HCPro
an H3Group brand

Briefings on HIPAA

Volume 17 Issue No. 10 OCTOBER 2017

INSIDE THIS ISSUE

Patient access

Patient portals and HIPAA: Upholding security and patient rights

Patients and providers have more access to information than ever before. An EHR can put a patient's entire medical history at a provider's fingertips. Patient portals can offer a similar level of access to patients, which can help them become better informed and engaged. Under HIPAA, patients have the right to access their own information, and technology can help organizations seamlessly honor that right.

Or can it? Although data abounds, some organizations and patients are still confused about what information must be provided and when and how patient requests for access must be honored. Picking or building the right portal can be tricky. An overly complicated interface or login procedure could prove frustrating for patients and lead to low utilization, thwarting the organization's efforts to provide patients with information. However, poor security controls can put the patient and the organization at risk.

A sound understanding of HIPAA will guide an organization's policies and make patient portals an easy win for all.

Growing use

Patient portal use isn't universal yet—but it's growing, according to the Medical Group Management Association's (MGMA) 2017 MGMA DataDrive Practice Operations Survey, released in August. At hospital-owned physician practices, 30% of patients use the portal, and at physician-owned practices, 15% of patients access the portal, the survey found. The most commonly used function was accessing test results (29%). Bill payment, communicating with providers and medical staff, downloading or transmitting medical records, and scheduling appointments tied for second place at 28%.

Many organizations rely on their EHR vendor for patient portal technology, says **Kate Borten, CISSP, CISM, HCISPP,** founder of The Marblehead Group in Marblehead, Massachusetts.

The much-maligned EHR adoption incentive programs ushered in by the HITECH Act played a significant role in spurring organizations' adoption of EHRs, according to a study in the August issue of *Health Affairs.*

Despite the justifiable criticisms of the program, it helped usher healthcare organizations into the 21st century and gave patients a new way to engage in and manage their care.

"The meaningful use program has definitely moved many more providers to implement patient portals, and a growing number of patients routinely use these portals to access information such as appointments and lab results," Borten says.

No standard solution

How well an organization manages its patient portal will depend on how mature its electronic data management and security programs are, says **Ben Goodman, CRISC,** founder and CEO of 4A Security and Compliance in New York.

"Healthcare organizations are really all over the map," he says. "There are some that are very good and aware and on top of things as far as security and compliance goes. And then there are others that are just waking up to the issues and thinking about it, even though they have probably gone down the road as far as meaningful use and digitization of healthcare records."

Although many organizations use patient portals that are packaged with their EHR, sometimes the patient portal is less integrated with the EHR, Goodman says. There is a wealth of options—from homegrown solutions to comprehensive systems offered by major vendors—representing a variety of approaches and system architecture, he adds.

The sheer variety of patient portal solutions, whether homegrown or provided by a vendor, can create a positive space for innovation and competition. However, that means the system architecture, features, and security of patient portals can vary widely between provider organizations and vendors.

"At some of the larger hospitals and healthcare systems, there you start to see some good quality web

HCPro an H3.Group brand

Briefings on HIPAA (ISSN: 1537-0216 [print]; 1937-7444 [online]) is published monthly by HCPro, an H3.Group division of Simplify Compliance LLC. Subscription is an exclusive benefit for Platinum members of HCPro's Revenue Cycle Advisor. Platinum membership rate: $895/year. • **Briefings on HIPAA,** 35 Village Road, Suite 200, Middleton, MA 01949. • Copyright © 2017 HCPro, a division of BLR. All rights reserved. Printed in the USA. Except where specifically encouraged, no part of this publication may be reproduced, in any form or by any means, without prior written consent of HCPro or the Copyright Clearance Center at 978-750-8400. Please notify us immediately if you have received an unauthorized copy. • For editorial comments or questions, call 781-639-1872 or fax 781-639-7857. For renewal or subscription information, call customer service at 800-650-6787, fax 800-785-9212, or email *customerservice@hcpro.com.* • Visit our website at *www.hcpro.com.* • Occasionally, we make our subscriber list available to selected companies/vendors. If you do not wish to be included on this mailing list, please write to the marketing department at the address above. • Opinions expressed are not necessarily those of **BOH.** Mention of products and services does not constitute endorsement. Advice given is general, and readers should consult professional counsel for specific legal, ethical, or clinical questions.

applications and patient portals, and that kind of tech can be very secure," says **Larry Ponemon, CIPP,** founder and chairman of the Ponemon Institute in Traverse City, Michigan. "But for the most part the patient portal does vary from a lot of homemade applications that are made by local hospitals and clinics to very sophisticated systems that are maintained by large healthcare networks."

With all the varied definitions of a safe and secure portal, an organization must choose the patient portal solution that best fits the needs of patients and the organization—and one that meets HIPAA requirements.

Secure access

Patient portals contain PHI; therefore, they must meet the requirements of the HIPAA Security Rule. However, several factors can make this a little more complicated than securing PHI accessed by an organization's staff using the organization's devices.

"Any external access to PHI presents potential risk," Borten says. "However, we expect that developers are thoroughly steeped in good coding practices and processes, and that portals are carefully implemented."

Organizations that use patient portal services offered through their EHR vendor should expect the vendor to offer a consistent level of security.

"Provider organizations typically rely heavily on their EHR vendors for portal technology, and they follow the same security protocols as for remote access to their EHR," Borten says.

However, as with any service offered by a third party, an organization can't assume that the patient portal is secure. An organization must understand security risks associated with a patient portal and be prepared to address them.

"There are a lot of unique risks posed by patient portals, especially since you have to accommodate users across a full spectrum of sophistication and requirements," Goodman says.

Some patients might be very tech savvy, but others will not be, he points out, and unlike access controls for staff, an organization has limited control over how patients access the patient portal. That puts the onus on the organization to manage security for a wide range of users it can't control.

Patient portals should be designed to be accessed by an individual's personal device. Although the covered entity (CE) or business associate (BA) that is providing the patient portal is bound by HIPAA's requirements, patients are not. A CE is required to ensure that its devices are properly secured, but that requirement does not apply to patients. An organization must be aware of that and take the appropriate steps to address vulnerabilities it can control, such as password strength standards.

"Because providers can't control their patients—unlike their own workforce—there is certainly risk that a patient may expose PHI through poor security and privacy practices," Borten says. "Patients may use devices that have been compromised with malware, such as a keystroke logger that can capture logon IDs and passwords. Patients may view their information in public places where it is exposed."

Developers should design patient portals so that no PHI is left on the patient's device, she says. And, the patient will have access to only his or her own PHI. That differs from remote EHR access by physicians and other staffers, who typically have access to many patients' PHI.

Another way organizations can address security vulnerabilities on the patient's end is by boosting security controls that protect the database where the PHI is stored, Ponemon says. The interface between the end user device and the database where the information is stored can be very secure—or highly vulnerable.

"There can be security at the end point, so if your device is contaminated with malware, and it tries to contact the data center at the hospital, for example, it will detect that the device has an anomaly or is suspicious, and it might not let you get into the database," Ponemon says.

Weak security can have disastrous consequences such as opening a door to a ransomware attack, he adds. If the database the patient portal is connected to is connected to other systems, malware can easily spread throughout the organization. However, endpoint device security protocols don't need to be restrictive, Ponemon says. Generally, if a device has basic, up-to-date antivirus software installed, it doesn't pose a significant risk.

"You don't have to have the most sophisticated security system on your device, but if it's insecure, it's detected at the gateway or sometimes at the device level itself," Ponemon says.

If the device is not secure, the patient portal could be set up to display a message asking the user to contact a support number to troubleshoot the device or connection, he says.

Access to the patient portal must be password-protected. Organizations should set reasonable password requirements and login protocols that are in line with security standards but that also take into consideration the wide range of users accessing the portal. The organization has a duty to protect PHI, but an overly burdensome login process could create obstacles to access for some patients.

"User identification and authentication at the patient portal is typically less stringent, or no more stringent today, than access to bank and other financial accounts," Borten says. "While some patients may not care about the privacy of their health information, other patients certainly do; hence, the security and privacy controls for all must be reasonable and meet community standards."

Information access

Some patient portals may connect directly to the organization's EHR. While that can ensure data is synched up and current on both ends, it creates vulnerabilities that the organization must address. Goodman has worked with clients whose patient portals connect to the EHR, and helped them explore options to mitigate the risks. Some of the solutions his company has worked on included creating a separate instance of the organization's database that is accessed by the patient portal or other methods to minimize the amount of data being exposed and create firewalls between the EHR and the patient portal.

"Obviously if you're putting your sensitive PHI database out there for anybody to access, then there's a lot more risk than if you're segmenting that off," Goodman says.

Patients are generally able to edit certain limited demographic data or contact information, but they are not permitted to change clinical data such as lab results. Amendments to PHI should be handled through processes set up in accordance with the Privacy Rule's request for amendment requirements, Borten says.

"This makes sense since that data can be used to treat patients, and providers must ensure data integrity," she says.

An organization must be mindful of what information is included in the patient portal. Some states, and other federal laws, require stricter protections than HIPAA for PHI pertaining to minors, behavioral health, genetic information, substance abuse, or HIV/AIDS, Goodman says. Organizations, including those developing patient portal software, should be aware of all privacy and security regulations that apply specifically to them and follow the appropriate requirements.

However, there are many benefits of patient portals. A patient portal gives patients easy access to their own PHI and removes some administrative burdens on the organization, Borten says. If a patient is able to check lab results on the patient portal, that can reduce the amount of time staff and patients spend playing phone tag. However, many organizations and patients mistakenly believe the patient portal gives access to the full set of patient data, the designated record set, to which patients have the right of access, she says.

"The advent of patient portals seems to have weakened many organizations' procedures for providing designated record set access and copies," Borten says. "The HIPAA Privacy Rule, effective over a decade ago, explicitly expanded the information patients are entitled

to see. But many providers still fall short of regulatory requirements, and many patients have no idea of the full scope of this right and the breadth of information."

Develop security

There is still a large variance in the industry when it comes to security, Ponemon says. Although some organizations are on top of security, others still struggle with the basics. Patient portals can be a major benefit to organizations and patients, but they must be properly managed from the start.

"In the short term, I think that you want to make sure that if you're building a portal, you're doing some basic application security like penetration testing, dynamic and static code analysis, and other application security steps to make sure that your application is not vulnerable to attack," Ponemon says.

Third-party testing provides extra assurance that the testing is done correctly, thoroughly, and without internal bias, he adds. Services such as managed service providers can conduct thorough, industry-standard testing.

"You want to protect that portal because it's a trust issue," Ponemon says.

Organizations must be alert for patient portal software-related security issues, Borten says. Developers must follow secure coding practices, testing, and change management processes. Otherwise, the application may contain vulnerabilities that hackers can exploit.

The patient portal must be included in the organization's risk analysis. The risk analysis should answer all questions about where and how data is stored, transmitted, or created and identify vulnerabilities at any point, Goodman says. The organization should address any significant vulnerabilities identified during the risk analysis, and, if the expected control is not used to mitigate a given vulnerability, thoroughly document the alternate control and the rationale behind that decision.

"The challenge is to identify the blind spots," Goodman says. "There's always things that people aren't thinking about or looking at."