12 Hous. J. Health L. & Policy 171

Houston Journal of Health Law & Policy
ISSN 1534-7907

WHEN PATIENTS INTERACT WITH EHRS: PROBLEMS OF PRIVACY AND CONFIDENTIALITY

Leslie P. Francis*

Increasing individuals' understanding and participation in their health care is good for their health and for the health care system. If people know more and become more involved, they will make better choices about health behaviors. They may also make more prudential choices about the quality and costs of care. So goes the argument for encouraging and enhancing technologies that allow interaction between patients and their providers, including patients' access to their health records. These technologies have been characterized by the Obama Administration as a "key element" of innovation strategy.[1] Proposals for regulations that would encourage patient-interactive technologies—such as rapid patient access to hospital discharge information—evoke lively and continuing controversy.[2] With electronic health records (EHRs) and panoplies of

* J.D., Ph.D. Associate Dean for Faculty Research and Development, Alfred C. Emery Distinguished Professor of Law, and Distinguished Professor of Philosophy at the University of Utah.

1 The White House, Consumer Data Privacy in a Networked World: a Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy 20 (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

2 For example, the American Hospital Association vehemently opposes including a 36-hour time frame for patient access to information after a hospital discharge in the criteria for "meaningful use" of electronic health records. Am. Hosp. Ass'n, Re: Medicare and Medicaid Programs: Electronic Health Record Incentive Program—Stage 2 Notice of Proposed Rulemaking (CMS-0044-P) 23-24 (April 30, 2012), *available at* http://www.aha.org/advocacy-issues/letter/2012/120430-cl-cms0044p.pdf.

remote communication technologies, patient access can be direct, in real-time, and interactive. Patient interaction with EHRs also presents privacy and confidentiality risks, the subject of this article.

The first section of the article describes several current initiatives to encourage patients' access to their EHRs, especially at the federal level. The second section details some of the most important privacy and confidentiality risks of these patient access initiatives relating to the interactive relationship with the EHR. From the perspective of privacy,[3] patients may be unaware of the extent to which information may be gleaned from them and then be available to others, including their health care providers. From a confidentiality perspective, inadequate identity proofing or authentication procedures may allow unauthorized individuals to access records. Moreover, rules governing records access by authorized personal representatives may reveal more than patients would expect or want. Use by patients of capabilities to download their records may open these records to confidentiality and security protections that are far less stringent than the protections afforded these same records in the possession of health care providers. The third section of the article makes several suggestions for protections that can enable patients to enjoy the great advantages of participative technologies with assurance that privacy

---

These comments have been criticized vigorously by policy advocates from organizations such as the Ctr. for Democracy and Tech., Deven McGraw, *Hospital Association Fights Digital Data Access for Patients* (May 2, 2012), https://www.cdt.org/blog; and the Nat'l P'ship for Women and Families, Christine Bechtel, *Don't Let Them Destroy Patient Protections in Health IT!* (May 2, 2012), http://blog.nationalpartnership.org/index.php/2012/05/patient-protections-hit/.

[3] Although "privacy" and "confidentiality" often appear as twinned, they are in fact distinct concepts. As the terms are used here, "privacy" refers to access to the person, for example use of a blood pressure cuff or a remote monitoring device to take a patient's blood pressure. *See* Leslie P. Francis, *Privacy and Confidentiality: The Importance of Context*, 91 Monist 52, 52 (2008). "Confidentiality" refers to use or disclosure of information once obtained, for example using a physician's records about patients' blood pressures to assess care quality or disclosing a patient's blood pressure in connection with screening for employment. *See id*. "Security" refers to the administrative, technical, and physical safeguards needed to ensure data integrity and limitation to specified uses and disclosures. 45 C.F.R. § 164.304 (2012). The Health Insurance Portability and Accountability Act (HIPAA) "privacy" rule, 45 C.F.R. Part 164 (2012), is thus properly denominated a "confidentiality" rule. *See generally* Francis, at 53; Nicholas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 Ill. L. Rev. 681,701 (2007).

and confidentiality are respected.

1. INTERACTIVE TECHNOLOGY INITIATIVES

Patient-centered technologies initially took the form of personal health record (PHR) systems, apparently first reported in 1978.[4] PHRs are a variety of devices that allow individuals to record and manage their health information.[5] Although PHRs were advocated as a means for patients to take charge of their health and were included as part of many wellness programs,[6] they were criticized as cumbersome, as inappropriately devolving responsibility for record maintenance to patients,[7] and as inadequately protective of confidentiality.[8] In the Health Information Technology for Economic and Clinical Health (HITECH) Act, Congress mandated breach notification requirements for PHR vendors and a study of the need for enhanced protection of PHRs.[9]

Consumer interest in patient-maintained PHRs has continued

4 *See* G. Britain, *Computerisation of Personal Health Records*, 51 Health Visitor 227 (1978).

5 As defined by Congress, a PHR is "an electronic record of PHR identifiable health information … on an individual that can drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." 42 U.S.C. § 1792(11) (2012).

6 For example, WebMD offers a PHR as part of packages marketed to employers to improve employee wellness and thus reduce health care and other employee costs. *Our Company*, WebMD, http://www.wbmd.com/mission.shtml (last visited July 20 2012). For a number of reasons, including concerns about influence from pharmaceutical company advertisers, WebMD revenues have fallen sharply. Susan J. Aluise, *WebMD's Business Model May Require Surgery: Competition from Social Media and Big Pharma's Ad Pullback Have Slammed the Health-Info Site*, InvestorPlace (Jan. 11, 2012), http://www.investorplace.com/2012/01/webmds-business-model-may-need-surgery/. Dossia was originally established by a consortium of several large companies concerned about employees' health and fragmentation of health care; it has recently seen some uptake among Fortune 500 companies. Dossia, *Press Release: Deployment of Dossia Health Management System Leads to Increased Engagement Among User Populations of Fortune 500 Companies*, (Dec. 12, 2011), http://www.bloomberg.com/article/2011-12-12/a__fyeeiQfEI.html.

7 Nicholas Terry, *Personal Health Records: Directing More Costs and Risks to Consumers*? 1 Drexel L. Rev. 216, 219-20, 224-29, 259 (2009).

8 Letter from Nat'l Comm. on Vital & Health Statistics to the Dep't of Health & Human Services 1, 3 (Sep. 28, 2009), available at http://www.ncvhs.hhs.gov/090928lt.pdf; Colin P. McCarthy, *Paging Dr. Google: Personal Health Records and Patient Privacy*, 51 Wm. & Mary L. Rev. 2243, 2245, 2259-61, 2266, 2268 (2010).

9 42 U.S.C.A. §§ 17937, 17953(b)(1) (2012).

lackluster at best. Several highly-publicized PHRs recently have taken new forms or been moth-balled.[10] Physicians too have expressed skepticism about the reliability of patient-maintained PHRs.[11] Instead of PHRs maintained by patients, the movement to consumer involvement in their health care has more recently emphasized technologies that allow patients to access their providers' record systems, communicate interactively with providers, or upload information directly into their providers' records.[12] Initiatives of particular relevance to this article are portals for patients to access their providers' EHRs and communicate electronically with their providers, remote sensing devices for patient data to be entered directly into EHRs, and EHR capabilities that allow patients to download electronic copies of information in their EHRs.

Patient portals. Portals allow patients to log into and view online their records maintained by their providers. These vehicles feature a variety of functions. Some portals will allow access to only a limited set of materials, for example recent test results. Other portals will allow patients to access the entire medical record. Some portals permit email communication between providers and patients. Some allow patients to schedule appointments or refill prescriptions. Some allow patients to enter information or to download copies of information, capabilities discussed further below. Some provide functions for tracking chronic conditions or preventive care recommendations.[13] As their name suggests, "portals" provide patients with a way into their physicians' EHRs; the medical information thus viewed remains part of the medical record and any

---

10 For example, Google Health has been discontinued and will close completely and delete all data as of January 1, 2013. *Google Health Has Been Discontinued*, Google, https://accounts.google.com/ServiceLogin?service=health&nui=1&continue=https://health.google.com/health/p/&followup=https://health.google.com/health/p/&rm=hide (last visited June 23, 2012).

11 Matthew K. Wynia, et al., *Many Physicians Are Willing To Use Patients' Electronic Personal Health Records, But Doctors Differ By Location, Gender, and Practice*, 30 Health Affairs 266, 268-271 (2011).

12 *See e.g.*, John D. Halamka, et al., *Early Experiences with Personal Health Records*, 15 J. Am. Med. Informatics Ass'n 1, 1-7 (2008).

13 For a description of some of the functions incorporated in patient portals, *see* Zsolt Nagykaldi, et al., *Impact of a Wellness Portal on the Delivery of Patient-Centered Preventive Care*, 25 J. Am. Bd. of Family Med. 158, 158-167 (Apr. 2012).

information entered through the portal also becomes part of the record.

Portals have for quite some time played a role in health management for health care organizations such as Kaiser Permanente or Geisinger Health System, each of which launched their portals in 2002.[14] The Veterans Health Administration developed My Health*e*Vet as a means for veterans to view some portions of their VA health records, obtain prescription refills, schedule appointments, and exchange messages with their providers.[15] Portals are convenient for patients and are regarded as having significant advantages for streamlining care, particularly with functions such as appointment scheduling or prescription refills that reduce the volume of calls to providers. Early research suggested that portals were more likely to be used by patients who were more affluent, better educated, younger, and healthier. More recently, efforts have been made to expand the use of portals to safety net populations[16] or patients with chronic illnesses such as diabetes[17] or hypertension.[18] Incentives to improve the coordination of patient care through methods such as Accountable Care Organizations[19] or patient-

14 For a discussion of the development and benefit of patient portals, *see* Seth Emont, Measuring the Impact of Patient Portals: What the Literature Tells Us, California Healthcare Foundation (May 2011), *available at* http://www.chcf.org/~/media/MEDIA%20LIBRARY%20Files/PDF/M/PDF%20MeasuringImpactPatientPortals.pdf

15 My Health*e*Vet, https://www.myhealth.va.gov/index.html,(last visited April 9, 2012).

16 *E.g.*, J.F. Hilton et al., *A Cross-Sectional Study* of *Barriers to Personal Health Record Use by Patients Attending* a *Safety Net Clinic*, 7 P LoS One 2 (2012), http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0031888; J.S. Kahn, *Personal Health Records* in a *Public Hospital: Experience at the HIV/AIDS Clinic at San Francisco General Hospital*, J. Am. Med. Informatics Ass'n 224, 224-228 (2010).

17 P.Y. Benhamou, *Improving Diabetes Management* with *Electronic Health Records* and *Patients' Health Records*, 37 Diabetes & Metabolism S53 (2011).

18 *E.g.*, Peggy J. Wagner et al., *Personal Health Records and Hypertension Control: A Randomized Trial*, J. Med. Informatics Ass'n, (2012); R.W. Grant, *Design and Implementation of a Web-based Patient Portal Linked* to an *Ambulatory Electronic Health Record: Patient Gateway for Diabetes Collaborative Care*, 8 Diabetes Tech. & Therapeutics 576 (2006).

19 An "Accountable Care Organization" is a clinically integrated provider organization that meets Medicare standards for participation in a program to share savings through meeting quality goals; this program was required by section 3022 of the Affordable Care Act. Final regulations for ACOs are at 42 C.F.R. Part 425, 76 Fed. Reg. 67802, 67803 (Nov. 2, 2011).

centered medical homes[20] are thought likely to increase use of patient portals.[21] Portal design is evolving rapidly with particular interest in portals for mobile devices such as smartphones.[22]

Incentives to encourage patient portals play a core role in health reform efforts at the federal level. The HITECH Act established a program of funding incentives for Medicare and Medicaid providers becoming "meaningful" users of EHRs.[23] The program is being implemented in stages.[24] "Stage 1" meaningful use for eligible providers listed providing patients with an electronic copy of their EHR on request as a required core element.[25] Stage 1 also listed providing patients with access to health information (including lab test results, problem list, medication list, and allergies, within 4 business days of the availability of the information to the provider) as one of the optional menu items to qualify as a meaningful user.[26] To receive Stage 1 incentive payments, providers were required to attest to their compliance by February 29, 2012;[27] Stage 2 proposed rules were issued February 23, 2012 and will require compliance by 2014 unless they are delayed.[28] Stage 2 proposes to replace the Stage 1 access requirements with more robust "view, download, and

20 Pioneered by family practice physicians and pediatricians, a "patient-centered medical home" is an effort to provide comprehensive and coordinated primary care. *See Joint Principles of the Patient-Centered Medical Home*, Patient-Centered Primary Care Collaborative (Feb. 2007), http://www.pcpcc.net/content/joint-principles-patient-centered_medical_home.

21 Emont, *supra* note 14, at 3.

22 Nicole Lewis, *GE Rolls Out Upgraded Online Patient Portal*, Info. Week (Feb. 15, 2012), http://www.informationweek.com/news/healthcare/patient/232600945. The GE Centricity portal now allows patients to audit access to their information as well as to grant or remove proxy access online, capabilities that are important to confidentiality and that will be discussed infra at 106-07.

23 Emont, *supra* note 14, at 4.

24 *CMS EHR Meaningful Use Overview*, Ctrs. For Medicare & Medicaid Servs., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Meaningful_Use.html (last visited Mar. 22, 2012).

25 42 C.F.R. § 495.6(d)(12)(i) (2012).

26 42 C.F.R. § 495.6(e)(5)(i) (2012).

27 *CMS Medicare and Medicaid HER Incentive Programs Milestone Timeline*, Ctrs. For Medicare & Medicaid Servs., https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/EHRIncentProgtimeline508V1.pdf.

28 Medicare and Medicaid Programs; Electronic Health Record Incentive Program—Stage 2, 77 Fed. Reg. 13, 701 (Mar. 7 2012) (to be codified as 42 C.F.R. pts. 412, 413, 495).

transmit" objectives for patients with respect to their EHRs.[29]

The design of many patient portals provides patients with the ability to view only portions of their EHR, such as problem lists or lab test results. Physicians have expressed concerns that access to the full medical record, including physician progress notes, may increase patient anxiety and decrease the utility of the information entered into records. More self-serving concerns have included increased time spent in answering questions from patients and increased susceptibility to malpractice claims. MyChart, one of the first and most widely used vehicles for patients to access their providers' EHRs, was designed with many functions but excludes progress notes.[30] The OpenNotes project has been designed to assess the impact of full patient-eye views into EHRs on both providers and patients.[31] Initial findings from the study include increased perception of the benefits of open notes on the part of physicians and much greater support for such transparency on the part of the vast majority of patients.[32]

Portals provide patients with doors into their providers' records. With portals, the record remains in the custody of the provider—it is the provider's EHR—and continues to enjoy all legal protections that apply to provider health records. The security and confidentiality rules of the Health Insurance Portability and Accountability Act (HIPAA) apply to information accessed via a patient portal.[33] HIPAA does not mean complete confidentiality of any information in the EHR, however. For example, HIPAA permits certain legally-required disclosures of protected health information for public health

---

29 *Supra* note 12, at 704. See *infra* for a discussion of the significance of download capabilities.

30 Halamka et al., *supra* note 12, at 1.

31 *About the OpenNotes Project*, OpenNotes, http://www.myopennotes.org/about.shtml, (last visited May 31, 2012); *see also* Tom Delbanco et al., *Open Notes: Patients Signing On*, 153 Annals of Internal Med. 121 (2010).

32 J. Walker et al., *Inviting Patient to Read Their Doctors' Notes: Patients and Doctors Look Ahead*, 153 Annals of Internal Med. 2, 121-25 (2011).

33 45 C.F.R. §16 0.103 (2012). HIPAA applies to "protected health information": health information that is individually identifiable and that is maintained by a covered entity such as a health care provider, insurer, or clearinghouse that maintains information in electronic form.

purposes[34] or for law enforcement[35] without patient authorization. This would apply to any information in the EHR, whether first entered by the provider or by the patient through a portal.

Download capability. Because patients may want or need to have access to their medical information when they do not have immediate internet access, capabilities for patients to download information from provider EHRs have also been an important aspect of the development of technology connecting patients to their health records. The HITECH Act gives patients the right, on request, to receive copies of their health information in electronic form.[36]

Federal agencies such as the Veterans Health Administration and the Centers for Medicare and Medicaid Services (CMS) have been promoting a "Blue Button" initiative for their beneficiaries to be able to download health information with ease.[37] Medicare makes claims and other information available as a downloadable Excel file that can be imported into other tools such as a PHR.[38]

When health information is downloaded from providers' EHRs into vehicles maintained by consumers separately from the EHR, it no longer has HIPAA protection. Recognizing that this raises issues with data privacy, confidentiality, and security, a group led by the Markle Foundation proposed an initial privacy and security framework for patients exercising the download capability.[39] A

---

34 45 C.F.R. § 164.512(b) (2012).

35 45 C.F.R. § 164.512(f) (2012).

36 HITECH Act, 42 U.S.C. § 17935(e)(1) (2009). This provision applies to providers maintaining EHRs. The requirement to transfer information applies to what is termed the "designated record set" under HIPAA, including records used to make treatment decisions and billing records, and does not include psychotherapy notes or information compiled in anticipation of litigation. 45 C.F.R. §164.524(a)(1) (2012).

37 Dep't of Veterans Affairs, *How Do I Get My HealtheVet Data As A Download?*, https://www.myhealth.va.gov/mhv-portal-web/resources/jsp/help.jsp?helpForPortalPage=downloadData (last visited Sept. 13, 2012).

38 Download My Data/Blue Button, http://www.medicare.gov/navigation/manage-your-health/personal-health-records/blue-button-download.aspx (last visited Apr. 9, 2012).

39 Markle Found., Markle Connecting for Health Common Framework for Networked Personal Health Information, Policies in Practice: The Download Capability (August 31, 2010), *available at* http://www.markle.org/health/publications-briefs-health/1198-policies-practice-download-capability. Recommendations of this framework are discussed *infra* at 111-12.

roundtable sponsored by HHS and the Federal Trade Commission (FTC) on December 3, 2010 surveyed the extensive data protection issues raised by PHRs, health-related social networking, and other vehicles containing health information about individuals that are outside the scope of HIPAA.[40] In February 2012, the White House released a "Consumer Privacy Bill of Rights" that called for the development of industry-sector specific codes of conduct implementing privacy protections and enforced by the FTC.[41] Such codes of conduct might be developed for vehicles containing consumer health information.

Remote Sensing Capabilities. The ability to glean accurate health information remotely from patients has enormous advantages for patient care. Patients in need of real-time monitoring can have information obtained for use in their care without the inconvenience, discomfort, or risks of being physically present in a health care facility. For fragile patients such as those with heart failure, remote monitoring can enable significant changes in conditions to be identified at an early stage and can avoid hospitalizations or even be life-saving.[42]

Technologies for assessing patients when they are outside of care settings are developing rapidly. These capabilities include patient-entered information, such as mood or activity level. They also include biosensors for measuring weight, blood glucose, blood pressure, and cardiac activity, among others. They also include functions for integrating and analyzing patient health information in the context of other important types of data, such as air pollution or

---

40 Office of the Nat'l Coordinator for Health Info. Tech., U.S. Dep't. of Health & Human Servs., Information Technology, *Roundtable: Personal Health records Understanding the Evolving Landscape*, http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&objID =3169 (last updated on Mar. 28, 2011).

41 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The FTC has legal authority to regulate unfair or deceptive trade practices. *Id.* at 7. It is an unfair trade practice to subject consumers to a substantial risk of harm that they would not reasonably expect, and it is a deceptive trade practice to give consumers misleading information about the extent of the confidentiality or security provisions their data will be given.

42 *See* A.L. Bui & G.C. Fonarow, *Home Monitoring for Heart Failure Management*, 59 J. Am. Coll. Cardiology 97, 100, 103-104 (2012).

pollen levels for asthmatics.[43] Apps may also include functions for connecting patients to social networks for support, competition, or sharing information.

The Robert Wood Johnson Foundation's Project HealthDesign has been a leader in stimulating innovative interactive technologies. Project HealthDesign sponsors selected design proposals for patient engagement, emphasizing underserved populations and populations with chronic illness. Current Project HealthDesign projects include a mobile smartphone app for asthma patients to report observations such as use of medications or symptom levels; clinicians can access a web-based dashboard to view patients' data, evaluate status, and recommend treatment changes.[44] Another current project monitors the routines of elders thought to be at risk for cognitive loss through the use of in-home sensors; the goal of this project is to allow identification and prevention of unsafe living situations and the potential need for long term care.[45] As another illustration of the types of information involved in Project HealthDesign innovations, iN Touch allows low-income teenagers and young adults to monitor information relevant to obesity and share it with health coaches and clinicians.[46]

For the past three years, HHS has sponsored "datapalooza" events designed to display novel ways of analyzing and deploying data.[47] These events have featured competitions and prizes for

---

43 *See e.g.*, Ben Rooney, *Asthma App Helps Suffers [sic] Manage Condition*, Wall St. J.: Tech Europe (Jan. 10, 2012, 7:29 AM), http://blogs.wsj.com/tech-europe/2012/01/10/asthma-app-helps-suffers-manage-condition; Eileen Zimmerman, *Vital Signs by Phone, Then, With a Click, a Doctor's Appointment*, The New York Times (April 11, 2012), http://www.nytimes.com/2012/04/12/business/smallbusiness/start-ups-use-technology-in-patient-doctor-interaction.html.).

44 Project HealthDesign, *BreathEasy*, http://www.projecthealthdesign.org/projects/current_projects/breatheasy, (last visited Apr. 9, 2012).

45 Project HealthDesign, *dwellSense* (formerly Embedded Assessment), 2012.http://www.projecthealthdesign.org/projects/current_projects/dwellsense (last visited Apr. 9, 2012).

46 Project HealthDesign, *iN Touch*, http://www.projecthealthdesign.org/projects/current_projects/intouch, (last visited Apr. 9, 2012). Manatt, Phelps & Phillips, LLP provided the iN Touch design team at San Francisco State University with an analysis of federal and state privacy and security laws applicable to their project.

47 Health Data Initiative Forum III, The *Health Datapalooza,* http://www.hdiforum.org (last

innovative, interactive technologies for use of health information. Todd Park, the instigator of the datapaloozas, was appointed White House Chief Technology Officer in March 2012.[48] The 2010 event announced an app competition[49]; these competitions are now widespread and have become a featured part of the datapaloozas, Health 2.0 conferences, and other events. Many of the winning apps utilize publicly available data ranging from GIS data to health indicators in ways that are easily visualized by individuals and communities.[50] Other winning apps have the capability to measure and upload biometric data directly from patients such as blood pressure readings.[51] Insurers such as Humana or United Health have developed online games that can be played in teams or as individuals to encourage people to meet exercise or diet goals.[52] At present, these devices do not include downloads from EHRs or PHRs, according to their published descriptions, but they certainly could be so designed—for example, as a way to verify that participants have actually met their stated targets. If so, any records downloaded into vehicles that are not covered under HIPAA would lack HIPAA protections. What must be emphasized from this brief summary is that interactive capabilities are evolving rapidly and employing an unprecedented variety of data sources.

---

visited June 23, 2012) (the third "datapalooza was" June 5-6, 2012).

48 John P. Holdren, *Todd Park Named New White House Chief Technology Officer,* White House Blog (March 9, 2012, 1:11 PM), http://www.whitehouse.gov/blog/2012/03/09/todd-park-named-new-us-chief-technology-officer.

49 Inst. of Med. of the Nat'l Academies, *The Community Health Data Forum: Harnessing the Power of Information to Improve Health,* http://www.iom.edu/Activities/PublicHealth/HealthData/2010-JUN-02.aspx (last updated June 25, 2012).

50 *See, e.g.*, Community Commons, http://www.health2con.com/devchallenge/files/hhs_app_challenge__community_commons1.pdf?cda6cl (last visited Sept. 17, 2012) (winner of the Healthy People 2020 Leading Health Indicators App Challenge).

51 *See e.g.,* Sensei, *Novartis CardioEngagement Challenge,* (Nov. 2011), http://www.health2con.com/devchallenge/files/sensei_novartis_cardiochallenge.pdf (discussing the Sensei app for smartphones, winner of the Novartis CardioEngagement Challenge).

52 Anna Wilde Mathews, *Playing for Wellness*, Wall St. J. Family Finances, http://online.wsj.com/article/SB10001424052702303816504577322240000793770.html, 2012 (last visited Apr. 7, 2012, 9:07 PM).

2. CONFIDENTIALITY AND PARTICIPATORY HEALTH TECHNOLOGIES: UNDERSTANDING ACCESS TO INFORMATION ENTERED THROUGH PATIENT PORTALS

Protecting health information viewed, transferred, or communicated through patient interaction with provider EHRs raises a host of issues of data privacy, confidentiality and security. Many of these issues have generated significant study and proposed solutions. This section and subsequent sections take up three less well attended and related confidentiality problems concerning the interactive relationship between patients and the information in their EHRs. The first is helping patients to understand that information entered into a patient portal, either by the patient or through a remote sensing device, may become part of the patient's medical record and may be used or disclosed by providers in the same way as information entered into the EHR by providers. The second is determining that the person actually interacting with the EHR is the patient him or herself, or someone granted access authority by the patient. The third is making sure that an authorized person is accessing only those portions of the record that the patient wants to have accessed by that person. The need for differentiated interaction with the EHR poses particular difficulties for adolescent patients, the case used in the discussion.

When patients contact their providers directly as through email, it is reasonable to assume that they would like their providers to be aware of the information transferred; that is, after all, the purpose of the transmission. Indeed, studies have concluded that patients are more likely to want to use portals if they believe they are having difficulty communicating with their providers.[53]

Less clear is whether patients presume that communications through patient portals, including email, become part of the medical record. One study suggested that patients seem unaware that communications through portals actually may have greater privacy

---

[53] Kuang-Yi Wen, et al., *Consumers' Perceptions about and Use of the Internet for Personal Health Records and Health Information Exchange: Analysis of the 2007 Health Information National Trends Survey*, 12 J. of Med. Internet Res. e73 (2010); Susan L. Zickmund, et al., *Interest in the Use of Computerized Patient Portals: Role of the Provider-Patient Relationship*, J. of Gen. Internal Med,. Supp. 1, 20, 30 (2008).

protection than ordinary email, although patients did express confidentiality concerns about direct communication with their providers over email.[54] This finding suggests that patients may not fully understand how portals function and the difference between portals and more informal communications. Given the variety of types of information likely to be entered through portals, such failures of understanding might lead to information access or use that would surprise patients. People may include information—or even language—in emails that they think of as casual and that they would not wish to have retained. Portals may include self-management functions into which patients enter quite sensitive information, such as mood; these may appear to patients as "their own" space, although they are part of the medical record. Biometric measurements may enter the record through portals.[55] All of this information may of course be highly beneficial for patient care; the point here is only that patients may be surprised by its status as part of their ongoing medical record.

The reverse may occur as well, although less so as provider-patient electronic communications take place through sophisticated portal systems. Patients given the possibility for direct email contact with providers may assume that communication has taken place and that information will be available for use in their treatment when in fact is has not. This was a major concern of professional guidelines for managing provider-patient electronic communications.

Guidelines from professional societies such as the American Medical Association (AMA) and the American Health Information

---

54 Jiali Ye, et al, *E-mail in Patient-Provider Communication: A Systematic Review*, 80 Patient Educ. & Counseling 266, 272-273 (2010).

55 GE Healthcare unveiled an "advanced" patient portal in February 2012 which is described as an "incredibly powerful tool" that allows for "flexible integration" of patient information into administrative, financial, and clinical workflows. GE, *Press Release: GE Healthcare Empowers Patients with Advanced Online Patient Portal* (February 2, 2012), https://www.genewscenter.com/Press-Releases/GE-Healthcare-Empowers-Patients-with-Advanced-Online-Patient-Portal-3638.aspx. For other examples of interactive portals, see descriptions at these web sites: Omedix, http://omedix.com/patient-portal/http://omedix.com/patient-portal/ (patients may upload information into "HIPAA compliant" portal); vitalelement, http://www.emedicaldesign.com/medical-patient-forms.htm (upload capability); eClinicalWorks, http://www.eclinicalworks.com/ec7de507-7be5-458e9e31-0a83321de807/news-and-events-press-releases-detail.htm (care coordination with biosensor upload capability).

Management Association (AHIMA) urge providers to clarify with their patients how information in electronic communications will be shared and to seek informed consent before instituting such a system.[56] AHIMA guidelines include both security and privacy recommendations for provider-patient communications such as email and text messaging; the extensive discussion of security includes matters such as the need for encryption.[57] Privacy guidelines caution that patients should be told whether office personnel will screen emails and thus whether communications will be seen and potentially filtered or answered by staff.[58] The AHIMA guidelines also state that all electronic communications with patients—including email and text messaging—should be treated as healthcare organizational business records and given the same treatment as any other medical records; among the advantages noted for this treatment is protection of liability.[59] Finally, AHIMA recommends that providers should have stated policies for communication, including policies "addressing issues that require the e-mail documentation to become **part of the patient record"** and policies for enforced record retention.[60]

The AMA Guideline[61] states that patient portals should establish informed consent concerning use and limits on access to health information in electronic records. Although the guideline seems

---

56 *See* AHIMA, *E-mail as a Provider-Patient Electronic Communication Medium and its Impact on the Electronic Health Record (AHIMA Practice Brief)* (October 2003), http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_021588.hcsp?dDocName=bok1_021588 (emphasis in original); *See also* AMA, *H-315.971: Patient Information in the Electronic Medical Record*, https://ssl3.ama-assn.org/apps/ecomm/PolicyFinderForm.pl?site=www.ama-assn.org&uri=%2fresources%2fdoc%2fPolicyFinder%2fpolicyfiles%2fHnE%2fH-315.971.HTM (last visited June 23, 2012).

57 *See* AHIMA, E-mail as a Provider-Patient Electronic Communication Medium and its Impact on the Electronic Health Record (AHIMA Practice Brief) (2003), http://library-ahima.org/xpedio/groups/public/documents/ahima/bok1_021588.hcsp?dDocName=bok1_021588.

58 *Id*.

59 *Id*.

60 *Id*.

61 AMA, Guideline H-315.971: Patient Information in the Electronic Medical Record, https://ssl3.ama-assn.org/apps/ecomm/PolicyFinderForm.pl?site=www.ama-assn.org&uri=%2fresources%2fdoc%2fPolicyFinder%2fpolicyfiles%2fHnE%2fH-315.971.HTM (last visited June 23, 2012).

written to apply to office staff, it is also clearly aimed at ensuring that patients understand which aspects of the medical record will be visible to them through the portal and which aspects will not: "Prior to granting a patient access to his or her EMR, informed consent should be obtained regarding the appropriate use of and limitations to access of personal health information contained in the EMR. Physicians should develop and adhere to specific guidelines and protocols for online communications and/or patient access to the EMR for all patients, and make these guidelines known to the patient as part of the informed consent process. Such guidelines should specify mechanisms for emergency access to the EMR and protection for and limitation of access to, highly sensitive medical information."[62] The AMA Guideline also indicates that if patients are allowed to enter information into the EHR, sourcing information should be included and a permanent record of any "allowed annotations and communications relevant to the ongoing medical care of the patient" should be maintained as part of the record.[63] The AMA Guideline states that physicians retain the right to determine which information from a PHR is imported into an EHR.[64] Finally, the Guideline provides that patients should not be able to delete any information in the EHR in order to maintain its "forensic nature."[65]

Several limitations with these guidelines are apparent. They date from early days of electronic communication, nearly ten years ago, and do not explicitly address the myriad forms of electronic interaction appearing today. Indeed, some matters treated in these guidelines—such as security matters—are now being addressed under federal Meaningful Use regulations. The guidelines are recommendatory, not obligatory, stating what providers should do rather than what they must do. Yet with impending nearly-mandatory inclusion of at least some interactive functions into many provider-patient relationships—Medicare and Medicaid providers must be "meaningful users" of EHRs by 2015 or face payment adjustments—further attention should be paid to whether aspects of

62 *Id.*

63 *Id.*

64 *Id.*

65 *Id.*

these guidelines such as patient informed consent should be mandatory. Finally, the clear emphasis of the guidelines is placed on protecting physicians from undue workflow burdens and liability risks. These are surely important concerns for providers and may benefit patients as well, if providers are reassured that they will be able to use information in a manner that helps their patients and will not fear interactive mechanisms.[66] Nonetheless, shaping guidelines primarily in terms of protecting physicians may unfortunately obscure the need for patients to understand the status of communications and how they may be used or disclosed.

3. CONFIDENTIALITY AND PARTICIPATORY HEALTH TECHNOLOGIES: WHO IS INTERACTING? IDENTITY, AUTHENTICATION, AND AUTHORIZATION

A second problem with confidentiality and interactive provider-patient technologies is ensuring that the provider is interacting with the person actually empowered to make the communication. Problems may arise at the time portal access is established, if persons other than the patient or the patient's authorized representatives have access to means to establish the portal. Portals, once established, require authentication of any communications, just at an ATM machine requires authentication of the person seeking to use it to access funds in a bank account. The existence of legally authorized patient representatives adds an additional layer of complexity. HIPAA defers to state laws concerning access to medical records such as guardians or holders of special powers of attorney for health care, with the special provisions for unemancipated minors and possible victims of abuse discussed below.[67] In addition, many portals are designed to allow patients to designate others who may have access to their records, a feature that is especially important for

---

66 Matthew K. Wynia, et al., *Many Physicians Are Willing to Use Patients' Electronic Personal Health Records, But Doctors Differ By Location, Gender, And Practice*, 30 Health Affairs 266 (Feb. 2011). For a discussion of liability risks of EHRs and recommendations for federal guidance, see Sharona Hoffman and Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 Berkeley Tech. L.J. 1523 (2009).

67 45 C.F.R. §164.502(g).

patients who may wish for support or consultation in managing their health.

Identity. The initial step in implementing a participatory technology such as a portal is getting it set up. From a privacy and confidentiality perspective, it is important to ascertain that the person setting up the account is as represented: either patients themselves or persons legally authorized to act for them. Given the extent to which personally identifiable information may be known more widely than by individuals themselves—Social Security numbers, for example, may be known by relatives or included in some divorce decrees and thus available to ex-spouses—verifying identity in a manner that preserves confidentiality is a not an easy matter, especially long distance. Internet identities are created for purposes as diverse as health, financial management, social networking, or playing games. Depending on the sensitivity, risks, and power of the information—among relevant factors—different strategies may be appropriate. The overall problem of creating a national strategy for trusted identities in cyberspace is currently being addressed by the National Institute of Standards and Technology (NIST).[68]

Medicare has established account registration and validation procedures for patients setting up a mymedicare.gov portal.[69] The typical Medicare beneficiary is enrolled automatically and is provided with instructions about how to access the account online—as might occur with pin numbers sent separately with a credit card. Any beneficiary seeking to self-enroll must validate their data by providing their Medicare number, last name, date of birth, gender, and zip code. Any authorized user registering the beneficiary must designate their relationship to the beneficiary; the selection menu includes: self, spouse, parent, child, grandparent, hospital/Nursing Home Administrator, social worker, and other. Enrollees must check boxes certifying that information is correct and that they agree to the rules and regulations regarding site use in order to continue the

---

[68] *See generally* NIST, *Recommendations for Establishing an Identity Ecosystem Governance Structure*, *available at* http://www.nist.gov/nstic/2012-nstic-governance-recs.pdf (last visited Sept. 17, 2012).

[69] *MyMedicare.gov Account Registration and Validation Process* (Sept. 30, 2011), on file with the author.

enrollment process. They must then validate their address (which they are provided automatically). To complete registration, they set up a username, secret question and answer, email address and confirmation if they desire, and password and confirmation. Enrollees are cautioned to select usernames and passwords that meet certain security standards, for example not using obvious numbers such as their Social Security number or their Medicare number. A difficulty with username and password selection, of course, is the tradeoff between security standards and ease of remembering for many people.[70] Any enrollee forgetting a username or password must answer the secret question to be allowed to create a new password—and three wrong answers to the question will lock the account and require re-registration.

In comparison, HHS has far more stringent standards for identification of employees and contractors, including those involved in the Medicare program.[71] Individuals must be sponsored by the agency as having a need for the identification. Issuance of identification credentials requires individuals to be physically present with two forms of identification, one of which must be a government-issued photo ID such as a passport or a driver's license.[72]

Requiring persons enrolling in myMedicare.gov to establish their identities by appearing in person with photo identification would impose daunting requirements on beneficiaries. Beneficiaries who are infirm, have time commitments such as work or care-giver responsibilities, live far from Social Security offices, or find transportation difficult, might easily find these requirements preclusive. The benefits of enrolling these beneficiaries in interactive

---

70 National Strategy for Trusted identities in Cyberspace*, Making Online Transactions Safer, Faster, and More Private*, http://www.nist.gov/nstic/ (last visited July 27, 2012) (a contributing factor to identity theft is the number of passwords people must remember for online access).

71 These standards are required by Presidential Directive under the Homeland Security program. *See* U.S. Dep't Homeland Sec., *Homeland Security Presidential Directive (HSPD) 12: Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004), *available at* http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm.

72 This description is contained in the training materials for sponsors, Department of Health and Human Services, *Personal Identity Verification Training*, *available at* http://www.ors.od.nih.gov/ser/dpsac/documents/HHS_PIV_Training_for_Sponsors_2-4-09.pdf (last visited July 27, 2012).

technologies could be substantial—especially as they may be among those who would be most helped by long-distance communicative capabilities.

Nonetheless, the comparison suggests areas of concern about the current identification process. First, there is no effort to obtain a photo ID or even a photograph of the individual establishing the account. With current remote technologies, it is not difficult for individuals to photograph themselves or government documents such as a passport, and transmit these photographs to the entity establishing identity. Second, there are no additional means for checking whether the individual providing the identifying information knows information that might be uniquely known to the person, or perhaps those very close to the person; persons establishing the account set-up their own secret questions and answers. In establishing accounts with credit monitoring agencies, by contrast, individuals are asked to answer questions about themselves drawn from information otherwise available to the entity responsible for the account before an account is created.[73] A similar technique is used by Kaiser for patients setting up myHealthManager. Kaiser originally had a clunky two-step process that mailed an authentication code to the patient's address on record after an attempt to set up an account was made.[74]In 2008, it replaced this method with a "one-step" method that includes questions to verify that the individual is the person claimed.[75] Finally, the current Medicare process is weak concerning the authority of the person establishing the account to act for the patient. Although designation of the relationship to the patient must be specified, the list of menu choices includes relationships such as facility administrator where legal authority to speak for the patient may be absent or even prohibited by state law, and omits relationships such as legal guardian where it may be established.

Authentication. Once set up, an interactive technology will

---

73 *See* Nicole Perlroth, *Utah Breach Shows Vulnerability of Health Records*, The New York Times (Apr. 10, 2012), http://bits.blogs.nytimes.com/2012/04/10/utah-breach-shows-vulnerability-of-health-records/.

74 Kate Christensen & Anna-Lisa Silvestre, Connected for Health: Using Electronic Health Records to Transform Care Delivery 140, 147-48 (Louise L. Liang ed., 2010).

75 *Id.*

require authentication of the user at each new use. Different factors are used for authentication: something possessed (an insurance card, an ATM card), something known (a Medicare number, pin number, password, mother's maiden name), or a feature of the person (a biometric, fingerprint, or voice print).[76] The strength of an authentication method is related to the strength of each factor and to the number of factors used. Mymedicare.gov cautions beneficiaries to select passwords that meet criteria for strength, but uses single-factor authentication—something known, a username and password. Two-factor authentication—as illustrated by an ATM card and a pin number—could be a significant barrier to use of interactive technologies by patients, depending on how it is constructed. On the other hand, single factor authentication may leave patients vulnerable to unauthorized entry by others, particularly if passwords are weak, can be guessed easily, or if beneficiaries are not careful about sharing them with others.

The AMA guidance referred to above recommends that physicians should take "reasonable steps to authenticate the identity of correspondent(s)."[77] The guidance also states that physicians are "encouraged" to have a written authentication protocol for all personnel and to keep a written record of each authentication.[78] A particularly helpful suggestion in the guidance is the need to establish minimum standards for authentication when a patient is new or not well-known, both circumstances in which authentication might be more difficult. Nonetheless, this guidance is quite non-specific and is recommendatory only.

The Office of the National Coordinator for Health Information Technology (ONC) has recently published guidance for certain health

---

76 *See* William E. Burr et al., *Electronic Authentication Guideline,* Nat'l Inst. of Standards & Tech. (2006), *available at* http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.

77 Am. Med. Ass'n, *H-315.971 Patient Information in the Electronic Medical Record*, http://www.ama-assn.org/ (follow "Advocacy" hyperlink; then follow "Policy Finder" hyperlink; then follow "Accept" hyperlink; then follow "Search AMA PolicyFinder Online"; then search "Health and Ethics Policies" for "electronic medical record"; then select "H-315.971").

78 *Id.* Notably, patient requests under HIPAA for an accounting of disclosures of protected health information need not include disclosures to the patient herself—and presumably not to authorized patient representatives—or disclosures for treatment, payment, or health care operations. *See* 45 C.F.R. §164.528(a)(1) (2012).

information exchanges concerning establishing and authenticating identity.[79] With respect to access by individuals to their own information in the exchange, the guidance requires strong identity and authentication policies and recommends policies that reach at least the third level of electronic authentication standards required when business is conducted with federal agencies.[80] Such level 3 authentication establishes "high confidence in the asserted identity's validity" both for initial establishment and for subsequent use of the identity,[81] a level of confidence required where authentication errors would pose even low risks for public safety or moderate risks for release of sensitive information or damage to standing or reputation.[82] Technically, level 3 requires presentation and verification of a government-issued photo ID, together with some other documentation of identity for initial credentialing—that is, for establishing an account initially—with subsequent authentication by a token of sufficient strength to guard against threats such as impersonation.[83] These requirements are stronger than either the identity verification or the authentication requirements for individuals to access myMedicare.gov.

Given the scope of the information and the fact that the guidance is designed to apply to all users, including both providers and patients accessing their own records, this difference is arguably appropriate. Nonetheless it is cause for reflection whether more than single factor authentication requirements ought to apply when

---

79 Office of the Nat'l Coordinator for Health Info. Tech., Dep't of Health & Human Servs., Pub. No. ONC-HIE-PIN-003, *Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program 1* (Mar. 22, 2012), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf.

80 *Id.* at 9. The reference in the guidance is to NIST 800-63 which is a technical elaboration of the Office of Management and Budget's E-Authentication Guidance for Federal Agencies. *See* Burr, *supra* note 76, at vi; *see also* Letter from Joshua B. Bolton to The Heads of All Departments and Agencies (Dec. 16, 2003), *available at* http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf.

81 Bolton, *supra* note 80, app. a § 2.1.

82 *Id.* app. a § 2.2.

83 Burr, *supra* note 76, at vii, 22-23.

patients interact through portals. Two-factor authentication applies to the use of ATM machines, for example: a card and a password. Online access to banking accounts for functions such as billpay also requires a type of two-factor authentication that would not be cumbersome for use in patient access to portals. When an individual establishes an internet banking account, a soft encryption key is planted in the computer originating the account. This is a second factor—something the individual "has"—which combined with username and password (something the individual knows) creates two factor authentication. Kaiser reports using the financial services industry model for establishing identity with widespread success.[84] If individuals later seek to access the account from an unfamiliar computer, they will be asked security questions which must be answered correctly before they are able to proceed. Other forms of two-factor authentication—such as a card reader device for individual computers, or a single use password—are more cumbersome and could likely raise barriers to portal use, however.[85]

Including Others in Participatory Technologies. Establishing authority to act on the patient's behalf through interactive technologies is a further, very complex problem beyond establishing and authenticating identity for participants. I have written elsewhere on the general issue of access to interoperable medical records by personal representatives.[86] Here, I take up two specific instances of this problem: the interactive technology function that enables patients to give others permission to participate interactively with their providers, and the problem of establishing interactive functions for adolescents.

A major selling point of many interactive technologies is the ability they give patients to bring others into their care.[87] The

---

84 Christensen, *supra* note 74.This report refers to establishing identity and does not state whether authentication methods also follow those in use in financial services.

85 I owe these points to John Houston.

86 Leslie P. Francis, *Skeletons in the Family Medical Closet: Access by Personal Representatives to Interoperable Medical Records*, 4 St. Louis U.J. Health L. & Poly 371 (2010).

87 For example, TelCare, a remote glucose monitoring device, allows both providers and family members (anyone with the patient's permission) to see real time glucose readings and trend data. *See* Telecare, *A relative of someone with diabetes*, http://telcare.com/get-involved/a-relative-of-someone-with-diabetes/(last visited July 27, 2012) For a portal

ubiquitous variety of portals—from Florida to New York, and Texas to South Dakota to Nevada and California—offer remarkably different approaches to portals. Some portals provide online forms for family members to request access.[88] Others invite patients to provide names online of the family members who are to have access.[89] Some invite patients and family members to stop by the clinic to each receive a separate username and password.[90] Some remind family members that if they are accessing on behalf of someone else, they should be sure to use that person's log in information so that the access goes to the correct chart.[91] Other patient portals, however, do not allow family members access to portals out of confidentiality concerns[92] but contemplate adding this feature in the future.[93]

The convenience and supportiveness of these vehicles is readily

---

example, *see* South Dakota Regional Health, *Patient Portal*, http://www.regionalhealth.com/Our-Locations/Clinics/Regional-Medical-Clinic/Patient-Portal.aspx (last visited July 27, 2012).

88 E.g., Personal Physician Care, P.A, *Personal Physician Care, Patient and Legal Guardian/Family Member Access Request to Online Patient Portal*, *available at* http://www.ppcare.net/forms/patient_and_legal_guardian_pp_access.pdf (last visited July 27, 2012). This form requires requesters in Delray Beach, Florida to self-certify that they are the patient's personal representative, or that they have been given express authorization by the patient. Apparently no further verification is needed.

89 *See e.g.*, Silver Sage Center for Family Medicine, *Patient Portal Policies and Procedures*, https://silversagecenter.com/silver-sage-center-for-family-medicine/new-patients/patient-portal-policy-and-procedures/ (Last visited July 27, 2012) (located in Reno, Nevada; uses gotomyclinic portal).

90 *See e.g,* Columbia Gorge Family Medicine, *Patient Portal Login*, http://www.columbiagorgefamilymedicine.com/#/patient-portal/4552698758 (last visited July 27, 2012) (located in Hood River, Oregon).

91 *See e.g.*, Stone Creek Family Medicine, *Patient Portal*, http://stonecreekfamilymedicine.com/?page_id=20 last visited July 27, 2012) (located in Montgomery, Texas).

92 *See e.g.*, Urban Family Practice, *Welcome to Urban Family Practice: What is Medent Patient Portal?*, http://www.urbanfamilypractice.com/portal.html (last visited July 27, 2012) (for patients in Buffalo, NY).

93 *Id. See also* Addabbo Family Health Center, *Frequently Asked Questions*, https://69.193.183.14:8080/FAQ.aspx (last visited July 27, 2012) (for patients in Queens, N.Y.; non-profit federally funded community health center). The illustrations given here are not a scientifically obtained sample; they were among the top 10 hits in a Google search conducted in July 2012 for "patient portal" and "family member." They are presented here as illustrations of the variety of portals available today—at least as they are publicly described.

apparent, but caution is in order. Most importantly, it seems from published descriptions that some of these portals do not require direct contact with the patient or some other means to establish the legal authority of the individual in question to access the record. Kaiser, for example, requires competent adult patients to establish access for another from within their secure accounts—and to renew this access every two years.[94] Other means to confirm the patient's wishes with respect to access by others to portals are readily available as well. Many of the examples in the preceding paragraph are aimed at established patients in family practices. Discussion of how the portal functions and the patient's wishes with respect to its use could be part of a patient visit—analogous to the recommendations to include discussion of advance care planning as a routine matter in primary care.[95] Surely, if the encouragement of patient engagement continues, the use of interactive technologies will be as important an aspect of care for many patients as end of life decision-making—with concomitant need for knowing the patient's preferences. If portal access is established online, providers' offices could make follow up telephone calls to the patient's address or email the patient to confirm that the access reflects the patient's wishes. The point here is not that shared portal access is a bad thing; it will increasingly play a role in interactive, patient-centered health care. The point instead is that as portal functions become more and more robust, it will be important to insure that their uses reflect the wishes of patients or their authorized representatives, just as other important decisions about health care are expected to do.

Minors. Adolescents present a particularly complex set of problems for interactive technologies. One study describes adolescent portals as an "opportunity" to "negotiate issues of confidentiality" and finds that although both teenagers and their parents welcome enhanced communication possibilities, teenagers are concerned to protect their confidentiality and parents are concerned that teenagers will be able to access medical care without

---

94 Connected for Health: Transforming Care Delivery at Kaiser Permanente 152 (Louise L. Liang ed., 2010).

95 American Medical Association, Report of the Council on Ethical and Judicial Affairs 4-I-10, Advance Care Planning, *available at* http://www.ama-assn.org/resources/doc/code-medical-ethics/2191a.pdf (last visited Sept. 17, 2012).

their knowledge.[96]

Under state laws, adolescents and their parents may have differing rights of access to records, depending on whether the minor had the legal power to consent to the care, whether the care fell within certain categories of sensitivity, the type of setting in which the care was provided, or whether the minor authorized the parent to view the record.[97] In New York, for example, providers may inform minors over the age of 12 of a request to view their records, and may refuse to release the records if the minor objects.[98] Types of care to which minors may be given the power to consent include reproductive care (sometimes but not always including abortion),[99] diagnosis and treatment for sexually transmitted diseases,[100] mental health treatment,[101] or substance abuse treatment.[102] Some states provide that only the minor may access records when he or she has the power to consent to the care in question.[103] Some states allow minors to consent to one or more of these forms of care but permit

---

96 David A. Bergman, et al., *Teen Use of a Patient Portal: A Qualitative Study of Parent and Teen Attitudes*, 5 Perspectives Health Info. Mgmt. 13 (2008).

97 *See generally* Caitlin M. Cullitan, *Please Don't Tell My Mom! A Minor's Right to Informational Privacy*, 40 J Law Educ. 417, 417-457 (2011); National Center for Youth Law, California Confidentiality Law: When Parents May Access Adolescent Records (2006), *available at* http://www.teenhealthlaw.org/fileadmin/teenhealth/teenhealthrights/ca/Ca-ParentAccessRules.pdf.

98 NY Pub. Health Law Ann. § 18(3)(c) (West 2012).

99 *E.g.*, N.C. Gen. Stat. Ann. § 90-21.5(a) (West 2012) (pregnancy care not including abortion, sexually transmitted disease care, emotional disturbance);Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797, 800 (Cal. 1997) (striking down a state statute requiring minor to obtain consent or judicial authorization prior to an abortion).

100 *E.g.*, Cal. Fam. Code Ann. § 6926(a), (b) (West 2012); Kan. Stat. Ann. § 65-2892 (West 2012); Mont. Code Ann. § 50-16-521(1) (West 2011); Wash. Rev. Code Ann. § 70.24.110 (West 2012).

101 Ky. Rev. Stat. Ann. § 214.185(1) (West 2012) (includes outpatient mental health treatment, substance abuse treatment, sexually transmitted disease treatment, and contraceptive and reproductive care excluding abortions); Tex. Fam. Code § 32.004(a)(1)-(3) (West 2012) (includes suicide prevention; chemical addition or dependency; and sexual, physical, or emotional abuse); Wash. Rev. Code Ann. § 71.34.530 (West 2012) (consent by minors 13 and older to outpatient care).

102 E.g., Conn. Gen. Stat. Ann. § 17a-688(d) (West 2012); Iowa Code Ann. § 125.33 (West 2012); La. Rev. Stat. Ann. § 40:1098.3 (West 2012); N.J. Stat. Ann. § 9:17A-4 (West 2012).

103 *E.g.*, Wash. Rev. Code Ann. § 70.02.130(a) (West 2012).

providers to decide whether or not to inform parents.[104] Maryland joins widespread consent powers for minors with the provider's discretion to inform parents of the treatment over the minor's objection—except in the case of abortion, when the record must remain confidential.[105] Oregon allows minors 14 years or older to consent to outpatient mental health or substance abuse treatment without parental consent but requires parents to be involved before the end of the treatment unless there are clear clinical indications to the contrary or the parents refuse.[106] Provisions for access by minors also may be linked with the related provisions that the minor may not access records concerning care to which s/he did not have the power to consent[107] or that the parent may not access records to which the minor had the power to consent without authorization.[108] In addition, federal law provides that information concerning certain substance abuse treatment may not be provided to a minor's parents without the minor's consent if the minor had the power to consent to the treatment under state law.[109]

Complying with these remarkably varied state law requirements is challenging for interactive technologies, to say the least. Challenges are multiplied when the provider serves patients in multiple jurisdictions, as do large provider systems such as Kaiser and even small practices located in towns near borders between states. Kaiser writes:

"The kp.org website seeks to provide online health record access to all Kaiser Permanente members who want it. We are much of the way there, providing access to all capable adults, to incapacitated adults via an approved proxy, and to children under twelve or thirteen (the age varies by state) via their parents or other care givers.

---

104 E.g., Ala. Code § 22-11A-19 (2012) (sexually transmitted disease treatment).

105 Md. Code Ann. § 20-102(c), (f) (West 2012).

106 Or. Rev. Stat. Ann. § 109.675(2) (West 2010).

107 *E.g.*, Cal. Health & Safety Code Ann. §123110(a) (West 2012).

108 *E.g.*, Cal. Health & Safety Code Ann. § 123115(a)(1) (West 2012).

109 42 C.F.R. § 2.14(b) (2012). *See also* Rebecca Gudeman, *Federal Privacy Protection for Substance Abuse Treatment Records: Protecting Adolescents*, Youth Law News 2 (July-September 2003), *available at* http://www.teenhealthlaw.org/fileadmin/teenhealth/teenhealthrights/yln/03_yln_3_gudeman_substance.pdf.

Teens are a difficult group to deal with because of the complex and inconsistent privacy laws that vary by age, condition, treatment, and state. We are continuing to explore ways to create meaningful and useful access for teens and, when appropriate, their parents."[110]

Adjusting interactive records so that adolescents may view portions that are open to them and parents may view portions that are open to them would require portals to set up structures for separate management functions of these different types of records. Developing these management capabilities has been recommended by both NCVHS and ONC,[111] although these tasks remain largely unaddressed.

Because of these management challenges, some portals simply do not provide access when a patient is between the ages of 13 and 18.[112] The resulting loss of potentially important interactions for minors and their providers—or their parents and their providers, or minors and their parents—are significant.

4. CONFIDENTIALITY AND PARTICIPATORY TECHNOLOGIES: DOWNLOADING RECORDS

Additional challenges to confidentiality are posed when patients download medical information. As described above, patients are being encouraged to download their information so that it will be readily available to them and so that it can be used with other tools such as mobile apps. As also described above, statutory protections may change when information is transmitted from one venue—the provider's EHR—to another venue that is not covered by HIPAA.

---

110 Kate Christensen and Anna-Lisa Silvestre, *Making Health Personal*, *in* Connected for Health: Transforming Care Delivery at Kaiser Permanente 139, 143 (Louise L. Liang ed., 2010).

111 Letter from Justine M. Carr, M.D., Chairperson, Nat'l Comm. On Vital & Health Statistics, to Kathleen Sebelius, Sec'y, Dep't of Health & Human Servs. (Nov. 10, 2010), *available at* http://www.ncvhs.hhs.gov/101110lt.pdf (last visited Sept. 17, 2012); *see also* Office of the Nat'l Coordinator, ONC-HIE-PIN-003, Privacy and Security Framework Requirements and Guidance for the State Health Information Exchange Cooperative Agreement Program (Mar. 22, 2012), *available at* http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_5545_1488_17157_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/onc_hie_pin_003_final.pdf (recommending more granular choice).

112 Bergman, s*upra* note 96, at 15 (citing the Palo Alto Medical Foundation as an example).

Indeed, many tools for individuals' management of their health information are not HIPAA-covered[113] but instead are covered by the Federal Trade Commission Act's prohibition on unfair and deceptive trade practices.[114]

The "Consumer Privacy Bill of Rights," proposed by the White House in February,[115] may help if it is implemented. Nonetheless, it remains sectoral by design: that is, it encourages different sectors of industry to create codes of conduct for protecting confidentiality that will then be enforced by the FTC.[116] A primary goal of this design structure is to allow for innovation that fits with industry needs.[117] A potential flaw of this design, however, is that the result may be divergent codes of conduct for different sectors of industry possessing individuals' health information.

To take just one example, interactive technologies for self-management by diabetic patients are developing so rapidly that their use is attracting review articles. One such review notes that the number of iTunes apps for these patients grew from 60 in 2009 to over 250 in February 2011.[118] This review compares available apps to guidelines for clinical management and concludes that the guidelines are only partially met. Another group of researchers describe the many questions of safety and efficacy raised by patient self-monitoring of blood glucose through smart apps.[119]

Neither review mentions the presence of differing confidentiality

---

113 U.S. Dep't Health Human Servs., Personal Heath Records and the HIPAA Privacy Rule 3, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

114 U.S. Dep't Health Human Servs., Health Information Privacy, Other Security Rule Notices and Materials. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/ (last visited July 5, 2012).

115 Exec Office of the President, *supra* note 39, at 6.

116 *Id*.

117 *Id*.

118 Taridzo Chomutare et al., *Features of Mobile Diabetes Applications: Review of the Literature and Analysis of Current Applications Compared Against Evidence-Based Guidelines*, 13 J. Med. Internet Res. 3 (July – Sept. 2011), *available at* http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3222161/?report=printable.pdf.

119 S.K. Garg and I.B. Hirsh, *Self-Monitoring of Blood Glucose*, 65 Int'l J. Clinical Prac. (Supp. 170) 1-9 (Feb. 2011).

protections from those promised in the app's privacy policy to those provided by HIPAA to information entered into the patient's EHR. Diabetes is just one condition among many for which interactive technologies are being developed, albeit a condition that is of particular contemporary concern.

5. CONCLUSION

The interactive technologies described in this article are exciting developments in health care. They have the potential to engage patients and those on whom they rely far more actively in the enterprise of maintaining health and managing disease. In short, they are a key aspect of the movement towards patient-centered care.

At the same time, these interactive technologies present new confidentiality challenges. Paper records in providers' offices stayed in those offices until they were physically moved elsewhere or destroyed. The entry of copy and fax machines was but a harbinger of what was to come and what may come in the near future. Medical information today is visible, downloadable, replicable, transferrable, and analyzable perhaps even with just a few clicks of computer keys. If patients are legitimately concerned that their information may find its way where they do not want it to go, they may be reluctant to enter fully into the enormous potential these interactive technologies offer for their health care.