at work or in school). Despite the best efforts of many providers to make the process seamless and patient friendly, the reality of health care privacy laws and medical records management has prevented the instantaneous and universal access to information many Americans expect. That said, the past few years have seen a revolution in patient access to health information as patient portals have proliferated among physician organizations and other health care providers.

This article begins with a brief discussion of the structure and use of patient portals and the legal risks that accompany them. The article then addresses practical issues regarding the documentation physician organizations may use when establishing and operating a portal.

What Is a Patient Portal?

A patient portal is a website that gives patients access, from a personal computer or other device, to health information maintained by a physician organization. A patient portal may allow a patient to view certain health information maintained by the physician organization; print, download, or transmit such information; request prescription refills; schedule appointments; make payments; view and download forms, such as a Notice of Privacy Practices; or exchange messages with the patient's health care providers.

Aside from a desire to provide convenience to patients, the adoption of patient portals by physician organizations also has been encouraged by the Medicare and Medicaid Electronic Health Record (EHR) meaningful use programs. The programs provide financial incentives for the "meaningful use" of certified EHR technology. To receive an EHR incentive payment, providers attest that they are "meaningfully using" their certified EHR technology by meeting certain measurement thresholds. One such threshold is the "view, download, transmit" measure, which requires that providers offer patients the ability to view online, download, and transmit their health information within four business days of the information becoming available to the provider.[1] While not specifically required, many physician organizations use patient portals to satisfy this measure.

Operational Matters and Risks

Any time patient information is stored electronically, particularly in the cloud, certain inherent privacy and security risks are present, including data corruption, hacking, and malware. Further, transmitting health information electronically exposes the information to potential interception or receipt by inappropriate recipients, whether malicious or inadvertent. While no patient portal can eliminate such risks, a physician organization may take certain steps to reduce them. Specifically, the physician organization may: (1) utilize software certified as satisfying privacy and security criteria promulgated by the Office of the National Coordinator for Health Information Technology;[2] (2) establish a verification protocol to ensure that only appropriate persons are granted access to the patient portal, as more fully discussed below; and (3) apply the organization's existing security program, including audits, encryption, and risk assessments to the patient portal.

A concern unique to patient portals is the often difficult task of determining what information to make available to patients via the portal. Factors to consider when making the determination include the usefulness of the information to patients and patients' ability to understand the information. For example, highly technical information or miscellaneous nursing notes may be of little value to patients and may, in fact, confuse patients who view the information in the absence of a health care provider. Further, special consideration should be given to: (1) patients who are minors; (2) lab results, the disclosure of which may be governed by state law, including state laws that limit the disclosure of such results to patients;[3] and (3) sensitive information, such as behavioral health, genetic testing, substance abuse, or HIV/AIDS information, which a physician organization may opt not to include on a portal due to concerns with inappropriate access, lack of patient understanding, or state laws.

The treatment records of minors illustrate the challenge physician organizations face when determining portal content. In many states, minors are granted the right to consent to certain treatments or procedures without the

consent of the minors' parents or legal guardians. Such treatments or procedures vary by state, but often include abortion, pregnancy counseling, outpatient behavioral health, or HIV testing. In general, when a minor consents to treatment, the minor controls the use and disclosure of records pertaining to such treatment, and not the minor's parent or guardian. Hence, if a physician organization grants a parent access to a minor's medical records via portal, and the portal contains information regarding services for which only the minor consented, the physician organization inadvertently may violate the minor's privacy rights. This may occur even if the portal makes available only routine patient information, such as test results (e.g., HIV or pregnancy test results) or appointment schedules (e.g., for outpatient behavioral health services). To prevent such an incident, a physician organization should evaluate the legal implications and requirements of each category of health information it proposes to make available on the portal.

Documentation

When a physician organization is establishing a patient portal, the physician organization should consider drafting and implementing four documents to facilitate patient access, educate patients regarding use of the patient portal, and help protect the physician organization in the event of an adverse incident.

Registration Form

The first document to consider is a registration form. Whether online or in hard copy, the form should request information sufficient to enable the physician organization to identify the patient, link the patient to a designated medical record or patient account, and verify that the individual submitting the registration form is the subject of the medical records for which the individual is requesting access. At a minimum, the registration form should request the patient's name, address, date of birth, and contact information (including email address). The physician organization also may consider requesting the patient's medical record number and/or the last four digits of the patient's Social Security Number (SSN) to better verify the patient's identity and link the patient to the correct medical records.

To ensure that the person completing the registration form is who she says she is, the physician organization should establish an identity-verification protocol. Most often, a physician organization requires the individual to present the registration form in person to an office manager or medical records professional, along with a copy of a valid government picture ID, such as a driver's license, state ID card, or passport. Alternatively, some organizations, recognizing the difficulty of getting individuals who currently are not undergoing treatment to visit the physician's office, have utilized telephone verification. Telephone verification typically entails the physician organization asking a series of security questions, the answers for which only the patient would know. Questions may include full SSN, date of most recent visit, reason for last visit, or similar personal questions. To many, the process is akin to a password-reset protocol for online banking.

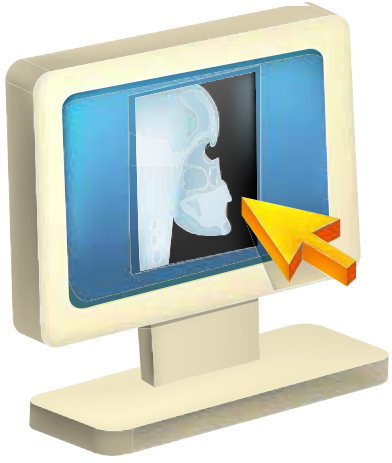
In the event a parent or legal guardian seeks to register to access a minor's or other individual's medical records through the portal, the physician organization should utilize a protocol to ensure that the individual requesting access has the legal right to access such records. Documentation to verify access may include a birth certificate, court order, or guardianship/conservatorship/power-of-attorney document. Specific requirements will vary by state. Also, note that because more than one individual may have a right to access a patient's records, more than one account may need to be created for a particular patient.

Access Agreement

The second document to consider, which may be combined with the registration form but typically is a stand-alone document, is an access agreement. The purpose of an access agreement is to set forth the patient portal's guidelines, terms and conditions of use, and to have the registrant read and agree to comply with such requirements. The content of the access agreement can be grouped into four categories: (1) provision of the patient portal service; (2) privacy and security considerations; (3) use guidelines; and (4) legal terms and conditions.

The access agreement's language on the provision of the patient portal service should put the patient on notice that the physician organization retains the right, at its discretion, to modify, suspend, or terminate the patient portal at any time and that the patient has no right to continuing use of the portal. The agreement also may address the physician organization's right to implement fees for portal access.

As discussed above, the privacy and security of health information created and accessed through the portal typically is a paramount concern of portal operators and users. The access agreement presents an opportunity to address pertinent privacy and security concerns prior to the user initiating use of the portal. For example, if the patient portal will contain



messaging functionality, the access agreement may state that messages sent via the portal may become part of the patient's medical record, and individuals with a legitimate need to know may see the messages, in addition to the intended recipient.

The access agreement also should establish basic expectations and requirements for how the patient may use the portal. If the patient portal includes messaging functionality, arguably the most important use guideline to address in the access agreement is that the patient portal is not to be used for urgent communications or medical emergencies. The access agreement should make clear that the physician organization may not immediately review messages sent through the portal and that not all messages will receive a response. The agreement also should make clear that if the user has an urgent matter, the user should call 911 or seek other emergency care.[4] Moreover, users may be informed that the portal is intended to supplement, not substitute, the user's usual communication with the physician or other health care provider.

In addition, the access agreement may prohibit the posting of offensive or inappropriate material on the portal or the use of rude or threatening language. The user also may be informed that the physician organization is not responsible for any disclosures that the user intentionally or unintentionally makes to third parties.

The last category of information to consider including in an access agreement is legal terms and conditions. While physician organizations should take care to avoid overwhelming users with intimidating legal jargon or unreasonable terms, the agreement should address certain topics to protect the physician organization and clarify users' expectations. Specifically, the agreement should contain: (1) a prohibition on the reproduction or personal use of any text, photographs, graphics, icon buttons, images, artwork, names, logos, and trademarks or service marks contained in the portal; and (2) a statement that the inclusion of links to other websites does not imply any endorsement of the material on the websites, the operators of the website, or any association with the operators.

Disclaimers

Disclaimers may be included in the access agreement and/or as a "pop-up" agreement upon a user accessing the portal (either upon initial access, upon each access, or periodically). Regardless of where the language is included, the physician organization should disclaim: (1) any responsibility for, or liability related to, third-party material made available through the portal, such as links to publications, articles, or third-party websites (e.g., American Heart Association); (2) that the user assumes all risk relating to the user's viewing of health information on the user's computer or device and the transmission of health information via a third-party network, such as the user's internet service provider; and (3) all warranties, including, but not limited to, implied warranties of merchantability, fitness for a particular purpose, and infringement. The agreement also may include a statement that the physician organization does not control, and is not responsible for, the content or performance of any links to websites operated by third parties. Moreover, the agreement should make clear that the portal is provided "as is" and that no guarantee is made regarding ability to access the portal at any particular time, location, or internet speed.

Proxy Agreement

In the event a registered user seeks to grant a third party access to the user's medical records through a patient portal, a proxy agreement should be utilized. A proxy agreement permits one party to act on behalf of another when accessing patient records. While the form of such agreements varies, a few key elements should be considered for inclusion. First, the registered user should complete and sign the proxy agreement and should be made aware of the significance of signing the proxy agreement. For example, the registered user should be informed that the proxy will have the same access and privileges as the registered user, and that this allows the proxy online access to the registered user's personal health information, including any HIV/AIDS, mental health, and/or drug and alcohol abuse and treatment information included on the portal. Second, to properly verify the proxy's identity, the form should request name, demographic, and identifying information about the proxy, in a manner similar to what is requested of the patient upon registration. Lastly, the proxy should acknowledge, in writing, the proxy designation and the portal's terms, conditions, and guidelines for use.

Looking Ahead

Patients likely will continue to demand, and government regulation likely will continue to encourage, timely and convenient access to health information. Looking ahead, physician organizations should anticipate patient portals becoming a standard tool by which to inform and communicate with patients. In many instances though, patient portals will need to operate within regulatory frameworks that predate and do not contemplate online access to medical records. Careful review and operation of patient portals is necessary to ensure that meeting patient expectations today does not inadvertently violate yesterday's regulations.

---

1 45 C.F.R. § 170.314(e)(1)

2 For additional information about the certification process and certified software, *see* www.healthit.gov/.

3 *See, e.g.*, Cal. Health & Safety Code § 123148 (2008).

4 Many physician organizations also include such a warning on the patient portal website.