Pre-Publication Draft

PLEASE DO NOT COPY, DISTRIBUTE OR CITE WITHOUT THE PERMISSION OF THE AUTHOR

A WINDOW INTO PATIENT PORTALS: LEGAL AND PRACTICAL ISSUES FOR PHYSICIAN PRACTICES

By Daniel F. Shay, Esq.

Alice G. Gosfield and Associates, P.C.
2309 Delancey Place
Philadelphia, PA 19103
215-735-2384
215-735-4778
dshay@gosfield.com
www.gosfield.com

Accepted for publication in the Health Law Handbook, 2017 Edition.
Alice G. Gosfield, Editor, © Thomson Reuters.
A complete copy of the Health Law Handbook is available from Thomson Reuters by calling 1-800-328-4880 or online at www.legalsolutions.thomsonreuters.com.

A Window Into Patient Portals:

Legal and Practical Issues for Physician Practices

I. Introduction

Physician-patient communication is an essential component of the practice of medicine for any physician specialty that directly interacts with patients. One of the main purposes of a patient portal is to enhance this central aspect of the practice of medicine, allowing fast and simple communication between physician and patient, and improving physician efficiency in the office. There are many benefits for physicians using a patient portal.

However, there are still hurdles associated with use of a patient portal. For example, the physician practice must purchase or license the necessary software, meaning the practice must take the time to research patient portal options. If the practice already has an electronic health records (EHR) system, the practice may find that it is "locked in" to using only the portal offered by the company that makes its EHR. In either case, the practice likely will have to sign (and have an attorney review) a license agreement covering the portal software. Of course, using any software that allows for the transmission and/or storage of electronic protected health information (EPHI) necessarily implicates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its regulations, especially the Security Rule, all of which requires the practice to undertake extensive, time-consuming steps towards compliance.

Once the portal is installed, the practice may find that patients are reluctant to use the portal, relying instead upon the more time-honored method of calling the office and waiting for a return call, or scheduling a visit. This can be doubly frustrating, if the practice is participating in the Medicare Incentive Payment System (MIPS), which includes within it many aspects of the

older "Meaningful Use" program, given that MIPS includes measures that require the use of a patient portal. Those patients who do sign up will be required to sign a Terms of Use agreement with the EHR vendor or practice, which will create additional legal considerations.

This article explores the issues surrounding the use of patient portals in physician practices. It addresses the nature of portal technology, and how it actually functions. It then discusses the potential benefits of using a portal, as well as the potential drawbacks and practical hurdles a practice may face using a patient portal. It further examines legal issues associated with patient portal use, including issues arising from license agreements between the vendor and the physician practice, and Terms of Use agreements between vendors or practices and patients, HIPAA concerns, and issues surrounding patient records ownership.

II. Patient Portals Background

According to the Federal government's HealthIT.gov website, a patient portal is "a secure online website that gives patients convenient 24-hour access to personal health information from anywhere with an Internet connection."[1] The description also includes a list of the types of information that can be accessed from a patient portal, including recent physician visits; discharge summaries; medications; laboratory test results; allergies; and immunizations. Some portals also permit secure messaging through an e-mail style interface, and allow for prescription refill requests, appointments scheduling, and even payment of outstanding bills. Portal technology can be useful and convenient, but also has its share of practical downsides. In recent years, the Federal government has also attempted to incentivize the adoption of portal technology across the healthcare industry.

[1] https://www.healthit.gov/providers-professionals/faqs/what-patient-portal.

A. Portal Technology Overview

At its most basic, a portal is simply software that allows for secure, remote access by an individual to an institution, where records pertaining to the individual's health care can be viewed. Portal technology has existed in one form or another since the 1990s, but implementation in the medical arena lagged behind other uses of the technology. The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009[2] was intended to spur the development and adoption of portal technology. However, adoption rates have still remained sluggish, with only 10.4% of hospitals in the United States having met the requirements under the Meaningful Use program to deploy a patient portal,[3] only 15% of consumers having access to emails with their physicians, and approximately 20% having access to online appointment scheduling.[4]

Similar to the definition of "patient portal" provided by HealthIT.gov above, the California Health Care Foundation defines a patient portal, as distinct from a "personal health record" (PHR), and describes a patient portal as a secure website that permits a patient to access their PHR.[5] A PHR is usually a standalone program that permit patients to enter data into the software, and which is owned by the patient (or their proxy). A portal, however, is usually owned (or licensed) by the physician practice or other health care provider, and functions as a

---

[2] Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, 111 P.L. 5.

[3] Garrido, Terhilda, Brian Raymond, and Ben Wheatley, "Lessons From More Than A Decade In Patient Portals," Health Affairs, April 7, 2016, located at, http://healthaffairs.org/blog/2016/04/07/lessons-from-more-than-a-decade-in-patient-portals/.

[4] "Majority of Americans Don't Use Digital Technology to Communicate With Their Doctors," results of a study conducted by Nielsen, November 4, 2015, available at, http://accountablecaredoctors.org/health-information-technology/majority-of-americans-dont-use-digital-technology-to-access-doctors/. The one bright spot in this study is that these numbers were found to have actually risen by 4 and 6 percent, respectively, since 2014.

[5] http://www.chcf.org/patient-portals/definitions.

separate website through which a patient may access their PHR. A portal is also usually – although not always – "tethered" to an EHR as part of the software suite, and allows patients to perform different functions from a PHR, such as those described above in the HealthIT.gov definition.[6] Finally, the information contained in a PHR is only updated when the patient chooses to update the information, whereas information residing within a portal is kept up to date by the physician practice.

Standalone portals do exist, however, and can be more robust and customizable in their feature sets than tethered portals. Tethered portals, however, are already fully integrated into the EHR suite, requiring no additional work to establish an interface. Moreover, they offer the practical benefit of one-stop-shopping. There is no reason, therefore, for a physician practice to spend the additional time researching other portals, their features, costs, or their ability to connect with the practice's EHR suite, when the practice already has built-in portal technology. The only reason to do otherwise is if the standalone portal offers features that the tethered portal does not, which the practice deems sufficiently attractive to justify the extra cost and effort of obtaining the standalone product.

B. Benefits and Barriers of Portal Use

Patient portals are generally believed to offer significant benefits to physician practices. First and foremost, a portal offers a secure method of communicating with patients, in comparison to unsecured emails or texts. To access information through the portal, a patient must log in to the portal website, and then enter a user name and password to view their information. The website itself is usually separate from the physician practice's business

[6] http://www.chcf.org/patient-portals/definitions. The additional functions of a portal include: completing forms online, communicating with providers, requesting prescription refills, reviewing lab results, or scheduling medical appointments.

website. To the extent that they are connected, the portal is most often accessed through a link on the main practice website. When a physician sends a message to the patient, the message is viewed and stored within the portal site itself, and the patient is merely notified by email to log in to the portal and view the message; the email sent to the patient contains nothing further of substance.

Portals can also improve efficiency. For example, the California Health Care Foundation found that use of a portal could potentially decrease the amount of time spent on the phone with patients. In a study comparing a primary care practice location using a portal to one which did not, the site using the portal saw an 18.2% drop in phone calls, and an overall drop in messages.[7] Other physicians have noted that using a patient portal helped to expand their practice three-fold in under three years, while also helping to keep staff costs low.[8] As other practices have described it, the use of a patient portal permits a physician to respond to patient inquiries between visits, rather than having to play "phone tag" with patients throughout the day.[9] At the same time, patients can use the portal to contact the practice at any time, night or day.[10]

Portals are also reported to improve quality of care for patients. For example, the use of secure email communications between patients and physicians is reported to result in improved

---

[7] Emont, Seth, Ph.D., M.S., Measuring the Impact of Patient Portals: What the Literature Tells Us, California Health Care Foundation, May 2011, p. 10. Located at http://www.chcf.org/publications/2011/05/measuring-impact-patient-portals.

[8] Geyer, Sheree, "Patient Portals Helping Increase Revenue, Decrease Costs," HealthcareITNews.com, April 29, 2016, available at, http://www.healthcareitnews.com/news/patient-portals-helping-increase-revenue-decrease-costs.

[9] "Patient Portal Increases Communication Between Patients and Providers," Spring, 2011, testimonial from Blackstone Valley Community Health Care, available at, https://www.healthit.gov/providers-professionals/blackstone-valley-community-health-care-case-study.

[10] "Patient Portal Implementation Improves Quality of Patient Care and Strengthens Preventive Care," Spring, 2011, testimonial from Dover Family Physicians, available at, https://www.healthit.gov/providers-professionals/dover-case-study. Of course, physicians may not necessarily respond immediately, but a portal permits a patient to leave a message directly for the physician, rather than having to rely on an intermediary, like a call service, to pass on the message.

Healthcare Effectiveness Data and Information Set (HEDIS) performance measures by between 2.5 and 6%.[11] Use of a patient portal is also reported to have improved the health of chronically ill pediatric patients suffering from asthma. In a study published in June, 2016, researchers found that use of portal technology resulted in increased rates of prescriptions and drug changes throughout the course of the year, in comparison to the previous year before adoption of the patient portal.[12]

However, patients have been slow to adopt the use of portals. In the abovementioned pediatric asthma study, the researchers found that actual rates of adoption and continued use of the free patient portal were extremely low. The study found that out of 9,133 potential parents of patients, only 237 actually completed a survey using the portal – a rate of only 2.59%.[13] Those parents of patients who adopted the portal continued using it at a rate of 65.8% (a total of 157 patients), although that number made up only 1.71% of eligible parents of patients.[14] The researchers determined that this low adoption rate suggested that, in spite of the potential benefits of using a portal, widespread adoption across the health care landscape was likely to be slow.

---

[11] Garrido, Terhilda, Brian Raymond, and Ben Wheatley, "Lessons From More Than A Decade In Patient Portals," Health Affairs, April 7, 2016, located at, http://healthaffairs.org/blog/2016/04/07/lessons-from-more-than-a-decade-in-patient-portals/.

[12] Fiks, Alexander, et al., "Adoption of a Portal for the Primary Care Management of Pediatric Asthma: A Mixed-Methods Implementation Study," Journal of Medical Internet Research, Vol. 18, No. 6, June, 2016, available at http://www.jmir.org/2016/6/e172/.

[13] Fiks, Alexander, et al., "Adoption of a Portal for the Primary Care Management of Pediatric Asthma: A Mixed-Methods Implementation Study," Journal of Medical Internet Research, Vol. 18, No. 6, June, 2016, available at http://www.jmir.org/2016/6/e172/. Completion of the online survey was classified as "adoption" for purposes of the study, as distinguished from continued use.

[14] Fiks, Alexander, et al., "Adoption of a Portal for the Primary Care Management of Pediatric Asthma: A Mixed-Methods Implementation Study," Journal of Medical Internet Research, Vol. 18, No. 6, June, 2016, available at http://www.jmir.org/2016/6/e172/.

In spite of what some might expect, a study conducted by Athenahealth – a developer of electronic health records software – found that there is no correlation between age and adoption rates. In other words, it is not as if younger, potentially more technologically savvy patients are more likely to use a portal than their older counterparts. Likewise, the size of the physician practice does not have a determinative effect on the rates of portal use by patients.[15] Instead, other factors tend to have more impact on slow rates of patient adoption.

For example, some physicians believe that lack of computer access can be a factor, especially for lower income patients.[16] Other physician practices report that patients are reluctant to use the practice's patient portal because the patients prefer alternate forms of communication, such as texting. For example, one physician practice reported, "We routinely send out messages on the portal. But we feel that the portal has lost functionality because people prefer text messages. So we text everybody. The portal is useful for patients who want to make appointments, ask for referrals, or ask a question."[17] In relation to their preference for text, patients may be reluctant to use a portal to communicate with physicians, simply because of the requirement to remember a user ID and password to log into the portal.

Deployment of a patient portal can also place burdens on the physician practice. For example, it may require either the hiring of additional staff, or requiring current staff to extend their duties to include responding to portal inquiries. For physician practices treating high

[15] Clain, David, "athenaResearch Study: The Current State of Patient Portal Adoption," July 30, 2015, available at http://www.athenahealth.com/blog/2015/07/30/athenaresearch-study-the-current-state-of-patient-portal-adoption.

[16] Fiks, Alexander, et al., "Adoption of a Portal for the Primary Care Management of Pediatric Asthma: A Mixed-Methods Implementation Study," Journal of Medical Internet Research, Vol. 18, No. 6, June, 2016, available at http://www.jmir.org/2016/6/e172/.

[17] Terry, Ken, "Patient Portals: Essential, But Underused by Physicians," Medical Economics, April 29, 2015, available at http://medicaleconomics.modernmedicine.com/medical-economics/news/patient-portals-essential-underused-physicians?page=full. The physician practice stated that it did not send PHI over unsecured texts. The practice also reported that roughly 90 percent of patients had portal access, but only about 1/3 actually used the portal.

volumes of patients daily, the use of a portal may slow workflow, resulting in lost productivity, at least when dealing with patients that send multiple secure emails and expect a rapid back-and-forth interaction with the physician.[18] Likewise, interaction with a patient using a portal is unlikely to be reimbursable by third party payors, and thus constitutes "free care" in the eyes of some physicians. One physician explained "Right now there's a problem in medicine that people want all their care over the phone, and this just adds another layer to 'I want all of my care for free.'"[19]

C. Required and Promoted Use of Patient Portals

Since as early as 2006, the Federal government has sought to promote the development and adoption of EHR technology and a nationwide network of interoperable health records software systems.[20] While this accomplishment remains unrealized for a variety of reasons,[21] one aspect of the government's efforts has included attempts to spur the adoption of patient portal technology. Towards this end, programs such as the Electronic Health Records Incentive Program (also known as "Meaningful Use") and its successor program have both included a mix of incentives and "requirements" to implement a patient portal.

---

[18] Heath, Sara, "Patient Portal Adoption Rates Hinge on Provider Viewpoints," January 27, 2016, available at http://patientengagementhit.com/news/patient-portal-adoption-rates-hinge-on-provider-viewpoints.

[19] Heath, Sara, "Patient Portal Adoption Rates Hinge on Provider Viewpoints," January 27, 2016, available at http://patientengagementhit.com/news/patient-portal-adoption-rates-hinge-on-provider-viewpoints.

[20] In 2006, the Office of Inspector General ("OIG") and Centers for Medicare and Medicaid Services ("CMS") modified the Federal Anti-kickback Statute Safe Harbor regulations and the Stark regulations, respectively, to permit the donation of EHR software under certain circumstances. 42 CFR § 1001.952(x); 42 CFR § 411.357(w), respectively. Neither regulatory change explicitly required that the donated software include a patient portal, however.

[21] A Government Accounting Office study found five general barriers to the establishment of a national, interoperable health information technology infrastructure. These are: (1) insufficiencies in standards for EHR interoperability; (2) variation in state privacy rules; (3) difficulties in accurately matching patients' health records; (4) costs associated with interoperability, and (5) need for governance and trust among entities. See, "Electronic Health Records: Nonfederal Efforts to Help Achieve Health Information Interoperability," GAO-15-817, September, 2015, available at http://www.gao.gov/assets/680/672585.pdf.

1. Meaningful Use

The government's earliest attempts to promote the adoption of patient portals by physicians and physician practices date back to 2010 and the publication of the original Stage 1 regulations for the Meaningful Use program.[22] This program created incentives for physicians to adopt and implement certified electronic health records technology ("CEHRT"), totaling up to $44,000 at its inception. This amount would be paid out over the course of several years, for eligible practitioners ("EPs") who successfully attested to being meaningful users of CEHRT each year.[23] In 2012, the incentives for attestation began to be reduced for EPs who were reporting for the first time that year. Beginning in 2015, the "carrot" of incentives was completely replaced with the "stick" of so-called "payment adjustments" (really, just a kinder, gentler way of saying "penalties").[24] These payment adjustments could amount to up to a 2.0% reduction to *all* Medicare Physician Fee Schedule payments made to the EP over the year.[25]

In practical terms, the Meaningful Use program set forth criteria for EPs to demonstrate meaningful use of CEHRT. These criteria were broken into two broad categories: core criteria, and "menu set" criteria. "Menu set" criteria required the EP to select five out of ten objectives to

[22] The government has also attempted to spur the adoption of EHRs and patient portals by hospitals. For example, Meaningful Use contains a measure requiring that over 50 percent of patients discharged by a hospital must be provided with an electronic copy of their discharge instructions and procedures. 75 Fed. Reg. 44355 (July 28, 2010). However, because the focus of this chapter is on physician practices, this chapter does not examine the Meaningful Use program's

[23] For more on Meaningful Use, see Shay, Daniel, "PQRS and its Penumbra," Health Law Handbook, (Gosfield, ed., 2012), pp. 87-119; Shay "To Quality and Beyond: Medicare and the Future of Quality Payment Programs," Health Law Handbook, (Gosfield, ed., 2016), pp. 31-66.

[24] Technically, this process began in 2013, since payment adjustments applied in 2015 were based on data reported in 2013.

[25] 42 CFR 414.90(e).

meet, while the EP was required to meet all fifteen core criteria objectives.[26] In the first iteration of the Stage 1 rules, several criteria could be met by EPs using a patient portal, although the precise language of the objectives did not explicitly require the use of a patient portal.

Core objective 12 required that an EP make available to patients a secure electronic copy of the patients' health records upon request. This measure would be met if at least 50% of the patients requesting an electronic copy were provided with such access within three business days.[27] The preface to the Final Rule for Stage 1 explained that one mechanism by which EPs could meet this objective was through the use of a patient portal.[28] Similarly, core objective 13 required that an EP make clinical summaries available to patients for each office visit. This objective would be met if the summaries were provided to patients for more than 50% of all office visits within three days.[29] As with core objective 12, CMS explained in the preface to the rule that this objective could be met through the use of a patient portal.[30]

Menu set objective 5 required that an EP provide patients with "timely electronic access to their health information" (e.g., lab results, problem lists, medications, allergies, etc.) within four business days of the information being available to the EP. This objective would be met by at least 10% of all patients seen by the EP being provided timely electronic access in accordance

---

[26] See, 75 Fed. Reg. 44567-44568, (July 28, 2010), for EP core and menu set criteria. These were originally published as 42 CFR § 495.6.

[27] 75 Fed. Reg. 44567, (July 28, 2010).

[28] However, CMS did not explicitly require the use of a patient portal to achieve this measure. In addition to portals, CMS described other methods of granting electronic access, including providing the information on a USB drive, a CD-ROM, or through a PHR. However, the information was required to be contained in the CEHRT adopted by the EP. 75 Fed. Reg. 44355, (July 28, 2010).

[29] 75 Fed. Reg. 44567-68, (July 28, 2010).

[30] 75 Fed. Reg. 44358, (July 28, 2010). Although, similar to core objective 12, other methods for communicating such information to patients were also acceptable, such as through a PHR, secure email, a CD-ROM or USB drive, or a paper copy.

with the timeframe established in the objective description. In discussing the menu set objective 5 requirements in the preface to the final rule, CMS noted that several commenters had been confused regarding the method by which such information should be provided to the patient. In response, CMS explained,

> "We believe we inadvertently created confusion by listing the examples of electronic media (CD or USB drive) in which this access could be provided. As many commenters inferred, *it was our intention that this be information that the patient could access on demand such as through a patient portal or PHR.*"[31]

In September, 2012, CMS published the first iteration of the Meaningful Use Stage 2 regulations, most of which went into effect in 2014.[32] The "2014 edition" revisions to Meaningful Use further promoted the adoption of portal technology. Both core and menu set objectives for Stage 1 were revised to more explicitly require the use of patient portal technology. For example, core objective 12, discussed above, was revised so that EPs were required to provide patients the ability to view *online*, download and transmit their health information within 4 business days of it being available to the EP.[33] Menu set objective 5, also discussed above, was removed from the menu set and became a core objective.[34]

---

[31] 75 Fed. Reg. 44356 (September 4, 2012), emphasis added. CMS also noted that it did not intend for this requirement to be another objective for providing patients with copies of their medical records on request. Instead, it explicitly distinguished between the "copy of electronic health information" objective, and the "provide electronic access" objective.

[32] 77 Fed. Reg. 53967 (September 4, 2012). Meaningful Use was originally broken into three Stages. The regulations governing each Stage were published gradually, rather than all at once, because at the publication of Stage 1, there was no way for anyone to be a Stage 2 or 3 meaningful user. Stage 1 was broadly described as having a goal of "data capture and sharing;" Stage 2 as "advanc[ing] clinical processes;" and Stage 3 as "improved outcomes." See, https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives. In broad strokes, each Stage increased the requirements to demonstrate meaningful use of CEHRT.

[33] 77 Fed. Reg. 54150 (September 4, 2012). Likewise, the measure to meet this objective changed to require that more than 50 percent of all unique patients seen during the reporting period were provided with timely (within 4 days) *online* access to their health information, although this was subject to the EP's discretion to withhold certain information.

[34] The former menu set objective was merged into the new core objective 12.

For the Stage 2 objectives, EPs were again required to meet all 17 of the core objectives, and select 3 menu set objectives out of 6. Among the core objectives, objectives 10[35], 11[36], 12[37], and 17[38] all required the use of a portal.[39] For example, in discussing core objective 17, CMS responded to a comment requesting clarification of the definition of a "secure message," by stating,

> "*We define a secure message as any electronic communication between a provider and patient that ensures only those parties can access the communication. This electronic message could be email or the electronic messaging function of a PHR,* ***an online patient portal,*** *or any other electronic means. However, we note that the secure message must also use the electronic messaging function of CEHRT in order to qualify for the measure of this objective.*"[40]

Likewise, in the preface to the Final Rule for Stage 2, when discussing Stage 2 core objective 10, CMS explained that "The patient must be able to access [health information] on demand, such as through a patient portal or personal health record (PHR)."[41] In addition, in a discussion of the measure by which EPs would be determined to have met the objective,[42] CMS responded to

---

[35] "Provide patients the ability to view online, download, and transmit their health information within 4 business days of the information being available to the EP." 77 Fed. Reg. 54153 (September 4, 2012).

[36] "Provide clinical summaries for patients for each office visit." 77 Fed. Reg. 54153 (September 4, 2012).

[37] A new objective, requiring that the EP "Use clinically relevant information from Certified EHR Technology to identify patient-specific education resources and provide those resources to the patient." 77 Fed. Reg. 54153, (September 4, 2012).

[38] Another new objective, requiring that the EP "Use secure electronic messaging to communicate with patients on relevant health information." 77 Fed Reg. 54154, (September 4, 2012).

[39] The menu set objectives were primarily focused on the capabilities of CEHRT, , such as menu set objective 4: the CEHRT was required to have the capability to identify and report cancer cases to a public health central cancer registry; or menu set objective 1: the ability to store the results of imaging tests, including explanations of the image and other accompanying information. 77 Fed. Reg. 54154, (September 4, 2012).

[40] 77 Fed. Reg. 54032 (September 4, 2012), emphasis added.

[41] 77 Fed. Reg. 54007 (September 4, 2012). In addition, rather than make this objective a menu set objective, CMS explicitly stated that the objective had been classified as a core objective because it was replacing two previous Stage 1 objectives, and therefore was not sufficiently different to justify placing it on the menu set.

[42] The measure to meet core objective 10 was twofold. First, more than 50 percent of the patients seen by the EP during the reporting period had to be provided with online access to their health information within 4 business days

additional commentary expressing concern that EHR vendors would be unable to make such capabilities available as part of CEHRT in time for the beginning of Stage 2 by noting that,

> "Many CEHRT vendors already make patient portals available that would meet the certification criteria and standards required for this measure. In fact, many vendors have already incorporated these capabilities into their CEHRT products in order to meet the measure of the Stage 1 objective to 'Provide patients with timely electronic access to their health information.'"[43]

The language of this response is significant, both in terms of outlining CMS' growing confidence in the spread of portal technology, and in terms of suggesting that such a spread was a direct result of vendors attempting to meet Meaningful Use requirements.

In 2015, CMS published a Final Rule which dramatically revised the Meaningful Use program.[44] This publication effectively eliminated Stages 1 and 2 as distinct Stages, and combined them into a single "Modified Stage 2." This final rule also included regulations for Stage 3. The new rule consolidated many of the separate objectives and measures from Stages 1 and 2, and combined them into a smaller number of measures.[45] Core and menu set objectives were condensed into 10 total objectives. These objectives included multiple measures, which had to be met to satisfy the objective.[46] In all of this consolidation, however, each of the core and menu set objectives that utilized patient portals were retained. Stage 2 core objective 10, survived as Objective 6: Patient Specific Education[47]; Stage 2 core objective 10 survived as

---

after the information was available to the EP. Second, more than 5 percent of the patients seen by the EP during the reporting period had to view, download, or transmit to a third party their health information.

[43] 77 Fed. Reg. 54009 (September 4, 2012).

[44] 80 Fed. Reg. 62761 (October 16, 2015).

[45] Including redesignating 42 CFR § 495.6 to 495.20.

[46] For a brief overview of the measures and objectives, see "EHR Incentive Programs for Eligible Professionals: What You Need To Know For 2016 Tipsheet," available at https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/2016_EPWhatYouNeedtoKnowfor2016.pdf.

[47] 42 CFR § 495.22(e)(6).

Objective 8: Patient Electronic Access (VDT)[48]; and, Stage 2 core objective 17 also survived as Objective 9: Secure Messaging.[49]

In addition, further highlighting CMS' commitment to incentivizing the adoption of portal and other health information technologies, CMS explained its decision to eliminate the portions of older measures that could be met through the use of faxed or printed paper copies. In response to a comment supporting the decision and highlighting that permitting Meaningful Use objectives to be met using paper-based methods could be hindering the development and adoption of digital technologies, CMS stated,

> "...We agree that limiting the focus of the program to only health IT solutions may encourage adoption as well as spurring further innovation among IT developers...While we do not in any way seek to limit the methods by which a provider may engage with a patient or share information, we do not believe that requiring providers to measure paper-based actions is consistent with the long-term goals of the [Meaningful Use] program. We believe that the requirements and focus of the program should be exclusively on leveraging HIT to support clinical effectiveness and patient safety, [health information exchanges], and quality improvement."[50]

Naturally, patient portals represent an integral aspect of this push to advance the use of health IT and digital technologies, as reflected in the objectives that employed and/or required patient portal technology.

2. The Medicare Incentive Payment System

In 2016, with the passage of the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA),[51] the landscape in federal health care programs abruptly shifted. Partially to offset

---

[48] 42 CFR § 495.22(e)(8), where "VDT" is an acronym for "view, download, transmit."

[49] 42 CFR § 495.22(e)(9).

[50] 80 Fed. Reg. 62783, (October 16, 2015).

[51] P.L. 114-10.

the elimination of the Sustainable Growth Rate, Congress created a new system to gradually move Medicare away from a pure fee-for-service payment system and towards a more value and quality oriented approach, known as the Medicare Incentive Payment System (MIPS), which emphasizes four categories for performance: quality, cost, clinical practice improvement activities, and meaningful use of CEHRT. Under MIPS, Medicare physician fee schedule payments to "MIPS eligible clinicians[52]" can be increased or decreased by a percentage amount each year, based on the MIPS eligible clinician's performance with respect to the four categories during the year, with each of the categories making up a specific portion of the MIPS eligible clinician's total score. Under the statute, meaningful use of CEHRT makes up 25 percent of the overall score.[53]

Regulations for MIPS were published in November, 2016.[54] The regulations altered some references from the statute, using "advancing care initiatives" instead of "meaningful use of CEHRT" and "improvement activities" instead of "clinical practice improvement activities."[55] The new MIPS quality payment program continues CMS' focus on the use of patient portals as part of an overall effort to spur the use of health IT.

The Meaningful Use objectives relating to patient portals in Meaningful Use survive under MIPS; thus, patient access and VDT, patient-specific education, and secure messaging all

---

[52] The MIPS Final Rule changed terminology from "Eligible Provider" or "EP" to "MIPS eligible clinician." 81 Fed. Reg. 77014 (November 4, 2016). This is in spite of the fact that the MACRA statutory language refers to "MIPS EPs."

[53] 42 USC § 1395w-4(q)(5)(E)(i)(IV). For more on MIPS, see Shay, Daniel, "To Quality and Beyond!: The Present and Future of Medicare's Physician Quality Reporting Systems," Health Law Handbook, Alice G. Gosfield, ed. 2016, pp.31-66.

[54] 81 Fed. Reg. 77008 (November 4, 2016).

[55] 81 Fed. Reg. 77010 (November 4, 2016).

remain as part of the "advancing care initiatives" requirements.[56] The former objectives themselves have been consolidated, however. They survive now as two overarching objectives: (1) Patient Electronic Access – whereby the MIPS eligible clinician provides patients with timely electronic access to their health information and patient-specific education; and, (2) Coordination of Care Through Patient Engagement – whereby the MIPS eligible clinician uses CEHRT to engage with patients about the patient's care. The measures, too, survive, but are now organized somewhat differently.[57]

However, the push for adoption and use of patient portals is not merely limited to the surviving Meaningful Use objectives and measures. MIPS expands the opportunities for eligible clinicians to use patient portals in satisfying measure requirements. Under the MIPS Final Rule, the improvement activities category accounts for 15% of the MIPS eligible clinician's total score.[58] Several objectives within the improvement activities category may be met using measures that incorporate the use of a patient portal. For example, under the population management subcategory,[59] eligible clinicians may "use reminders, and outreach (for example,

---

[56] 81 Fed. Reg. 77228 (November 4, 2016).

[57] For example, the measures for the Patient Electronic Access objective now are: (1) that at least one patient is provided timely access to view online, download, and transmit his or her health information, and that the MIPS eligible clinician ensures that the patient's health information is available for the patient to access using any application of their choice that is configured to meet the technical specifications of the Application Programming Interface (API) in the MIPS eligible clinician's CEHRT; and (2) that the MIPS eligible clinician use clinically relevant information from CEHRT to identify patient-specific educational resources and provide electronic access to those materials to at least one unique patient seen by the clinician during the reporting period. For the Coordination of Care Through Patient Engagement objective, the measures require: (1) that at least one patient seen by the MIPS eligible clinician actively engage with the EHR made accessible by the MIPS eligible clinician, which could be satisfied through a combination of VDT using the EHR software, the use of an API, or a combination of the two; and, (2) at least one patient must be sent a message or replied to using a secure message through the electronic messaging function of CEHRT. In essence, the measure for Meaningful Use Objective 8 was split into two separate measures for two separate objectives, while two other objectives became measures themselves.

[58] 42 CFR § 414.1355(b)(1).

[59] The Improvement Activities category is required, by statute, to have certain subcategories, including those described above. 42 U.S.C. § 1395w–4(q)(2)(B)(iii). See also, 81 Fed. Reg. 77188 (November 4, 2016).

phone calls, emails, postcards, patient portals, and community health workers where available) to alert and educate patients about services due; and/or routine medication reconciliation."[60] Likewise, under the beneficiary engagement subcategory, there are two opportunities to use a patient portal. First, the eligible clinician may offer access to an enhanced patient portal that can provide up-to-date information regarding relevant chronic disease health or blood pressure control, and which includes interactive features that allow the patient to enter health information and/or enables two-directional communication regarding medication changes and adherence.[61] Eligible clinicians may also create enhancements and provide ongoing, regular updates and use of websites and tools that include consideration for compliance with section 508 of the Rehabilitation Act of 1973, or for improved design for patients with cognitive disabilities -- including designing a patient portal or website that is compliant with section 508.[62]

Further encouraging the use of patient portals, CMS permits eligible clinicians to essentially "double dip" by engaging in these activities. Within the MIPS Final Rule itself, CMS explains that the activities described in Table 8 of the Final Rule[63] can be tied to the advancing care information performance category. CMS provided an example of how this would actually work in practice. For example, Table 8 includes an improvement activity in which a MIPS eligible clinician would provide 24/7 access for advice about urgent and emergent care. CMS explained,

> "The Secure Messaging measure under the advancing care information performance category requires that a secure message was sent using the electronic messaging function of CEHRT to the patient...If secure messaging functionality is used to provide 24/7

[60] 81 Fed Reg. 77205, 77821-77822 (November 4, 2016).

[61] 81 Fed. Reg. 77208, 77825 (November 4, 2016).

[62] 81 Fed. Reg. 77285 (November 4, 2016).

[63] 81 Fed. Reg. 77203-77209 (November 4, 2016).

> access for advice about urgent and emergent care (for example, sending or responding to secure messages outside business hours), this would meet the requirement of using CEHRT to complete the improvement activity and would qualify for the advancing care information bonus score."[64]

CMS' commitment to the advancement of patient portal usage by health care providers is clear. From the earliest days of the Meaningful Use program through the current MIPS measures, CMS has taken and continues to take steps to incentivize the adoption of such technology by Medicare participating providers, most recently by continuing past efforts while simultaneously offering additional MIPS scoring bonuses for use of patient portal software.

III. Legal Issues

Even without the pressure of Medicare-driven payment adjustments driving physicians towards adoption of patient portal technology, physicians may simply see the benefits of using patient portals as worth the investment. There are, however, several areas of legal concern that can arise with patient portals. These include issues with agreements – both between the physician practice and software vendors, and between the practice's patient and either the physician or vendor; questions surrounding HIPAA compliance; and patient records ownership issues.

A. Contracts.

Unlike EHR software generally, physician portals implicate the use of two different agreements: a vendor/practice license agreement, and another use agreement with the patient (either between the patient and the vendor, or the patient and the practice) often referred to as a "Use Agreement" or "Terms of Use." The practice's license is usually similar to an EHR software license agreement. With "tethered" patient portals, the practice's license is, in fact, the EHR software license agreement, since the portal is usually being licensed as part of an overall

[64] 81 Fed. Reg. 77203 (November 4, 2016).

software suite.[65] However, an EHR software license agreement including a "tethered" patient portal may still have aspects that are unique and deserve special consideration beyond simply what is discussed in a typical license agreement.

1. Vendor/Practice Agreements

In some cases, the EHR license agreement may not directly address the use of the patient portal, simply referring to it as part of the overall software package licensed to the practice. This may appear in a "Statement of Work" or some other summary document outlining the specific software modules licensed. In other cases, requirements surrounding the portal may be part of the main body of the agreement, or may be attached as an Exhibit or Addendum.

When the license agreement does address the portal functions of the EHR, it may impose specific duties on the practice in relation to use of the portal software. For example, some EHR license agreements require that the practice notify the vendor in the event that the practice discovers the unauthorized access of the portal. This language may be worded broadly, in a manner that would implicate (1) access by someone who is not the patient, using the patient's login and password; (2) access by a third party using malware or other hacking methods; or, (3) access by a member of the practice's workforce exceeding the scope of the workforce member's duties. Even if the practice has no concerns about complying with such a requirement, it is still important to confirm with the vendor the intended scope of the provision, which may necessitate revising the language to be more precise.

---

[65] For further discussion of common clauses in EHR software license agreements, see, Shay, Daniel, "A Primer on Electronic Health Records License Agreements," Health Law Handbook, Alice Gosfield, ed., 2006, pp. 425-457; Shay, Daniel, "Downstreamed Physician EHR License Agreements: Understanding the Ebb and Flow," Health Law Handbook, Alice Gosfield, ed., 2008, pp.45-76.

An EHR license agreement may also require that the practice provide a Terms of Use agreement to its patients, containing certain provisions required by the vendor. The practice may or may not have the freedom to add to the language of this Terms of Use agreement. Consider the following example:

> "*Patient User Terms of Use*. Customer understands and agrees that Patient Users will be required to register to be able to access the Patient Portal. During the registration process or anytime thereafter, Patient Users may be asked to accept terms of use and a privacy policy related to their access to the Patient Portal (collectively "Patient Portal Terms"). At a minimum, the Patient Portal Terms must include those provisions which are pre-populated in the Patient Portal Terms by [Vendor] and which [Vendor] may change from time to time. Customer is fully and solely responsible for including any additional terms and maintaining such additional terms; provided, however, that such terms shall not conflict with this Agreement or the [Vendor] pre-populated Patient Portal Terms or impose any obligations on [Vendor]."

Such language would naturally prompt the practice or its attorney to request a copy of the Patient Portal Terms, to evaluate the terms of such documentation. In this case, the privacy policy would need to be reviewed for compliance with the requirements of HIPAA, especially in relation to the practice's own Notice of Privacy Practices and obligations as a covered entity. Moreover, the practice would want to review the specific language of the Terms of Use agreement to ensure that there were no requirements that would conflict with the practice's own intentions and goals in providing the portal to its patients.

Terms relating to the use of patient portal functions may also explicitly state that the practice is responsible for defining the content that is made available to patients through the portal. Of course, the functionality of the portal itself might otherwise restrict what can be shared through it. Similar to EHR license agreements in general, the license may also explicitly state that the vendor may de-identify and use patient information, often without restriction. In such circumstances, the practice or its attorney might want to inquire as to the uses of de-identified information. For example, the vendor might use the information for internal quality

improvement purposes, or it might commercialize the data, selling it (as part of an aggregated set of data from multiple providers and practices) to a third party such as a pharmaceutical company.

2. Patient Terms of Use Agreements

As discussed above, practices utilizing patient portals also usually have a separate Terms of Use agreement between either the practice and the patient, or the software vendor and the patient. These agreements vary wildly with respect to the type of language they use (e.g., "legalese" vs. "plain language"), their level of detail, length, and the legal focus of the documents. Put simply, there is no single, common style across all Terms of Use agreements. However, these agreements tend to adopt three general styles: (1) an agreement that is designed more to protect the practice and/or the software vendor (the "legalistic style"); (2) an agreement designed primarily to inform the patient/user of what they may expect from their use of the patient portal (the "informal style"); and (3) a hybridization of the first two styles.

The "legalistic style" of Terms of Use agreements often appears very similar to an EHR software license agreement. It is typically structured like a formal contract, containing paragraph numbers and headings, subsections, and common contractual terms such as: indemnification; confidentiality (with respect to the software itself, including its interface design, features, etc.); choice of law and venue; representations and warranties; and all-capitalized waivers and bold-faced, all-capitalized disclaimers of liability. This approach usually includes clauses designed more to protect the vendor from liability, to protect its intellectual property, and to serve almost as a sub-licensing agreement with the patient.

By contrast, the "informal style" usually does not contain many of these elements. It is often not structured like a formal contract, lacking paragraph headings or section numbers. It is also usually written far more with the lay reader in mind. This style of document is usually also

much shorter than the other two, in some cases amounting to only approximately two pages of 11- or 12-point font text. This style may include a general description of how the patient portal functions, although the description will not be especially technical. It may also include recommendations about how to use the software, although they will not necessarily be phrased as contractual obligations. For example, consider the following language from one Terms of Use agreement drafted in the "informal style":

> **"The Patient Portal is not intended to provide internet based diagnostic medical services. The following limitations also apply:**
>
> - If you lose your password or username, you may request a new one through the Patient Portal or in person at the office by providing valid identification.
>
> - Always remember to log out and close your browser when you are finished accessing password protected patient portal services. This prevents someone else from accessing your personal information."[66]

The language quoted above comes from a two page document for a family medicine physician practice. The agreement also includes a brief patient acknowledgement of the risks and benefits relating to use of the portal, and that the patient's use of the portal is voluntary. It also includes a signature line and date line. However, these are the most formal aspects of the document; the remainder of the document includes a description of the portal's features, and instructions on how to access the portal, an instruction to view the practice's HIPAA policies (available separately). Its focus is far less on establishing the terms of a license to use the software between the vendor or practice and the patient, and far more as a plain-language document to inform the patient of what he or she can expect in using the portal.

The "hybrid style" of Terms of Use document blends elements of both the formal and informal styles described above. Often, such Terms of Use agreements will be structured like a

[66] Family Practice Group Patient Portal User Agreement. Emphasis in the original document. Available at http://www.familypracticegrouppc.com/wp-content/uploads/2015/05/Patient-Portal-Agreement_5.12.15.pdf.

formal contract, including section headings and numbering, and may include sections relating to, for example: term and termination, disclaimers of liabilities and warranties, indemnification clauses for the patient's/user's improper use of the portal software, and representations and warranties. However, this style of Terms of Use document often uses less formal language, referring to the user in the second person as "You" rather than in the third person as "Patient" or "User," and describing matters such as how the user may register to use the portal, and suggestions for how to ensure privacy of user data.

For example, one hybrid style Terms of Use agreement for a patient portal from a group of health clinics includes both a bold-faced, all-capitals section regarding limitation of liabilities; a choice of law clause; indemnification terms; as well as a section regarding privacy and protection risks, which states:

> "In order to reduce the privacy and security risk associated with the use of the [Group] Patient Portal for communicating your personal health information, please consider implementing the following procedures:
>
> - Keep your email and password private. Do not share your password with anyone.
> - Ensure [Group] Health Services has your correct email address. If your email address changes, please notify [Group] of the change.
> - Use a screen saver or close your [Group] Patient Portal when you have finished reviewing information. Do not leave protected health information and/or messages on the screen for others to read.
> - Do not store protected health information on a public computer or on your employer-provided computer; otherwise personal information could be accessible or owned by your employer."[67]

In spite of the stylistic differences between "Terms of Use" agreements, they do share some common language. For example, most include language that specifically instructs users

[67] MyAltaMed Patient Portal End User Agreement, Section 14. Available at http://altamed.org/files/Static%20Page%20Files/End%20User%20Agreement-ENG.pdf.

how *not* to use the patient portal. Almost all "Terms of Use" documents specifically state that the patient portal is not appropriate for use in an emergency, and instruct the patient to contact emergency services or dial "911" in such circumstances. They may also state that the patient portal does not offer internet-based diagnosis, treatment, triage, or other services, or should not be used as a substitute for an office visit.[68] In many cases, they also restrict access for minors, and only permit individuals aged 18 or over, or guardians of minors to access the portal.

Many also include a clause outlining the expected response times for patient inquiries, usually between 24 hours and 72 hours. However, these clauses may vary in the degree of formality and detail they provide. For example, compare the following excerpts from three separate "Terms of Use" agreements, regarding response times:

Example 1:

> "The MyAltaMed Patient Portal is checked by AltaMed staff during normal office hours of operation, which are 8:00 a.m. to 5:00 p.m. Monday through Friday, with the exception of holidays. Reasonable efforts will be made to respond to non-urgent requests and e-mail inquiries within a reasonable time after receipt. You are responsible to monitor whether you have not received a response and should call the office in the event that you do not receive a response."[69]

Example 2:

> "Reasonable efforts will be made to respond to email and telephone inquiries within one (1) business day, but no later than three (3) business days, after receipt. Response time may be longer if the Patient Portal service is interrupted for maintenance, upgrades, or emergency repairs related to events beyond our control. In this respect, you agree not to

[68] See, Wayne Memorial Hospital Patient Portal User Agreement, available at http://www.waynehealth.org/patients/portal/user-agreement; Montrose Memorial Hospital Patient Portal User Agreement, available at http://montrosehospital.com/Resources/MMH-PatientPortalUserAgreement.pdf. In one instance, the Terms of Use agreement explicitly stated that the portal could not be used for requests for narcotics or controlled medications. See, Family Practice Group Patient Portal User Agreement, available at http://www.familypracticegrouppc.com/wp-content/uploads/2015/05/Patient-Portal-Agreement_5.12.15.pdf.

[69] MyAltaMed Patient Portal User Agreement, available at http://altamed.org/files/Static%20Page%20Files/End%20User%20Agreement-ENG.pdf.

hold Montrose Memorial Hospital, Inc. in any way liable or responsible to you for such modification, suspension or disruption of the portal."[70]

Example 3:

"It may take 72 hours to receive a response to a message sent through the Patient Portal. If you do not receive a response within 72 hours you should contact the office at [telephone number]."[71]

The first Example includes the greatest amount of detail with respect to the times of day during which the user may expect a response, but provides little more than assurances of "reasonable efforts" to respond within a "reasonable time" after receipt of a non-urgent email request. Example 2 also states that the patient can expect "reasonable efforts" to be made in responding, but provides a timeframe that is considered "reasonable": one to three business days after receipt. However, there is no statement regarding the hours of operation of the practice's response staff. The final example provides even less detail, simply stating that patients should follow up with the practice if a response is delayed longer than the stated 72 hour window.

Legally and practically speaking, there are benefits and drawbacks to each approach in overall style of Terms of Use agreement. A more formalistic Terms of Use agreement certainly will be better to protect the physician practice and/or software vendor in the event of a dispute with a user. It may also protect the practice from liability from the software vendor. If, for example, the Terms of Use agreement includes an explicit prohibition against reverse-engineering the patient portal software, or restricts the use of trademarks or copyrighted information contained within the patient portal, then the physician practice will be much better positioned to disclaim responsibility if a patient or user engages in such behavior. Absent such

[70] Montrose Memorial Hospital Patient Portal User Agreement, available at http://montrosehospital.com/Resources/MMH-PatientPortalUserAgreement.pdf.

[71] Family Practice Group Patient Portal User Agreement, available at http://www.familypracticegrouppc.com/wp-content/uploads/2015/05/Patient-Portal-Agreement_5.12.15.pdf.

language, the software vendor is more likely to sue or at least demand some form of damages from the physician practice, especially since the practice is the party with the proverbial "deep pockets."

On the other hand, these documents are meant to be read by lay people, not lawyers. Especially for patients who may already be reluctant to use a patient portal in the first place, a wall of "legalese" text may either be ignored, or may act as a barrier to entry by the patient. Even though patients – as consumers of online products – are likely familiar with "click to proceed" agreements, as a general matter they may be less willing to read (or scroll) through several pages of formal contractual language merely to access the results of a blood glucose test. At best, a more formalistic style of Terms of Use agreement might prompt the patient to simply click "I Accept" without actually bothering to read the document, which could lead to disputes in the future. Towards this end, the more "informal style" may be more helpful, and may help promote patient engagement and use of the patient portal.

The hybrid approach requires finding the right balance of legally defensive language and ease of understanding, similar to how well drafted contracts strike a balance between specificity and flexibility. While finding the right mix of these elements may be difficult, the hybrid style may be the best approach to crafting a Terms of Use agreement, assuming the vendor does not already require the practice to use a specific form. Without adequate legal protection, the practice may find itself needlessly exposed to risk. Likewise, without being understandable to the lay reader, patient adoption may suffer or patients may not effectively understand how to use (and how *not* to use) the portal.

Alternatively, the physician practice could provide educational materials written in clear, concise lay terms, which offer instruction to the patient on how to effectively use the portal and

protect the privacy of their information, while also requiring patients to execute a more formalistic Terms of Use agreement. This would achieve the same goals as the hybrid approach, albeit in a manner that involves more paperwork.

B. HIPAA and Related Concerns

Patient portal software falls squarely within the scope of HIPAA and its regulations, since they permit both the transmission and storage of EPHI. All three of the main "Rules" under HIPAA – the Privacy Rule, Security Rule, and Breach Notification Rule – are potentially implicated in the use of patient portals.

1. Login/Credential Security Issues

When a patient first attempts to obtain access to a physician practice's patient portal, the practice faces a critical decision in terms of how to begin the process of establishing patient access rights. The issue of granting patients access to patient portal software implicates several aspects of the Security Rule.[72] With these requirements in mind, the practice must first consider whether to permit the patient to sign up for the portal entirely online and in the privacy of their own home, whether to require that the patient complete paperwork at the practice's office before granting access, or whether to take a hybrid approach to the process.

Of course, the patient likely will prefer to be able to establish access online, at home (or elsewhere). This approach may also be attractive to the practice, because it requires the patient to spend less time at the office, completing paperwork. As a practical matter, however, this approach does mean that if the patient faces any difficulty in establishing their credentials at home, they will need to contact the practice for help. By contrast, in-person/in-office portal

[72] Specifically, the requirements to establish administrative and technical safeguards. With regards to administrative safeguards requirements, the practice must consider its obligations under the "information access management" requirement. 45 CFR § 164.308(a)(4). With regards to the technical safeguards, the practice must consider its obligations under "access control" and "person/entity authentication." 45 CFR §§ 164.312(a), and (d), respectively.

registration may be expedited by practice staff, who are already familiar with the portal registration process. Another option is for the practice to provide the patient with instructions regarding how to register for access, and allow the patient to do so at home.

One method that can strengthen the security of at-home registration for patients is two-factor (or multi-factor) authentication. As a general matter, two-factor authentication requires that the user authenticate themselves using two pieces of evidence to demonstrate that the user is who they claim to be. By way of comparison, single-factor authentication would involve a user demonstrating their authority to access a system by giving a correct password. Two-factor authentication could require a password and an additional piece of evidence such as something uniquely provided to the individual by the authorizing entity. In the simplest terms, a bank ATM card uses two-factor authentication: accessing money in the account from an ATM requires that the user have (1) the physical bank card (or card number), and (2) the pin number.[73] Physician practices can and often do employ similar mechanisms, such as generating a unique user ID for their patients, a special log-in code or PIN in addition to a user-created password, the answer to a secret question, or some other mechanism.

Issues surrounding authentication also implicate how the practice must respond to circumstances where authentication factors must be re-established by the users. If a user loses or forgets a password, PIN, or other authentication factor, how will the practice respond? Such circumstances create an additional requirement to authenticate the user purely to generate a new authentication factor that can be used in the future. The practice may require the patient to call or come in to the office to accomplish this, or to authenticate themselves using a different factor (e.g., answering a secret question used only for password resets).

[73] For more on multi-factor authentication, see https://en.wikipedia.org/wiki/Multi-factor_authentication.

With the rapid spread of smartphones and the use of mobile applications, the practice may choose to offer the use of an app so that patients may access the patient portal from their smartphones or tablets. Such an option may prove extremely attractive to patients who are frequent users of such devices, especially since a mobile application provided by the practice's software vendor will likely offer secure communication, as opposed to the use of unsecured communications like texts. Of course, this also implicates HIPAA security concerns regarding authentication. However, the use of a smartphone or tablet and a mobile application may also open up additional avenues for the practice to use authentication factors not otherwise available to users accessing the patient portal from a traditional PC.

Many smartphones and tablets now allow for the collection of biometric data, such as fingerprint scanning through a touch-pad on the device, or facial or retinal recognition through the use of the device's camera. Of course, the practice's software vendor must make available a mobile application in the first place, and that application must also be programmed to permit such biometric data to be used for authentication, but such an approach may prove more secure than the use of PINs or passwords which are either too difficult to remember, or worse, are easily remembered but capable of being easily guessed or hacked.

However, legally speaking, there is ultimately only so much that a practice can do to ensure the security of the patient portal (and any systems connected to it). If the patient or end user ultimately permits an unauthorized person to use their credentials to access the system, there is little the practice can do.[74] Nevertheless, the practice should attempt to educate patients/authorized users to protect their access credentials, and require the patient to

[74] However, the practice still has a duty under the HIPAA Security Rule to periodically audit its own systems containing EPHI. 45 CFR §§ 164.308(a)(1), 164.312(b). Therefore, the practice should conduct or arrange for automated audits that can detect aberrant behavior or strange patterns in patient portal accounts, if feasible. Of course, this will depend on the capabilities of the software the practice utilizes.

acknowledge that anyone to whom the patient willingly grants access will be able to see the contents of the patient's records. This language can be included in the Terms of Use agreement. The practice may also want to consider including a requirement that the patient inform the practice if the patient suspects any unauthorized access has occurred.

2. Patient Rights: Access and Amendment

Under the HIPAA Privacy Rule, patients have a right to access their PHI; more specifically, they have the right to "to inspect and obtain" a copy of their PHI.[75] This requirement does have certain exceptions, however, including the content of psychotherapy notes and information compiled in anticipation of a criminal, civil, or administrative proceeding.[76] In addition, a health care provider may deny the patient access to their PHI when, among other reasons, the health care provider determines that such information would endanger the life or physical safety of the patient or another person.[77]

The Privacy Rule, also grants the patient a right to request amendments to their medical record.[78] Similar to the right of access, a health care provider may deny the patient's request to amend the record for limited reasons. These include where the information is accurate and complete. The health care provider may also deny the patient's request in part, and grant the request in part.[79]

Patient portals, and the PHI stored and made available to patients through the use of such software, naturally implicate this requirement. Physician practices must decide precisely what

---

[75] 45 CFR § 164.524.

[76] 45 CFR § 164.524(a)(1).

[77] 45 CFR § 164.524(a)(3).

[78] 45 CFR § 164.526.

[79] 45 CFR § 164.526(d).

information to provide to the patient through the portal. Typically, the portal will not grant access to the patient's full medical record, and will only provide certain information (e.g., laboratory results, medication lists, problem notes, messages between the patient and their physician, diagnostic images, etc.). Some of this may be determined purely by the portal software's capabilities; it may not be able to display all of the information that might be contained in the patient's record. The practice must – unless the denial meets one of the exceptions described in 45 CFR § 164.524(a) – provide the patient with access to their full record on request.[80] However, to the extent that the physician practice may determine what information the portal displays, it faces a decision in terms of just how much information to provide the patient through the portal, without at least requiring that the patient make a specific inquiry for a full copy of their medical record.

For example, suppose the patient's medical record includes notes from the physician that either express disbelief, or question the patient's veracity with respect to smoking status, or how many drinks the patient consumes per day. This information likely would not be included in the information that is made available regularly through the portal, since it would likely only invite disputes from the patient. However, if the patient requests a copy of their full medical record, the physician will have to produce the information, unless doing so would risk endangering the patient's or another person's life or physical safety. Similarly, if the patient requested that the physician's note be revised so as to eliminate the physician's disbelief of the patient's statement, the physician could reasonably deny the request, provided that the note itself was accurate and

[80] This requirement also applies to the "view, download, transmit" measure in MIPS. However, the VDT requirement under Meaningful Use/MIPS does permit the physician to exercise his or her discretion with regards to the exceptions contained in 45 CFR § 164.524.

reflected the physician's professional judgment, which was necessary to be preserved in the medical record.

The federal government's drive towards increasing patient engagement, especially through patient portals, makes these issues all the more relevant for physicians. Because programs like MIPS require that patients be provided with electronic copies of their medical records upon request, the use of a patient portal makes it that much more likely that a patient will request that the practice provide such information electronically through the portal. Even when the portal itself does not display the requested information in the normal interface, the data might be transmissible to the patient as an attachment to a secure email sent through the portal. Towards this end, physician practices need to confront how they will respond to such requests.

In addition, physician practices should consider ensuring that Terms of Use agreements explicitly state that the information presented on the portal is not the patient's full medical record, and that the patient may request a copy of their full medical record, which will be provided in the format requested by the patient. In fact, Terms of Use agreements often include such language, especially those using an informal or hybrid style.

3. Additional HIPAA Considerations

The use of a physician portal necessarily involves the transmission of EPHI across electronic communications networks, subject to the HIPAA Security Rule. Therefore, a physician practice using a patient portal will need to take the use of the software into account as part of its security risk assessment (SRA).[81] Recent years have seen a rise in enforcement by the Department of Health and Human Services Office for Civil Rights (OCR), especially with

[81] Required under 45 CFR § 164.308(a)(1)(ii)(A).

respect to the Security Rule, and, since 2012, targeting small physician practices.[82] One need only examine the OCR's Resolution Agreements to discover that an absent or ineffective SRA regularly plagues health care providers.[83] The OCR has described the performance of an SRA as "foundational" and as the first step in identifying and implementing safeguards that comply with and carry out the requirements of the Security Rule.[84] Without one, a covered entity cannot know where its risks and vulnerabilities lie, and therefore cannot draft effective policies to reduce or eliminate such risks. As the government has explained, covered entities must review and revise their SRA whenever they modify their electronic infrastructure.[85] Thus, adding a patient portal – if one was not initially included in the EHR software suite – will require updating the practice's SRA. The results of the SRA should also lead the practice to update its relevant policies and procedures relating to its administrative, physical, and technical safeguards, with respect specifically to the portal software itself.

The physician practice will also have to enter into a business associate agreement (BAA) with the portal software vendor. This may be included in the license agreement for the overall EHR software package, or as a separate document for a standalone patient portal. In virtually every instance, the vendor will insist upon the physician practice signing the vendor's form of BAA. Provided that the agreement otherwise meets the requirements of the Privacy Rule[86], and

---

[82] For more on challenges relating to SRAs, see, Shay, Daniel, "HIPAA and Meaningful Use Audits and the Security Risk Analysis Nexus," Health Law Handbook, Alice G. Gosfield, ed., 2015, pp. 429-464.

[83] OCR Resolution Agreements may be found at https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html?language=es.

[84] "Guidance on Risk Analysis Requirements Under the HIPAA Security Rule," p.1, July 14, 2010, at http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

[85] "Top 10 Myths of Security Risk Analysis," HealthIT.gov, at http://www.healthit.gov/providers-professionals/top-10-myths-security-risk-analysis.

[86] 45 CFR § 164.504(e).

otherwise contain no objectionable language, there is nothing wrong with signing the vendor's BAA. As a practical matter, the vendor will likely refuse to do business with the practice if the practice insists upon the vendor signing the practice's own BAA. This is because the vendor does not wish to keep track of variations in its obligations between each particular BAA presented by each practice; it is simply easier for the vendor to insist that the practice use its single form.

C. Patient Records Ownership Concerns

The use of patient portals may raise additional issues surrounding the ownership of patient records. In the past, this question was less of a concern for both physicians and patients. Patient medical records came primarily in paper form, and patients either did not want to, or simply had not considered the option to obtain and maintain such documentation on themselves. However, with the development of electronic medical records and electronic imaging, and with the proliferation of computers and internet communications, the storage and transmission of patient medical records has become much easier. In addition, patients themselves have become more involved in their own care, leading to more desire to at least have access to copies of their own records. Federal and state laws have also established that patients have rights to copies of their records, thereby creating even more of a sense of "ownership" among patients.

At first blush, one might assume that there is a clear answer to the question of who owns a patient's records: the health care provider or the patient themselves. In fact, the answer is somewhat murky, and there is no single, national standard for patient record ownership. Twenty-two states have statutes or regulations which explicitly state whether patients or

providers own the patient's medical records.[87] Of these, only New Hampshire explicitly states that patients own their records[88]; the remaining state laws and regulations all make the provider the owner of medical records.[89] Other states do not have statutory or regulatory language regarding the issue of ownership, but have addressed the matter under state common law.[90]

However, many states also have patient "bills of rights" or other laws which grant the patient a right to access copies of their own medical histories.[91] In addition, HIPAA grants patients rights including rights to restrict disclosure of their PHI[92], rights of access to copies of

---

[87] See, "Who Owns Medical Records: 50 State Comparison," HealthInfoLaw.org, available at, http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison. The states are: Alaska, California, Florida, Georgia, Indiana, Kansas, Louisiana, Maryland, Mississippi, Missouri, New Hampshire, New Mexico, North Carolina, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Utah, Virginia, and Wyoming.

[88] The statute states in part "Medical information contained in the medical records at any facility licensed under [New Hampshire's hospital licensure laws]shall be deemed to be the property of the patient." N.H. Rev. Stat. § 151:21(X).

[89] For example, Pennsylvania's hospital licensure regulations state that "Medical records are the property of the hospital, and they shall not be removed from the hospital premises, except for court purposes. Copies may be made available for appropriate purposes such as insurance claims, and physician review, consistent with [regulations governing records confidentiality.]" 28 Pa. Code § 115.28.

[90] See, Holtkamp Trucking Co. v. Fletcher, 932 N.E.2d. 34 (Ill. App., 2010), a workers compensation case wherein the state workers compensation commission attempted to subpoena the physician's records. The Illinois Court of Appeals stated "The subpoena commanded defendant to mail medical records to plaintiff's attorney. The subpoena might just as well have commanded defendant to mail a stethoscope to plaintiff's attorney, because the medical records were defendant's property, the same as the stethoscope." Id., at 43-44. See also, McGarry v. J.A. Mercier Co., 262 N.W. 296 (Michigan, 1935), a case in which the Michigan Supreme Court stated that a physician's refusal to provide an employer who contracted for an employee's health care copies of X-ray images, stating "In the absence of agreement to the contrary, such negatives are the property of the physician or surgeon who has made them incident to treating a patient." Id., at 297.

[91] See, 10 NYCRR § 405.7(b)(24); 16 Del. Code § 1121(19); OAR § 847-012-0000.

[92] 45 CFR § 164.522.

their PHI[93], rights to request amendments to their PHI[94], and rights to accountings of disclosures of their PHI[95].

Given the broad scope of federal and state rights for patients, the possibility exists that a patient may assume that they own the records of their care. With increased access to such records through patient portals, patients may begin to adopt an attitude – however unfounded in light of state law – that they own the records of the care they received. In states where no laws explicitly state who owns the records, this may create friction between the patient and the physician, if the patient attempts to assert ownership (rather than merely a right to a copy of their records). Regardless of who actually is determined to retain a property right to the records themselves, the physician will certainly have a custodial role to play with respect to the records, and at least will likely have a right to retain copies to respond to payor requests and malpractice claims against the physician. Still, physician practices and their attorneys may wish to investigate state law regarding actual ownership of patient medical records, if only to assist in drafting an effective Terms of Use agreement that will notify the patient of state law.

V. Conclusion

Patient portals are fast becoming a fact of life for physician practices. The federal government has sought to hasten their implementation by physician practices in previous years through the incentives and penalties associated with the Meaningful Use program. These efforts continue under the MIPS program, which ultimately ties physician fee schedule payments to MIPS performance, with an eventual upwards or downwards adjustment of up to 9.0%. With

[93] 45 CFR § 164.524.

[94] 45 CFR § 164.526.

[95] 45 CFR § 164.528.

such a significant potential penalty for practices that score poorly, it is likely that those physician practices which do not already have a portal in place will obtain one in the near future.

Doing so will expose physician practices to a range of new legal issues, such as the need for a review of a patient portal vendor software license agreement or an amendment of an existing EHR software license agreement to add portal functionality, and for a well-drafted Terms of Use agreement. In addition, physician practices will need to address HIPAA compliance requirements with respect to the portal software itself, and may need to confront questions regarding patient records ownership.

All of these issues can be daunting for physician practices, especially when a significant portion of their Medicare income is on the line, and when faced with risks associated with HIPAA compliance in an environment of increasing enforcement and oversight efforts. It is up to knowledgeable health care legal counsel to assist these physician practices in navigating the pitfalls involved in patient portal implementation.