KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

Building a Strong Privacy and Security Policy Framework for Personal Health Records·

The Center for Democracy & Technology

July 21, 2010

A growing number of individuals use electronic personal health records (PHRs) to manage personal health information and connect to health-related services. Early evidence suggests that PHRs have strong potential to help people become more engaged in the management of their own health care. But the success of PHRs depends on whether consumers trust that their information will be safeguarded. To protect consumers and foster innovation in this evolving field, CDT recommends that the government set baseline legal requirements for PHRs and related applications, and also establish incentives to encourage companies to voluntarily adopt more comprehensive policies that mirror the Markle Common Framework for Networked Personal Health Information.

Introduction

At its core, a personal health record (PHR) is an electronic tool that is intended to allow consumers to store, manage, use, and share their personal health information. Various PHR products allow individuals to connect to health-related services, such as pharmacies and health care providers. A large survey released in April 2010 by the California Health Care Foundation found that 1 in 14 Americans have an electronic PHR.[1] Numerous factors have likely limited the growth of PHRs, including consumer privacy concerns and the challenge for PHR vendors in settling on a sustainable business model.[2] Consistent, comprehensive privacy and security safeguards for PHRs can address both problems by providing greater consumer protection and clarity for the marketplace on the bounds of appropriate business practice.

· CDT thanks Lygeia Ricciardi, Ed.M., Principal, and Jason Rothstein, Clear Voice Consulting, LLC, and Alan Rubel, M.A., J.D., Ph.D., Greenwall Fellow in Bioethics, Health Law and Policy, for their significant contributions to this paper. We also thank Josh Lemieux of the Markle Foundation.

[1] Consumers and Health Information Technology: A National Survey, California Health Care Foundation, pg. 5, Apr. 2010 (hereinafter CHCF Survey), http://www.chcf.org/~/media/Files/PDF/C/ConsumersHealthInfoTechnologyNationalSurvey.pdf.

[2] Id., pg. 19.

In this paper, the Center for Democracy & Technology (CDT) recommends a policy framework comprised of a mix of regulatory requirements and voluntary best practices. This paper proposes baseline rules that the government should establish through legislation or agency rulemaking. To encourage industry best practices, the regulations should include a safe harbor with requirements that mirror the Markle Common Framework for Networked Personal Health Information (the Markle Common Framework). The Markle Common Framework sets comprehensive policy and technical expectation for PHRs, which CDT considers to be best practices for PHRs and related applications.[3]

Implementation of the American Recovery and Reinvestment Act[4] (ARRA) and health reform legislation (the Patient Protection and Affordable Care Act[5]) provide increased business incentives for the PHR industry. Although the bulk of the incentive funds under ARRA are directed toward the adoption by health care providers of electronic health records (EHRs), the criteria for accessing this funding includes electronically sharing data with patients, which could pave the way for an expansion in PHR use. Implementation of health reform could also lead to an increased focus on "engaged consumers" who have tools at their disposal to monitor and manage chronic conditions, understand treatment choices, access personalized health advice, support lifestyle changes, evaluate insurance options, share data with other parties to gain insight and expertise, and hold the health care system to a higher standard of accountability. Effective PHRs can support all of these consumer behaviors.

Yet consumers and industry alike face another important challenge: many PHRs are not covered by several of the existing health information privacy oversight and regulatory mechanisms. For consumers, this means fewer assurances about how their information will be handled or how policies will be enforced. For industry, patchwork or ambiguity in regulations can chill investment and innovation.

Now is the time for stakeholders to implement a clear and robust privacy and security framework for all PHRs that combines baseline rules and voluntary best practices. This paper focuses largely on the content of those baseline rules. The baseline regulations can be implemented through legislation, or, more likely, Congress can delegate rulemaking authority to one or more of the relevant federal agencies: the Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services (HHS). ARRA directed HHS, in consultation with the FTC, to produce a report by February 18, 2010, concerning privacy and security protections for PHRs not covered by the Health Insurance Portability and Accountability Act (HIPAA).[6] CDT will submit this paper to both agencies to help inform that report.

---

[3] Markle Connecting for Health Common Framework for Networked Personal Health Information, Markle Foundation, Jun. 2008, http://www.connectingforhealth.org/phti/.
[4] Pub. L. No. 111-5 (Feb. 17, 2009) (hereinafter ARRA).
[5] Pub. L. No. 111-148 (Mar. 23, 2010).
[6] ARRA section 13424(b).

This paper draws from a workshop on PHRs that CDT hosted in May 2009[7] and specifically adapts the Markle Common Framework, This paper also builds on recent recommendations on PHRs from the National Committee on Vital and Health Statistics (NCVHS),[8] and reflects recent recommendations on protecting consumer privacy online that CDT submitted to the Federal Trade Commission (FTC).[9]

At a high level, our privacy and security regulatory recommendations for PHRs are as follows:

- Require consumer consent to collect, use, disclose, and maintain data *in* a PHR.
- Establish a safe harbor to encourage best practices
- Require PHR providers to provide opportunities for consumers to amend, correct or annotate information in a PHR.
- Prohibit compelled use of a PHR.
- Require PHR providers to have data retention policies.
- Require PHR providers to adopt reasonable security protections, including strong authentication policies.
- Require PHR providers to use immutable audit trails.
- Prohibit the unauthorized re-identification of aggregate/de-identified data from a PHR.
- Require that data in a PHR be portable, human-readable and divisible by the individual.
- With respect to personal data collected about PHR account holders, require that PHR providers implement robust fair information practices, including collecting and using only the minimum amount of information necessary to accomplish a given purpose; giving account holders notice and some control over data collection, providing full transparency about the scope of data collection, and allowing consumers to view and correct such data.
- Make all PHRs subject to consistent federal rules.
- Extend federal policies beyond PHR vendors to others with significant access to PHR information (for example, third-party applications and websites).
- Require PHR providers to clarify to consumers their relationships with third-party applications and websites.
- Require strong and consistent enforcement of rules.
- Preserve privilege of data in PHRs

Defining PHRs

[7] See Appendix A for a list of PHR workshop attendees.
[8] National Center for Vital and Health Statistics, Letter to HHS Secretary Sebelius, Sep. 28, 2009, http://www.ncvhs.hhs.gov/090928lt.pdf.
[9] See Refocusing the FTC's Role in Privacy Protection, Center for Democracy & Technology remarks for the FTC Consumer Privacy Roundtable, Nov. 6, 2009, http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf. ("CDT Comments to the FTC, Nov. 6, 2009").

In one form or another, consumers or patients have long kept personal health records: copies of diagnoses, lists of medications, health diaries, and so forth. What is new and merits special attention is the commercial development of the electronic, longitudinal, interactive and sharable personal health record.

To date, the only PHR definition appearing in federal law is in ARRA, which states that a PHR is "an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."[10]

Although the ARRA definition is a good starting point, additional clarity about what is considered a PHR would aid policy development. A PHR is not necessarily a single entity, but rather a suite of tools that can enable certain activities, such as tethered portals that function as a window into portions of a health care provider's electronic clinical record or insurance claims records, or other platforms and services that can be accessed and populated by any number of applications. A comprehensive definition of PHRs should incorporate the following concepts:

- The PHR is primarily focused on information related to health.
- The consumer consents to the creation of the PHR and is the primary user of information contained in it.
- The consumer may add a variety of types of information to the PHR, whether generated by providers, the consumer, devices, or by other parties.
- The consumer controls access to the information in the PHR, deciding whether and what to share, with whom, and for what purposes.
- The PHR is distinct from the records maintained by health care providers, although it may incorporate copies of such records.
- The PHR may be longitudinal, enabling the consumer to see changes over time related both to clinical and non-clinical factors and events.
- The PHR should be a tool for action, not just a repository of information. Its ultimate aim should be to enable consumers to use information to better manage and enhance their own health (and/or the health of their family members).

Benefits of PHRs

Actual PHR users report a number of positive effects directly related to PHR use, including:

- Feeling more knowledgeable about their health.
- Feeling more knowledgeable about the care provided by their doctors.

[10] ARRA section 13400. "PHR identifiable health information" includes individually identifiable health information, as defined in HIPAA (which includes personal health information provided by a covered entity), as well as information provided by or on behalf of individuals and that identifies such individuals (or with respect to which there is a reasonable basis to believe the information can be used to identify them). See ARRA section 13407.

- Asking new questions of their doctors.
- Feeling more connected to their doctors.
- Taking steps to improve their health.
- Feeling more at ease talking to family members about health issues.[11]

PHR users also report that PHRs are useful for:

- Making sure their health information is correct.
- Looking at test results.
- Renewing prescriptions on-line.
- Emailing providers.
- Scheduling doctor visits.
- Managing family health information (including keeping track of children's records).
- Getting reminders for tests.
- Seeing doctor's instructions.[12]

Veterans using the My Health*e*Vet PHR express high levels of satisfaction (8.3/10.0). My Health*e*Vet users are highly likely to return to the site (8.6/10.0) and recommend the site to other veterans (9.1/10.0).[13]

PHR Usage Levels and Future Trends

Depending on how PHRs are defined, analysts estimate that there are roughly 200 PHR products on the marketplace, of which about 50 have a significant level of usage.[14] Roughly half of U.S. adults express some interest in using a PHR.[15] However, actual consumer adoption of PHRs today is less than 10 percent. This likely is due to a combination of factors, including lack of convenience, the newness and still evolving nature of the service,[16] as well as concerns about privacy.[17] However, within certain subpopulations, PHR adoption rates are much

---

[11] CHCF Survey, pg. 9.
[12] CHCF Survey, pg. 8.
[13] Kim Nazi, "Veterans' voices: use of the American Customer Satisfaction Index (ACSI) Survey to identify My Health*e*Vet personal health record users' characteristics, needs and preferences," *J. of the Am. Med. Informatics Ass'n* 2010; 17: 203-211.
[14] Based on estimates from the Markle Foundation and Chilmark Research. For details, see Chilmark's iPHR 2008 Market Report: Executive Summary, Analysis & Trends of Internet-based Personal Health Records' Market, http://chilmarkresearchstore.com/iphr2008execsummary.html.
[15] CHCF Survey, pgs. 15-16.
[16] Chilmark Research and Deloitte estimate PHR use at 3.5% and 9% respectively. The Chilmark report is available at http://chilmarkresearchstore.com/iphr2008execsummary.html. See also Deloitte's 2009 Survey of Health Care Consumers: Key Findings, Strategic Implications, pg. 7, http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/us_chs_2009SurveyHealthConsumers_March2009.pdf.
[17] See, e.g., the 2008 survey by Knowledge Networks and the Markle Foundation, showing that more than half of respondents who say they are not interested in having a PHR cite privacy concerns as a reason for not wanting one. Findings are available at

higher. For example, more than one-third of Kaiser Permanente patients use the HMO-provided PHR platform.[18]

One thing is clear: health is a very popular topic on the Internet. Consumer use of electronic health information services, including websites, information generated by other consumers (e.g., blogs, newsgroups, ranking sites),[19] and smart phone applications,[20] is high and/or trending upward, as is the extent to which consumers indicate an interest in using PHR-type services.[21] Several other trends suggest a significant opportunity for personal health records to meet patient needs in the future. For example:

- *Changing population patterns:* As baby boomers transition into later life and require increased medical care, PHRs can help to address the demands this demographic places upon the health care system. Meanwhile, digitally savvy younger generations will expect greater access to and control over their health information. These trends will converge, as younger users become caretakers for their aging parents and grandparents and look to PHRs to help them better perform that role.

- *The rise of social networking.* The flair of social networks for sharing information dovetails with the benefit of using PHRs to share health data with other parties to gain insight and support. As online social networking sites have blossomed, they have increasingly become forums for the active sharing of health information, including both

---

http://www.connectingforhealth.org/news/pressrelease_062508.html. This bolsters the findings of numerous previous surveys, for example, one by Lake Research and American Viewpoint for the Markle Foundation in Nov., 2006, which concluded that, with regard to electronic personal health information, "identity theft and privacy risks are still top concerns for the public." For more information, see http://www.markle.org/downloadable_assets/research_doc_120706.pdf. The most recent PHR survey from California Healthcare Foundation found that concern about privacy was a top barrier to using a PHR. CHCF Survey, p.19.

[18] Chris Rauber, "Kaiser Says 3M Enrollees Track Health Online," San Francisco Business Times, Apr. 22, 2009, http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2009/04/20/daily41.html.

[19] According to the Pew Internet and American Life Project, 61% of American adults look online for health information in 2009 (up from 25% in 2000). In addition, a majority of people who look for health information online use "user-generated" health information. See "The Social Life of Health Information," http://www.pewinternet.org/Reports/2009/8-The-Social-Life-of-Health-Information.aspx?r=1. In its 2010 survey, the California Healthcare Foundation found that 67% of respondents had searched online for information about a disease or medical problem. CHCF Survey, p.4.

[20] For a description of the growing field of smartphone health apps, see Jason Rothstein and Lygeia Ricciardi's post on the Project HealthDesign blog, "A Pocket Full of ODLs," (Jul. 27, 2009) http://projecthealthdesign.typepad.com/project_health_design/2009/07/a-pocket-full-of-odls.html.

[21] See the Markle Foundation's Survey, "Americans Overwhelmingly Believe electronic Personal Health Records Could Improve Their Health," (Jun. 2008) http://www.connectingforhealth.org/resources/ResearchBrief-200806.pdf, CHCF Survey pgs. 15-17.

traditional and non-traditional health indicators. This trend has implications both for PHRs themselves, which may increasingly incorporate social networking components, as well as for other social networking platforms that may support the creation of PHRs.

- *Cloud computing.* With the emergence of cloud computing as a major technological trend, PHRs may evolve from stand-alone files or single-access point websites to data hubs or platforms that pull and push information through multiple access points, including telephones, mobile computing devices, smart medical devices, related information services (e.g. health savings account access points), and other methods not yet foreseen.

Despite the potential need for these tools, a critical factor in their adoption and use will be trust. Surveys have identified privacy concerns as the primary reason why individuals choose not to adopt PHRs.[22] Consistent regulations and privacy protections for PHRs can accelerate adoption and innovation by preserving consumer trust, as well as providing the PHR marketplace with greater certainty than the current legal structure.

PHRs and Current Law – Why Not Just Extend HIPAA?

Understanding PHR privacy protections from a legal perspective is not straightforward. In part because they are relatively new, no single federal statute clearly or adequately applies to all forms of PHRs. The Health Insurance Portability and Accountability Act (HIPAA) and the HIPAA Privacy and Security Rules have the clearest and broadest applicability to PHRs, but only when those PHRs are offered by HIPAA-covered entities (such as health systems or payers) or their business associates.[23]

In recent years, however, numerous PHR-related platforms and services have been offered by entities that fall outside the bounds of the traditional health system and thus outside the coverage of HIPAA, including software manufacturers, search engines, online health sites, and financial institutions. To complicate matters further, because many HIPAA-covered entities partner with non-covered entities to provide PHR services, the HIPAA Privacy and Security Rules may cover a particular PHR product or service in some circumstances but not others, depending on the details of particular business arrangements.

Though some have suggested that HIPAA should be extended to all PHRs, regardless of who offers them, the need for consistent policies would not be met

[22] See footnote 17.

[23] As discussed in more detail later in this paper, we do not believe that the HIPAA Privacy Rule, as currently structured, provides appropriate protections for consumers using PHRs. Thus we have urged HHS to narrowly construe the provision in ARRA requiring PHR vendors to be business associates in certain circumstances. For more details, please see http://e-caremanagement.com/privacy-law-showdown-legal-and-policy-analysis.

by extending HIPAA coverage in its current form to all PHRs.[24] The HIPAA Privacy Rule does not translate well for regulating a tool designed primarily for consumer use (the HIPAA Security Rule, however, may be an appropriate fit). HIPAA was specifically designed to regulate only the sharing of information among traditional health care system entities. As a result:

- HIPAA permits personal health information to flow without consumer or patient authorization for treatment, payment, and health care operations.
- HIPAA permits other uses without consent (e.g., disclosure to researchers, law enforcement).
- Although HIPAA requires express patient authorization in a number of situations--including the use of health information for marketing and use of health information for any purpose by employers--these requirements (especially the ones concerning marketing) have historically provided weak privacy protections.

HIPAA's approach of permitting broad categories of data to flow without consumer consent is entirely inconsistent with the concept of PHRs as tools operated at the consumer's discretion. Instead, we believe that a better approach would be to apply a comprehensive framework designed specifically for PHRs that draws from HIPAA and other sources. [25]

Several other federal laws and related regulations, including the Electronic Communications Privacy Act, the Federal Trade Commission Act, and the Gramm-Leach-Bliley Act, as well as state laws such as California's Confidentiality of Medical Information Act, may also apply or be relevant in crafting PHR policies. For a more thorough overview of the current legal environment as it may apply to PHRs, see Appendix B.

An analysis of the current legal landscape reveals an incomplete patchwork that does not fully or consistently protect PHR data. Yet a strong baseline of rules for PHRs is important to maintain consumer trust and sustain industry investment. CDT has set forth recommendations in this paper to address this need.

The Role of Certification in Enforcing Privacy Protections for PHRs

Certification is a process whereby an entity establishes standards for a type of product or service and confers certified status to those that comport with the standards.

Historically, the government-recognized Certification Commission for Health Information Technology (CCHIT) has been the certification body for the broader

[24] See the Statement of Deven McGraw, Director of CDT's Health Privacy Project, at the Hearing on Personal Health Records before the National Committee on Vital and Health Statistics Subcommittee on Privacy, Confidentiality & Security on Jun. 9, 2009, http://www.ncvhs.hhs.gov/090609p6.pdf.

[25] See also the CDT memo, "Why the HIPAA Privacy Rules Would Not Adequately Protect Personal Health Records," (Sep. 2008), http://www.cdt.org/files/pdfs/HIPAA-PHRs_0.pdf.

health IT industry. CCHIT began work in 2008 to develop a certification program for PHRs, focusing its efforts primarily on privacy and security. For example, draft PHR certification criteria include provisions regarding consent, access control, record amendment, and account termination.

ARRA established that providers and hospitals must meaningfully use "certified" electronic health records (EHRs) to qualify to receive federal stimulus dollars.[26] To implement this provision of ARRA, the Office of the National Coordinator for Health IT (ONC) recently released federal regulations on a permanent certification program for health information technology (HIT).[27] ONC also has left open the possibility that its certification and testing program may one day include PHRs.

Although the CCHIT and ONC certification criteria include some of the general protections recommended in this paper, certification criteria cannot substitute for the needed policies, practices and enforcement mechanisms yet to be established in law or regulation.[28]

Certification is particularly useful for promoting interoperability, functionality, and usability. It can also help advance data protection by encouraging the adoption of innovative technologies that bolster privacy and security policy. While certification cannot guarantee compliance, the role of certification in health IT is to ensure that EHR and PHR products possess the ability to comply with laws and policies. Certification criteria should also allow enough flexibility for health care providers to go beyond policy requirements to, for example, offer patients greater privacy protection than that required under the law.

However, certification must not become a proxy for the policies and practices needed to protect the privacy of information of both EHRs and PHRs. The threat of losing certification status is unreliable as a major mechanism of enforcement in the absence of a policy framework.[29] The mere presence of privacy and security capabilities in PHR technology does not mean that protections will be correctly implemented, or that the PHR vendors' actual policies and practices will further support these capabilities. Instead, the law must set baseline privacy and security requirements, including formal enforcement mechanisms, which certifying entities should then use as a basis for certification criteria narrowly focused on ensuring the capability for compliance.

---

[26] ARRA Sections 4101-4104.

[27] The text of the Certification NPRM is available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=1745&parentname=CommunityPage&parentid=1&mode=2&in_hi_userid=10741&cached=true. ONC has issued a final rule for a temporary certification program for EHRs, available at http://healthit.hhs.gov/portal/server.pt?open=512&objID=2885&parentname=CommunityPage&parentid=72&mode=2&in_hi_userid=12059&cached=true.

[28] CCHIT PHR Certification Criteria (Draft), Sep. 29, 2008, http://www.cchit.org/files/comment/09/01/CCHITCriteriaPHR09Draft01.pdf. PHRs

[29] See comments submitted on ONC's proposed certification rule by the Markle Foundation and endorsed by CDT at http://www.markle.org/downloadable_assets/20100510_collabcmts.pdf.

Voluntary certification may have a part in supporting or promoting privacy and security of PHRs, but this issue should be revisited once appropriate federal privacy and security policies are in place. CDT sees no current policy reason for requiring mandatory certification of PHRs through regulation. CDT views PHR certification as a possible role for the HIT industry to fill, as opposed to certification by government bodies. Either way, an effective certification process should include independent audit and oversight to monitor compliance with certification criteria over time.

Recommended Protections for PHRs

As CDT has noted on many occasions, building trust in health IT – including the use of PHRs – requires a comprehensive privacy and security technology and policy framework. Congress and regulatory agencies must establish baseline protections in legislation and regulation upon which industry best practices may build. Both regulation and industry best practices play critical roles in implementation. CDT's recommendations below are primarily directed at Congress and federal regulatory agencies seeking to initiate protections for consumers using PHRs.

CDT supports a PHR regulatory framework that preempts state laws if, similar to HIPAA, the regulations are established as a floor of protections upon which states may build more protective laws.[30] A possible alternative is a single federal standard that includes strong protections for consumers.

As stated previously, CDT drew heavily on Markle Common Framework in shaping these recommendations. The Markle Common Framework was developed and supported by a diverse group of 56 stakeholder organizations, including leading privacy advocates, technology companies, consumer organizations, and representatives of HIPAA-covered entities.[31] The Markle Common Framework is based on internationally accepted fair information practices (FIPs) and articulates in detail the 14 policy and technology practices which PHR providers must fulfill to fully implement the FIPs.

CDT strongly believes that the FIPs have remained relevant for the digital age despite the dramatic advancements in information technology that have occurred since these principles were initially developed. However, most privacy schemes to date have focused largely on a subset of the FIPs: notice and consent. Relying exclusively on notice-and-consent compliance regimes places the onus for privacy on the consumer to navigate an increasingly complex data environment. Unfortunately, little actual privacy is achieved when protections rely solely on notice and consent.

---

[30] Preemption would likely require Congressional action, either enacting the rules as formal legislation or authorizing an agency rulemaking to preempt contradictory state laws.

[31] For a list of endorsers of the Markle Common Framework for Networked Personal Health Information, see http://www.connectingforhealth.org/resources/CCEndorser.pdf.

Although insufficient on their own, notice and consent are crucial components of privacy protections. This is particularly true with respect to the data in a consumer's PHR, which, as discussed in more detail below, should be subject to a high level of consumer control over access, use and disclosure in order for consumers to use PHRs as active tools for health self-management. To avoid some of the pitfalls that may arise from heavy reliance on consent, it is critical for policymakers to monitor the scope of activities in this space and act promptly against those who would take unfair advantage of consumers.[32]

1. Require consumer consent to collect, use, disclose, and maintain data in a PHR

a. A two-tiered protocol: general and specific consent

If we expect consumers to actively use PHRs to manage their health or the health of their family members, the rules for use must support a high degree of consumer discretion. Consequently, PHR providers should be required to give consumers broad control over how information in the PHR is collected, used, disclosed, and maintained.[33]

The baseline standard for access to data in the PHR should be a clear opt-in consent that is not conditioned on the use of the service. In implementing such consent, CDT urges policymakers to adopt the approach to consent described in the Markle Common Framework and agreed to by a wide array of PHR providers.[34] This approach establishes two tiers of consent—an initial, general consent provided as part of the process by which the consumer consents to initiate a PHR account, covering the basic collection, use, and disclosure of personal health information in the PHR (including a description of the reasons for such uses and disclosures), and a more specific additional or "independent" consent for any data collections, uses, or disclosures of personal information that would be unexpected or considered sensitive by a reasonable consumer.[35] This independent consent must be obtained from consumers in advance of said information use or disclosure.[36]

Broadly speaking, general consent is sufficient for routine access to data in the PHR by the PHR vendor in order to effectively maintain the account if the vendor makes explicit in product descriptions and privacy notices the terms of the

---

[32] See CDT Comments to the FTC, Nov. 6, 2009, where we urge FTC to more actively use its unfair trade practices jurisdiction to crack down on activities that violate consumer privacy.

[33] Markle Common Framework CP3. Consumer Consent to Collections, Uses, and Disclosures of Information, http://www.connectingforhealth.org/phti/docs/CP3.pdf

[34] Id.

[35] Id.

[36] Such independent consent should be based on – but need not necessarily be as detailed as—HIPAA authorization requirements, which include a description of the information to be used or disclosed, the person authorized to make the use or disclosure, the person to whom the use or disclosure may be made, an expiration date, and, in some cases, the purpose for which the information may be used or disclosed. http://www.hhs.gov/ocr/privacy/hipaa/faq/use/264.html.

offering and does so in keeping with the Markle Common Framework.[37] Independent, specific consent should be sought for any activity that the consumer would not reasonably expect or fully understand, or has the potential for abuse or misuse of consumer data, including marketing uses and research activities. This two-tiered approach offers flexibility in determining which situations merit general vs. specific consents. For example, in the case of consent for access by or disclosure to a health care professional or health plan, it may be appropriate for consumers to give consent for certain users to access particular kinds of records at any time, without requiring specific consent for each instance of access. At a minimum, consent with respect to how information *in* a PHR is accessed, used and disclosed should be distinct from any consents obtained with respect to data collection about consumers' use of the account or their online behavior.

A general opt-in consent also may be appropriate in instances in which data in the PHR is accessed, used or disclosed in aggregate or de-identified form. For example, advertising, research or public health uses of aggregate or de-identified data may be permitted with a general consent, as long as the uses are disclosed in a clear and effective way, as discussed in more detail below. It is critical that PHR vendors be required to use statistically sound methodologies for aggregating or de-identifying data and be held accountable if they or their business partners re-identify this data. We note that some PHR vendors have a "break the glass" policy that allows them to access data in consumers' PHRs without authorization in the event of a medical emergency.[38] A general consent would be appropriate for such a policy.

PHR users should be able to voluntarily participate in public health research and surveillance with their PHR information after granting specific, independent consent to the PHR service provider. Otherwise, public health uses of identifiable data in a PHR should be permitted only when authorized by law and ideally only when the information cannot be accessed effectively through provider and plan records. Compulsory government access to personally identifiable information in the PHR (whether for public health, law enforcement, or other reasons) should require a warrant plus notice to the consumer.

Consumer consent is a critical safeguard for PHRs, but we recognize that relying too heavily on notice and consent regimes often shifts the onus of privacy protection on consumers and places the bulk of the bargaining power with service providers.[39] This problem is exacerbated by the fact that many (though not all) independent PHR vendors depend on business models that anticipate revenue from advertising and partnerships with third-party suppliers of health-related products and services. These vendors are likely to market to their users on the basis of health information within the users' PHRs. Given the limits of

---

[37] Markle Common Framework CP2, Policy Notice to Consumers, http://www.connectingforhealth.org/phti/docs/CP2.pdf.

[38] See for example Dossia Privacy Statement on Personally-Controlled Health Records, at http://www.dossia.org/for-individuals/privacy-statement.

[39] For additional details on CDT's view of the role of individual consent in protecting health information, see http://www.cdt.org/healthprivacy/20090126Consent.pdf.

consent, CDT urges regulators to be vigilant of unfair marketing practices in the PHR space.[40]

b. Form of consent

For consumers to provide meaningful consent (general or specific) for the collection, use, disclosure, and maintenance of PHR data, their choices must be presented in an effective and understandable way.[41] For too long, notification of individual rights with respect to data collection and use has been buried in the onerous legalese of privacy policies or terms of service. Research shows that consumers rarely read privacy policies or terms of service. Instead, many Internet users wrongly assume that the words "Privacy Policy" mean that their personal information will not be collected or shared, even when the policy says just the opposite.

Therefore, CDT believes it is time to move beyond equating effective notice and consent with a lengthy privacy policy, whether for PHRs or for any other online services. Instead, PHR providers and related entities should be required to provide concise and effective ways to notify consumers about their rights to consent with respect to personal data in PHRs.[42] The FTC has already put a stake in the ground on this issue through its recent Final Rule on breach notification.[43] Here, the FTC included a provision stating that companies' disclosures regarding how consumers' information is used must give consumers meaningful choices and should not be buried in lengthy privacy notices.[44] Agencies and industry groups should consider developing standardized notices based on consumer testing.

One way to begin effectively informing consumers about data collection and use is to use more accurate language on the website, such as "Data Collection Practices" rather than "Privacy Policy."[45] This phrase could serve as a link on a

---

[40] See CDT Comments to the FTC, Nov. 6, 2009.

[41] Markle Common Framework CP2, Policy Notice to Consumers, http://www.connectingforhealth.org/phti/docs/CP2.pdf.

[42] Id.

[43] Federal Register Vol. 74, No.163, Federal Trade Commission Health Breach Notification Final Rule (Aug. 25, 2009), http://edocket.access.gpo.gov/2009/pdf/E9-20142.pdf.

[44] Id. Also, in Jun. 2008, HHS launched a three-phase project to develop a model privacy notice and facts-at-a-glance for PHRs that would help consumers understand and compare privacy policies across PHRs. We applaud HHS' efforts, especially the systematic way in which the information is organized, but the latest version is still too long to be of much value to consumers (for example, information about how data in a PHR is used does not appear until page six of the 12-page document). See http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848091_0_0_18/PHR_NoticeBlankTemplate.pdf.

[45] This is a practice CDT recommends for all Web sites. See CDT's paper on Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient On Its Own To Protect Consumers (Dec. 2009), http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.

PHR provider's website to more detailed information about consumers' ability to control how health data can be transferred to their PHR, and how data in the PHR can be accessed, used or disclosed.

Another way to acquire more meaningful consume consent to uses and disclosures of data in the PHR is to employ an "unavoidable notice" in the form of a window that pops up on the PHR provider's website and provides consumers with information about, and obtains their consent to, collection and uses of their data. A consumer's successful interaction with this window could also serve as a condition for opening the PHR account in the first place.

With respect to the access, use and disclosure of data in the PHR, default settings should be avoided to maximize consumer choice. However, if default settings are used, PHR providers should be required to utilize the most privacy-protective default settings. Consumers cannot truly opt-in if the less privacy-protective defaults are preselected for them. These default settings should be clearly disclosed and defined for users at the outset.

Third party applications attached to the PHR may have different collection and use policies than the PHR platform. There is a risk that consumers will not distinguish between the privacy practices of applications and those of the PHR platform. PHR users should be clearly notified of any changes or implications to their privacy choices that may come with the use of an application and be afforded the opportunity to exercise specific consent regarding the purposes to which the application puts their data.

In addition, if PHR providers make material changes to the policies that govern consent to how data in a PHR can be collected, used, disclosed, and maintained, then the consumers' consent to the previous policies may not appropriately be implied. To resolve this issue, PHR providers should notify users of the proposed changes and be required to do so in a clear, prominent, and meaningful way.[46] Only upon receiving opt-in consent from consumers should PHR providers collect, use, disclose, and maintain data in a PHR under the new policies. However, for a system like this to function, the scope of what is considered a "material change" needs to be clear. A standard for material change is needed, and it must be properly enforced.

2. Establish a safe harbor to encourage best practices

A well-designed safe harbor regime would enhance the protections offered by baseline PHR privacy and security rules. A voluntary safe harbor can encourage industry best practices, create certainty for companies (because following approved practices would be deemed compliance with the rules), and promote innovation in privacy protection as PHR providers develop privacy solutions to meet safe harbor requirements.

[46] Markle Common Framework CP2, Policy Notice to Consumers, http://www.connectingforhealth.org/phti/docs/CP2.pdf.

A safe harbor strategy recognizes differences in performance by treating actors who qualify for safe harbor more favorably than those who do not.[47] The favorable treatment could include a variety of "carrots and sticks", such as exemption from certain liabilities, penalties or requirements for companies meeting safe harbor requirements.[48] The purpose of the safe harbor is not to encourage mere compliance with legal requirements, nor is it a pathway for entities to self-regulate based on weak standards. Rather, entities seeking to qualify for safe harbor would have to demonstrate that their privacy practices are more protective than that which the law requires.[49]

CDT suggests that the safe harbor requirements for PHRs should mirror the Markle Common Framework, filling any gaps between the Common Framework and what PHR federal rules ultimately require of PHR providers. As the product of collaboration between industry players, privacy experts and consumer groups, the Common Framework is an ideal resource for developing safe harbor requirements.[50]

To be effective, the safe harbor regime must have independent approval and oversight components to ensure companies applying for safe harbor actually meet the standards and maintain compliance over time. No PHR vendor or related entity should be deemed to qualify for safe harbor without a first undergoing a comprehensive audit to ensure compliance with the requirements. Once an entity qualifies for safe harbor, an icon or seal might be useful to notify consumers of the entity's safe harbor status. For the icon concept to work, the symbol should be tested with real consumers to ensure they understand its significance.

3. Require PHR providers to have policies for handling disputes concerning information in the PHR

PHRs may afford new opportunities for consumers to identify possible errors or omissions in their health data, including that which originates from provider records.[51] To enable these activities, PHR providers should be required to

---

[47] There is recent precedent for safe harbors in the health IT privacy and security arena. HHS established a safe harbor in its interim final rule on breach notification for health information. See U.S. Dept. of Health and Human Services, Interim Final Rule on Breach Notification for Unsecured Protected Health Information, 45 CFR 164.402 (2010).

[48] Letter to Chairman Rick Boucher from Professor Ira Rubenstein, Jun. 1, 2010.

[49] Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, Public Law & Legal Theory Research Paper Series, Working Paper No. 10-16, New York University School of Law (Mar. 2010), http://ssrn.com/abstract=1510275. Note: Professor Rubinstein serves on the CDT Board of Directors.

[50] Id., pgs. 29-35.

[51] For an example of a case in which an individual identified errors in his PHR, see "Electronic Health Records Raise Doubt" in the *Boston Globe*, Apr. 13, 2009. http://www.boston.com/news/nation/washington/articles/2009/04/13/electronic_health_records_raise_doubt.

establish, and clearly convey to their users, policies for handling disputes concerning the content of the PHR.[52]

Many PHRs contain data from two categories of sources: copies of information obtained from members of the traditional health system (including health care providers, insurers, etc.) and data generated or acquired by consumers themselves, whether directly entered by them, or fed into the PHR by devices or other sources that are not part of the traditional health care system (including data from a monitoring device that the consumer operates, from a commercial Web site, or from a consumer's own health-related observations).

Policies governing disputes about the validity of data should draw a distinction between these different categories of data. With respect to copies of data that users might not be permitted to change directly (including but not limited to data that originates with members of the traditional health system), users should be given a way to attach notes or complaints to the PHR disputing the validity of the data – and the note should remain appended to the data any time it is disclosed from the PHR. (This is similar to how the HIPAA Privacy Rule treats patient amendment of data in covered entity records.) PHR vendors also should consider mechanisms for communicating patient disputes about data back to the original source for consideration.[53]

Users should be free to change data that they input themselves or that comes from other non-traditional health system sources; if this is not the case, that must be made clear to the individual in the privacy policy and a similar pathway for annotating the record must be made available.

4. Prohibit compelled use of a PHR

Despite the many potential benefits associated with PHRs, individuals should be free to choose whether or not to open a PHR account.[54] Employers, health plans, and others should be explicitly prohibited from requiring individuals to open PHR accounts as a condition of employment, membership, or for any other reason.[55] PHR accounts should also not be routinely opened for consumers who do not explicitly activate them, as this can expose personal data to uses not necessarily anticipated by the consumer. Similarly, consumers should not be compelled to disclose the information held within the PHR, or whether they are using a PHR, without due process of law.[56]

---

[52] Markle Common Framework CP6, Dispute Resolution, http://www.connectingforhealth.org/phti/docs/CP6.pdf.

[53] Markle Common Framework CP8, Consumer Obtainment and Control of Information, http://www.connectingforhealth.org/phti/docs/CP8.pdf.

[54] See Robert Gellman, *Personal Health Records: Why Many PHRs Threaten Privacy*, World Privacy Forum, Pg. 5, Feb. 20, 2008, http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

[55] Markle Common Framework CP7, Discrimination and Compelled Disclosures, http://www.connectingforhealth.org/phti/docs/CP7.pdf.

[56] In a related example concerning social network sites (rather than health sites or PHRs specifically), ABC News reported on Jun. 19, 2009 that the City of Montana asked job

5. Require PHR providers to have data retention and account termination policies

Individuals should be able to terminate their PHR accounts and know that their data will be destroyed, including deletion of all backup and other copies, within a reasonable time. PHR providers should be required to disclose in their privacy notices their practices in this area.[57] Data retention policies should include a regular schedule for responding to user requests to terminate their accounts. Such policies should also define what constitutes an "inactive" account, and define how long data will be held after there is no user activity, and the processes that the PHR vendor will use to try to notify the account holder, prior to termination of the account. Vendors must not be permitted to hold data in inactive accounts indefinitely.

The mechanism by which consumers terminate their accounts must be easy to access and clearly described, including details about what will happen and when, how long copies of data may persist, any possibility for reactivation of a closed account, and who may be able to access personal health information before it is fully deleted.[58] Policies should also cover disposition of PHR accounts upon the death of the account holder. Data should not be provided to next of kin unless the account holder has specifically consented to this.

In addition, PHR providers must offer to give consumers electronic copies before an account is closed, or transfer the data to another PHR of the consumer's choice. (See the recommendation on portability, below.) Consumers should be able to direct, within reason, the format in which they receive or transfer this data.

6. Require PHR providers to adopt reasonable security protections, including strong authentication policies

Because of the sensitive nature of health information that may be contained in a PHR, it is essential that PHR providers be required to adopt reasonable security protections, including technical, administrative and physical safeguards.[59] Policymakers should consider whether it is appropriate to impose requirements such as those found in the HIPAA Security Rule, those required by Gramm-Leach-Bliley, or by the FTC pursuant to its FTC Act authority.

---

applicants to disclose not only the fact of their membership in online social networking sites such as Facebook, but also asked them to share their passwords to those sites. http://abcnews.go.com/Technology/JobClub/Story?id=7879939&page=2. As the FTC points out, the fact of having a PHR account may indicate that a consumer has a particular health condition. See Federal Trade Commission, Health Breach Notification Rulemaking, Project No. R911002, pg. 12.

[57] Markle Common Framework CP8, Consumer Obtainment and Control of Information, http://www.connectingforhealth.org/phti/docs/CP8.pdf.

[58] Id.

[59] Markle Common Framework CT6. Security and Systems Requirements, http://www.connectingforhealth.org/phti/docs/CT6.pdf.

In particular, it is important for PHR providers to adopt strong user authentication policies.[60] The Markle Common Framework recommends an authentication framework that should be used to construct requirements for robust authentication policies for PHR providers. The Common Framework authentication approach has four components: identity proofing, use of identifiers or tokens, ongoing monitoring, and ongoing auditing and enforcement:[61]

- Identity proofing – The process by which a person's individual "identity" is verified using outside evidence or credentials. The federal government should leverage the expertise of the National Institute for Standards and Technology (NIST) and other appropriate agencies to recommend a framework for acceptable methods and accuracy thresholds for initial identity proofing and authentication for individual consumers accessing their personal health information online.

- Identifiers or tokens – Once identity proofing is performed, organizations issue or require users to use tokens or identifiers. They may include physical documents (e.g., driver's license) or biological markers (e.g., fingerprints), or they may be based on knowledge (e.g., passwords), or some combination (e.g., token plus PIN).

- Ongoing monitoring – After tokens have been issued or identifiers linked to an identity, systems are put in place to establish behavior patterns of individuals and alert authorized parties if behavior changes suspiciously.

- Ongoing auditing and enforcement – If an organization relies upon third parties for identity proofing or the issuing of identifiers or tokens, it must have mechanisms to audit those third parties and correct any problems.[62]

7. Require PHR providers to use immutable audit trails

Immutable audit trails are an important mechanism for protecting privacy and strengthening user trust. PHR providers should be required to use immutable audit trails that note each instance of access and attempted access to consumer data and to give users access to such audit trails concerning their own data upon request.[63] Notice that immutable audit trails exist, as well as directions for how to access them, should be included in the PHR privacy policy.

A precedent for this recommendation exists in HIPAA, which provides that patients have a right to obtain from covered entities an annual report of disclosures from their records (except disclosures for treatment, payment or

[60] Markle Common Framework CPT2, Authentication of Consumers, http://www.connectingforhealth.org/phti/docs/CT2.pdf.
[61] Id.
[62] Markle Common Framework CPT2, Authentication of Consumers, http://www.connectingforhealth.org/phti/docs/CT2.pdf.
[63] Markle Common Framework CT3, Immutable Audit Trails, http://www.connectingforhealth.org/phti/docs/CT3.pdf.

health care operations) over the period of six years prior to the request.[64] ARRA strengthens this right: covered entities may no longer exempt disclosures for TPO, although the accounting need only cover the previous three years.[65] Consistent with CDT's recommendation that consumers should have control over information in PHRs, the audit provisions should require the tracking of all uses and disclosures of information in the PHR without a set time limitation.

8. Place strong prohibitions on the re-identification of aggregate/de-identified data from a PHR

As mentioned above, where the PHR vendor's policies permit the use of aggregate or de-identified data in a PHR, vendors should be required to use rigorous methods to prevent re-identification, including, when applicable, contractually binding business partners from unauthorized re-identification of data. However, in recognition of the increasing technological difficulty of protecting de-identified data against re-identification, CDT has called for a strengthening of the current HIPAA Privacy Rule on de-identification, as well as stronger legal prohibitions against re-identification.[66] Regardless of what happens under the HIPAA rule, policy pertaining to PHRs should include a strong prohibition against unauthorized re-identification of data obtained from PHRs, including penalties for those who inappropriately re-identify.[67]

9. Require that data in a PHR be portable, human-readable and divisible

PHR users must be able to transfer their data among PHR products in order to build longitudinal records of their health information that span providers over time. Consumers should also be able to open up more than one PHR account. In addition, users may choose to use their data in a variety of applications or devices external to the PHR. To meet these consumer interests, PHR providers should initially be required to make health data available and downloadable to users in a human-readable format. Ultimately, PHR providers and related applications should use industry-standard data sets as they become available and more broadly implemented.[68] Federal incentives programs such as Meaningful Use should encourage the use of standardized clinical summary formats.

---

[64] See CFR section 164.528. ARRA amendments to HIPAA expanded covered entities' obligation to share with patients' information about disclosures including routine activities for purposes of treatment, payment, and operations—which had not previously been required. (ARRA requires access to reports for only a three-year period.) See ARRA section 13405(c).

[65] See ARRA section 13405(c).

[66] For CDT's general recommendations concerning treatment of de-identified data, see "Encouraging the Use of, and Rethinking Protections for De-Identified (and 'Anonymized') Health Data" (Jun. 2009) http://www.cdt.org/healthprivacy/20090625_deidentify.pdf.

[67] See Markle Common Framework CT4, Limitations on Identifying Information, http://www.connectingforhealth.org/phti/docs/CT4.pdf, which recommends that chain of trust agreements prohibit reidentification.

[68] Markle Common Framework CT5, Portability of Information, http://www.connectingforhealth.org/phti/docs/CT5.pdf.

PHR users should also be able to share only part of their records, rather than be limited to sharing only the whole record or not at all. A PHR is less useful if users can only disclose the entire longitudinal record to doctors who may find only a fraction of it relevant. Users should have the ability to decide what information in the PHR they consider sensitive and segregate it. Users should then be able to exercise different privacy choices with regard to the two sets of data, such as restrict viewing of the segregated data in the PHR with an additional password designated by the user.

10. Require PHR providers to adopt FIPs for data collected about consumers' use of PHRs or their activities on-line

It is likely that PHR service providers and related entities will want to collect data about their users' behavior as it relates to using their PHR accounts or their activities online. For example, PHR providers may routinely collect data about a consumer's interaction with the PHR site, or use cookies to collect data about the web pages a consumer views while logged into his or her online PHR account. Such ancillary data is personal to the user and must be included within a privacy framework designed to protect data associated with PHRs.[69]

As mentioned above, CDT submitted comments to the FTC regarding how to address some of the unique privacy challenges that have emerged in the digital age.[70] In these comments, CDT urges the FTC to apply a full set of FIPs such as those outlined by the federal Department of Homeland Security in 2008—which are also similar to the iteration underlying the Markle Common Framework. CDT also released a paper that provides more detailed recommendations for protecting consumers in the online behavioral advertising space through the application of a full set of FIPs.[71] We urge policymakers to implement these principles to protect data collected about PHR users.[72]

11. Make all PHRs subject to consistent federal rules

To avoid creating confusion and potential harm to consumers, as well as stifling investment and innovation on the part of PHR providers, PHRs should be subject to consistent rules, regardless of whether or not they are offered through entities covered by HIPAA (either as covered entities or business associates). [73]As previously discussed, making rules consistent for all PHRs does not imply that it

---

[69] Markle Common Framework CT1, Technology Overview, http://www.connectingforhealth.org/phti/docs/CT1.pdf.
[70] See CDT Comments to the FTC, Nov. 6, 2009.
[71] See CDT's paper on Online Behavioral Advertising: Industry's Current Self-Regulatory Framework is Necessary, But Still Insufficient On Its Own To Protect Consumers (December 2009), http://www.cdt.org/files/pdfs/CDT%20Online%20Behavioral%20Advertising%20Report.pdf.
[72] Markle Common Framework CP3, Consumer Consent to Collections, Uses, and Disclosures of Information, http://www.connectingforhealth.org/phti/docs/CP3.pdf.
[73] Markle Common Framework CP1, Policy Overview, http://www.connectingforhealth.org/phti/docs/CP1.pdf.

is appropriate to simply extend HIPAA rules in their current form to uncovered entities supplying PHRs or related health information products or services. Rather, a new set of policies and practices modeled on the recommendations set forth in this paper and the Markle Common Framework should be required for entities that provide PHRs.

Unfortunately, ARRA's provisions reinforce the existing distinction between PHRs offered by HIPAA-covered entities or their business associates and those that are not covered by HIPAA. Thus, further efforts by policymakers are needed to establish consistency in the policy framework.[74] For example, ARRA tasks HHS to work with FTC in making recommendations concerning regulations for PHRs – but this study is directed to cover only PHRs that fall outside of HIPAA's scope, which would customarily be regulated by the FTC. Similarly, the provisions in ARRA requiring that individuals be notified in the event of a breach of information in their PHRs are different for PHRs covered by HIPAA and those that are not. For PHR vendors not covered by HIPAA, the definition of breach turns on whether or not the individual authorized the particular access, use, or disclosure of information in the PHR. In contrast, a breach of information in a HIPAA-covered PHR depends on whether or not the Privacy Rule has authorized the particular access, use, or disclosure of information.

To help address this inconsistency, CDT has urged HHS to extend the definition of breach that applies to non-HIPAA covered PHRs to all PHRs offered to consumers on terms that give the individual control over information in the PHR.[75] If the PHR provider gives individuals control over how data is accessed in their accounts, notification should occur in all circumstances in which the individual has not authorized the access or disclosure (the definition of breach for PHR vendors not covered by HIPAA). CDT is also urging HHS, which is required to make recommendations to Congress on rules for PHRs, to recommend consistent policies for all PHRs.[76]

12. Extend federal policies beyond PHR vendors to others with significant access to PHR information

Since one of the benefits of PHRs is to make it easier for consumers to share their health information, user protection policies would be incomplete if they did not extend beyond PHR providers to others who may gain access to personal

[74] National Committee on Vital and Health Statistics, Statement of Deven McGraw, Hearing on Personal Health Records (Jun. 9, 2009), http://www.cdt.org/healthprivacy/20090609_phr_testy.pdf.

[75] See CDT's Joint Comments to HHS on Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements The American Recovery and Reinvestment Act of 2009, (May 21, 2009) http://www.cdt.org/files/pdfs/CDT%20Comments_Guidance_HHS_Health%20Breach%20Notification.pdf. See also CDT's Joint Comments to the FTC on Health Data Breach Notification Rulemaking (Jun. 1, 2009), http://www.cdt.org/files/pdfs/CDT%20Joint%20Comments%20to%20FTC.pdf

[76] Id. See also National Committee on Vital and Health Statistics, Statement of Deven McGraw, Hearing on Personal Health Records (Jun. 9, 2009).

health information through a PHR.

ARRA contemplates the need to directly regulate entities that access data in a PHR. The statute requires HHS and FTC to develop privacy and security recommendations that apply also to: 1) entities that offer products or services through the website of the PHR provider, 2) entities not covered by HIPAA that offer products or services through the website of a covered entity that provides PHRs to consumers, 3) entities not covered by HIPAA that access health information in a PHR or send information to a PHR, and 4) third party service providers used by the PHR provider (or by one of the other entities above) to help in providing PHR products or services.[77]

In developing its regulations on breach notification for PHRs not covered by HIPAA, the FTC essentially adopted the same classification, referring to entities in categories 1-3 above as "PHR related entities." However, the FTC expanded the concept of "third party service provider" (category 4) to include not only entities that provide services to PHR vendors, but also to third parties that provide services to PHR related entities *and* that access or disclose unsecured PHI in a PHR as a result of the services.[78] An example of a PHR related entity is one that provides an application using data from the PHR to help users monitor a particular aspect of their health, such as blood pressure readings over time. A third party service provider, by contrast, would be the provider of a "back end" service, such as backing up data, which is in most cases not evident to the user.

Under the FTC rule, entities covered by categories 1-3 must directly notify an individual in the event of a breach of that individual's data; third party service providers are responsible for notifying the vendor, who in turn must notify the individual. This approach places direct obligations on entities that access an individual's data because they establish a relationship with the account holder, while requiring chain of trust agreements for third party service providers. This strategy distinguishes between entities that have established a direct relationship with the individual user, and therefore should be fully accountable to that user, and those whose access to data is dependent on their contractual relationship with the PHR vendor. CDT thinks this approach is good public policy.

Unfortunately, the HIPAA Privacy Rule, as recently amended by ARRA, creates – through its business associate rules – confusion about the responsibilities of PHR vendors, PHR related entities, and providers of third party services. Business associates under the Privacy Rule are entities or individuals not part of a covered entity's workforce that perform a service on behalf of the covered entity using protected health information.[79] Under ARRA, business associates can be held accountable by regulators for failure to comply with some provisions of the Privacy Rule, but their obligations to individuals are largely defined by the terms of their agreement with the covered entity.[80] For example, in the event of a breach by a business associate, the business associate is obligated to notify the

[77] See ARRA section 13424 (Studies, Reports, Guidance).
[78] See FTC, Final Rule, 16 CFR Part 318.
[79] 45 C.F.R. section 160.103.
[80] See ARRA sections 13401 and 13404.

covered entity, which then has the obligation to notify the individual whose data was breached.[81] Under the framework we set forth above, this is appropriate when the business associate is behaving more like a third-party service provider. However, there are circumstances in which a business associate is the vendor of the PHR or operates more like a PHR related entity and has an independent relationship with the consumer.

Under ARRA, if a PHR vendor or PHR related entity is also a business associate, it is unclear whether the entity is directly accountable to the consumer or not. In our view, the standard of direct accountability should govern, and policymakers should provide further clarification.

13. Require PHR providers to clarify to consumers their relationships with third-party applications and websites

An individual PHR provider's ecosystem will likely include a number of actors, including PHR entities offering various applications and websites to help consumers better manage and enhance their own health care or that of a family member. But when consumers interact with these applications and websites, the latter may gain access to the contents of their PHRs. Therefore, per our discussion above, the same federal policies that apply to PHR providers should be extended to their third-party applications and websites in an effort to further protect the privacy and security of user data. PHR providers also should clearly communicate with users about the precise nature of their relationships with these applications and websites. This transparency will help build consumer trust in PHRs and ensure that consumers feel safe in their interactions with third party applications and websites.

Consumers control access to the information in the PHR, deciding whether to share it with applications and websites, and for what reasons. But in doing so, consumers may not realize that applications introduce third parties into the PHR space. Moreover, consumers may not be readily aware of the policies governing these applications and websites. Therefore, PHR providers should state clearly what privacy and security protections the PHR provider takes responsibility for with respect to third-party applications and websites, and what responsibilities are left to the discretion of the applications and websites themselves. Additionally, this information should not be buried in a PHR provider's privacy policy or terms of service. Rather, this information should be made clear to the user in an effective and prominent way.[82]

For example, a PHR provider could employ a "warning screen" whereby a user would receive an unavoidable notice about the PHR provider's relationship with a third-party application or website before any transfer of health data takes place. Additionally, a PHR provider could use its "Help Page" or "FAQ" section to educate consumers about its relationship with third-party applications and websites. Policymakers and service providers should consider these and other

[81] See ARRA section 13407 (a) and (b).
[82] Markle Common Framework CP2, Policy Notice to Consumers, http://www.connectingforhealth.org/phti/docs/CP2.pdf.

potential mechanisms by which this information might be more effectively communicated by PHR providers to consumers.

14. Require Strong and Consistent Enforcement of Rules

It is critical for policymakers to continue to monitor the scope of activities in this space and act promptly to prohibit those that take unfair advantage of consumers.[83] Building trust in PHRs requires development, implementation, and *effective enforcement* of a comprehensive set of privacy and security policies and technology requirements. Such effective enforcement will likely be achieved through a mix of strategies, including chain of trust agreements, leveraging government's buying power through spending conditions, self-attestation with independent third-party validation, consumer-based ratings, and enforcement of existing and new laws. [84]

Today, regulatory enforcement responsibility and penalties differ depending on the applicable legal regime. PHRs covered by HIPAA are subject to the Privacy Rule's enforcement provisions, which were considerably strengthened in ARRA and are enforced by HHS. In contrast, the FTC has authority to bring action against some PHR vendors if they violate their privacy policies or engage in other conduct deemed to be unfair or deceptive under Section 5(a) of the FTC Act.[85] The procedures and remedies available to the FTC are quite different from those of HHS, and there is no assurance that conduct found illegal by one would be found illegal by the other.

As previously mentioned, ARRA directed HHS to consult with the FTC make recommendations to Congress on privacy and security rules for PHRs, including enforcement.[86] In this study, the agencies also need to recommend which agency should enforce protections for PHRs. CDT recommends that consistent privacy and security rules be established for all PHRs and, ideally, that the FTC be given the authority to enforce those requirements against all entities offering PHRs or services related to PHRs. The FTC is most equipped to take on the role of enforcer because, as the nation's consumer protection agency, it has extensive experience in protecting the rights of consumers.

However, CDT acknowledges that the FTC and HHS are more likely to share enforcement responsibilities for PHRs, and that HHS has expertise in dealing with the rights of consumers with respect to data controlled by health care entities. If Congress determines that HHS should continue to regulate those PHRs provided by HIPAA covered entities, it would still be very important that

---

[83] See CDT Comments to the FTC, November 6, 2009, where we urge FTC to more actively use its unfair trade practices jurisdiction to crack down on activities that violate consumer privacy.

[84] Markle Common Framework CP9, Enforcement of Policies, http://www.connectingforhealth.org/phti/docs/CP9.pdf. See also CP4, Chain-of-Trust Agreements, http://www.connectingforhealth.org/phti/docs/CP4.pdf.

[85] 15 U.S.C. section 45(a)(1). The reach is limited by scope of authority under section 5.

[86] ARRA section 13424(b). The study and report must be completed by February 18, 2010.

PHRs be subject to consistent rules and that both regulating agencies make enforcement of these rules a top priority.

An effective enforcement scheme for PHRs would, at a minimum, include the following elements:

- Authorization to both federal and state consumer protection authorities for enforcement of federal provisions. Resources for enforcement are always strained, and authorizing both federal and state authorities to enforce federal consumer protection laws, which have precedent,[87] will enhance the potential for a more effective enforcement regime.

- Criminal and civil penalties set at a level that provides a strong incentive for compliance with the law.

- Clear audit authority.

- Regular public reports to Congress by federal regulators on enforcement.

In addition, CDT believes it is appropriate in this context to provide individuals with a private right of action to sue in federal court for violations of PHR privacy provisions. We note that neither HIPAA as amended by ARRA, nor section 5(a) of the FTC Act, affords individuals a private right of action, even for the most egregious violations.

However, the unique nature of PHRs presents a particular circumstance in which a private right of action would be an appropriate enforcement option. Consumers are being encouraged to put some of their most sensitive data into "the cloud" on the promise that the data will be safe and that the consumer will have a high degree of control over that information. The PHR is, by definition, intended to be uniquely the consumer's *personal* record. Therefore, PHR providers should be directly accountable to the consumer.

A private right of action could be structured with some limits on damages to discourage frivolous suits. For example, the Telephone Consumer Protection Act (TCPA) allows individuals to bring a private right of action for violations; recovery is set at $500 for each violation.[88] If the court finds the defendant willfully or knowingly violated the TCPA. The court may, in its discretion, increase the award to an amount equal to not more than three times the $500 limit.[89]

---

[87] HIPAA rules can be enforced by state Attorneys General (AGs), see ARRA section 13410(e). In addition, state AGs can enforced federal antitrust laws, CAN-SPAM (P.L. 108-187) ("Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003"), and the Communications Act of 1934. These laws typically include provisions to ensure that entities are not subject to both federal and state action for the same offense, and CDT supports the inclusion of such provision with respect to PHRs as well.

[88] 47 USC 227. TCPA was enacted in 1991 to regulate commercial solicitation calls made to residences.

[89] Id.

15. Preserve privilege of data in PHRs

The confidentiality of many medical records is protected via the doctor/patient privilege to encourage frank discussion within the doctor/patient relationship. Privilege, however, traditionally depends on the secrecy of the communication and can be waived if the keeper of the privilege – i.e., the patient – voluntarily discloses the privileged information to a party outside of the privileged relationship. It is unclear whether courts would consider privilege to be waived if the patient transfers medical data to a PHR,[90] but the risk for waiver of privilege through PHRs is strong enough that it should be addressed in regulation.[91]

CDT believes doctor/patient privilege should be preserved to encourage use of PHRs as health self-management tools and to maintain openness between patients and doctors. Most privilege law is established at the state level, so in order to preserve privilege then either federal law would have to preempt state law in this area or the state regulators would have to address the issue. Either way, federal or state regulators should explicitly state that privilege in medical data is not lost for the sole reason that it is uploaded to a PHR or transferred between doctor and patient using an electronic communication service.[92] Regulators should also consider how to preserve legal protections for other kinds of health information (i.e., genetic, substance abuse, mental health) that may be eliminated if the information is transferred to a PHR.

Conclusion

Use of PHRs could help bring about significant improvements in health care, providing consumers with an effective way of storing and managing their health data and giving them tools to be more engaged in their own health. Whether PHRs will realize their potential depends in substantial part on the extent to which consumers trust that data they store in and share via their PHR is appropriately protected from misuse. Federal law today offers only a patchwork of protections at best – and does not effectively respond to the risks confronting consumers using these tools.

Building consumer trust in PHRs requires the implementation and enforcement of a comprehensive, robust framework of privacy and security protections that apply

---

[90] Some courts recognize that attorney/client privilege may not waived by mere use of an email service to transmit confidential communications, despite the routine practice among email service providers of scanning messages for business purposes. See generally Marjorie A. Shields, Annotation, *Application of Attorney-Client Privilege to Electronic Documents*, 26 A.L.R. 6th 287 (2007) (identifying numerous cases where privilege was and was not found to exist). See also Nancy A. Wanderer, *E-mail for Lawyers: Cause For Celebration and Concern*, 21 Me. B.J. 196, 196 (2006).

[91] See Robert Gellman, *Personal Health Records: Why Many PHRs Threaten Privacy*, World Privacy Forum, Pg. 5, Feb. 20, 2008, http://www.worldprivacyforum.org/pdf/WPF_PHR_02_20_2008fs.pdf.

[92] Some state legislatures have enacted similar provisions for electronic communication services. See, e.g., N.Y.C.P.L.R. 4548 (2007) and Cal. Evid. Code § 917(b) (2009).

to both the data in the PHR, as well as data collected about consumers as they use their PHRs. The Markle Common Framework, already strongly supported by industry stakeholders and consumers, provides a comprehensive set of policy and technology expectations for PHRs. CDT calls on regulators to bolster this framework with a baseline of legally enforceable privacy and security protections, as well as incentives for industry best practices. By preserving consumer trust and providing certainty to the PHR marketplace, the right PHR regulations can drive the revolution in self-managed health care that is waiting to happen.

Appendix A –
CDT PHR Workshop Participants, May 13, 2009

Julie Barnes, New America Foundation
Peter Blenkinsop, International Pharmaceutical Privacy Consortium
Alice Borelli, Intel
Pablo Chavez, Google
Alissa Cooper, CDT
Dave deBronkart, Society for Participatory Medicine
Christine Dodd, IBM
Stephen Downs, Robert Wood Johnson Foundation/Project HealthDesign
Joyce Dubow, AARP
Colin Evans, Dossia
Steve Findlay, Consumers Union
Lisa Gallagher, HIMSS
Harley Geiger, CDT
Bob Gellman, Privacy and Information Policy Consultant
Joy Grossman, Center for the Study of Health System Change
Leslie Harris, CDT
Jody Hoffman, Better Health Care Together
Brian Huseman, Intel
Irene Koch, Brooklyn Health Information Exchange
Joseph Kvedar, Center for Connected Health
Richard Marks, Patient Command, Inc.
Philip Marshall, WebMD
Deven McGraw, CDT
Julie Murchinson, Health 2.0 Accelerator
Sheel Pandya, CDT
Jody Pettit
Eva Powell, National Partnership for Women and Families
Joy Pritts, Georgetown University Health Policy Institute
Alison Rein, AcademyHealth
Lygeia Ricciardi, Clear Voice Consulting
Jason Rothstein, Clear Voice Consulting
Alan Rubel, CDT
Josh Seidman, Center for Information Therapy
Michael Stokes, Microsoft
Ann Waldo, Ann Waldo, PLLC
Marcy Wilder, Hogan & Hartson
Claudia Williams, Markle Foundation
Bill Yasnoff, NHII Advisors

Appendix B –
Brief overview of current legal environment as it applies to PHRs

HIPAA

The HIPAA Privacy Rule (Privacy Rule) applies to some but not all PHRs. The Privacy Rule sets forth specific requirements and prohibitions regarding access, use, and disclosure of individually identifiable health information (i.e., protected health information, or PHI) by "covered entities" and business associates of covered entities. Covered entities include health plans, health care clearinghouses, and most health care providers who submit health care claims electronically.[93] Business associates of covered entities are persons or organizations that provide services for or functions on behalf of the covered entities that involve use or disclosure of individually identifiable health information, for example, claims processing, data analysis, and billing.[94] Through contracts known as – "business associate agreements" – covered entities must require their business associates to protect the PHI they receive.[95]

The Privacy Rule restricts covered entities from using or disclosing protected health information under any circumstance other than those enumerated in the rule. It allows information to be shared with the individual,[96] with other entities for "treatment, payment, or health care operations,"[97] and when the information is properly de-identified.[98] Other exceptions include disclosures to law enforcement and for public health purposes. For disclosures that are not for treatment, payment, and health care operations, or are not otherwise covered by an express exception, the Privacy Rule requires patient authorization. The Privacy Rule does not allow for blanket or general consent to disclosure of protected health information. Under the Privacy Rule, an authorization form must be in plain language and must specify the information to be disclosed, to whom the information will be disclosed, when authorization expires, and in some cases the purpose of the disclosure.[99]

The HIPAA Privacy Rule applies to PHRs provided by covered entities, such as health care providers or insurers, or by business associates of covered entities, such as those that contract with covered entities to provide PHRs. However, many PHRs will be provided by non-covered entities. This includes, for example, those offered as Internet products (e.g., from Google, Microsoft, and WebMD) and those offered by individual employers. HIPAA does not apply to such PHRs.

---

[93] See HHS Office of Civil Rights Privacy Brief: Summary of the HIPAA Privacy Rule (May 2003), http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.
[94] Id., p. 3; 45 C.F.R. §160.103.
[95] Id.; 45 C.F.R. §§164.502(e), 164.504(e).
[96] 45 C.F.R. §164.502(a)(1)(i).
[97] 45 C.F.R. §164.502(a)(1)(ii).
[98] 45 C.F.R. §§164.502(a)(1)(iii), 164.502(b), 164.514(d).
[99] 45 C.F.R. §164.508(c). See generally Center for Democracy & Technology (CDT), Rethinking the Role of Consent in Protecting Health Information Privacy (Jan. 2009), http://www.cdt.org/healthprivacy/20090126Consent.pdf.

ARRA

The American Recovery and Reinvestment Act of 2009 (ARRA) addressed certain gaps in HIPAA's applicability. Under the ARRA, an entity offering PHRs, but which is not a HIPAA-covered entity, is a "vendor of personal health records."[100] Under ARRA, such vendors of PHRs are subject to the requirement to notify their users if their information is breached.[101]

In addition, ARRA extended the HIPAA Privacy Rule to vendors of PHRs when they offer a PHR on behalf of a covered entity "as part of [the covered entity's] electronic health record." There has been some confusion about the scope of this section. It appears to apply only to PHR vendors insofar as they contract with covered entities so that the covered entity can provide its own PHR to its patients. It appears not to apply to situations where a covered entity enters into an arrangement with a PHR vendor so that patients can easily enroll in the vendor's PHR.[102]

Finally, the ARRA directs the HHS Secretary, in consultation with the Federal Trade Commission, to provide recommendations to Congress regarding privacy and security protection for PHRs that do not fall under HIPAA.[103]

FTC Act

Another federal statute applicable to PHRs is the Federal Trade Commission Act (FTC Act).[104] Section 5 of the FTC Act states that "unfair or deceptive acts or practices in or affecting commerce ... are ... unlawful."[105] The Act empowers the FTC to conduct investigations. If, after an investigation, the FTC has reason to believe a violation has occurred, it can commence an administrative enforcement proceeding and may seek equitable remedies, including restitution for injured consumers and disgorgement of profits from violators.[106]

The FTC Act has used its Section 5 authority to address privacy and security concerns, and the authority, while limited, certainly applies to PHRs. The FTC has made it clear that it is illegal under Section 5 to violate privacy or security promises made in privacy policies or other assurances to consumers. Thus, the Act could be used where PHR providers advertise that consumer information is private, but have practices that fail to protect privacy to the extent implied in the advertising.[107] The efficacy of the FTC Act in this regard is limited insofar as there

---

[100] American Recovery and Reinvestment Act of 2009, Title XIII, subtitle D, Privacy (ARRA), §13400(18), ("The term 'vendor of personal health records' means an entity, other than a covered entity . . . that offers or maintains a personal health record.")
[101] ARRA §13402. The breach notification requirement will go into effect in Sep. 2010.
[102] ARRA §13408.
[103] ARRA §13424.
[104] 15 U.S.C. §§41-58.
[105] 15 U.S.C. Sec. §45(a)(1)
[106] 15 U.S.C. §45(b). It may also commence an administrative rulemaking process to remedy unfair or deceptive practices that occur industry-wide. 15 U.S.C. §57(a).
[107] Bruce Schneier, Do You Know Where Your Data Are?, Wall Street Journal, Apr. 28, 2009.

is no requirement that PHRs have a privacy policy or make any statements about privacy and security in the first place. In addition, however, in some cases, the FTC has brought enforcement actions and obtained consent orders even in the absence of a security or privacy assurance against companies that failed to protect the security of customer data or that engaged in certain activities harmful to the privacy of users. CDT has urged the FTC to more aggressively use its unfairness jurisdiction in privacy cases.[108] However, the exact scope of what the FTC will consider to be illegal privacy or security practices in the absence of a promise remains unclear; the FTC is effectively developing standards on a case-by-case basis.

ECPA/SCA

Another federal law that may apply to PHRs is the Electronic Communications Privacy Act (ECPA), specifically the provisions known as the Stored Communications Act (SCA). The SCA prohibits entities providing "electronic communication service" or "remote computing service" to the public from divulging the contents of communications carried or stored by that service, absent consent.[109] It also sets out conditions under which such entities can be compelled to divulge the contents of such communications.[110] "Remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[111] PHRs seem to fit within this definition.[112] In fact, the legislative history of the SCA specifically references offsite storage and processing of medical information by hospitals as remote computing services.[113] However, there are important limitations to the SCA's applicability in the context of PHRs.

First is the matter of consent. The SCA's protections can be waived by consent.[114] The "terms of service" that consumers must agree to before using a PHR could include provisions giving consent to a wide range of disclosures. It is unclear whether consent in terms of service would be adequate – the answer may depend on how the consent is presented -- but, if it were adequate, it would override the Act's protections.

Another limitation of the SCA is that it prohibits disclosures only by providers of service "to the public." Certainly where anyone can sign up for a PHR, it would be provided to the public. However, where PHRs are offered only to those in some kind of prior relationship, for example if an employer offers PHRs to its

---

[108] See CDT's November 6, 2009 Comments to the FTC on Refocusing the FTC's Role in Privacy Protection, at http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf.
[109] 18 U.S.C. §§2702(a)(1)-(2).
[110] 18 U.S.C. §2703.
[111] 18 U.S.C. §2711(2).
[112] See, for example, R.D. Marks, eHealth Initiative Policy Paper: Regulating Personal Health Records—Why HIPAA Won't Work (2008), http://www.ehealthinitiative.org/events/papers/Patient_Command_09-01-08.pdf.
[113] S. Rpt. No. 99-541, at 2-3 (1986).
[114] 18 U.S.C. §2702(b)(3).

employees or if a health plan offers a PHR to its members, they likely would not be offered to the public and therefore would not be covered by the SCA. [115]

Also, the protections of ECPA apply to communications stored by a remote computing service only if "the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[116] If a PHR is advertising supported and the entity offering the PHR analyzes individual patient records to target ads, the PHR might not be covered by ECPA. Likewise, if the PHR service includes targeted medical advice or other analytic services using the content of a subscriber's records, the service may fall outside ECPA's coverage. Finally, it should be noted that the SCA allows governmental entities to use a mere subpoena to obtain communications held by a remote computing service, in many cases without notice to the subscriber.[117]

ECPA and the SCA have been criticized as being too narrowly based upon the technology extant at the time they were drafted, and it has been suggested that they be revisited to make them compatible with subsequent technological development.[118] In their present form, though, ECPA and the SCA seem to be applicable to at least some PHRs.

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)[119] applies to financial institutions, which are "companies that offer financial products or services to individuals, like loans, financial or investment advice, or insurance."[120] While most providers of PHRs would not fall within the purview of the GLBA, there may be some financial institutions that offer PHRs; for example, a bank might offer a PHR in conjunction with a health savings account. In such cases, the privacy protection provisions of the GLBA might apply. Those protections include the requirements that financial institutions establish precautions to protect consumer information from anticipated threats, provide adequate notice of their information sharing policies, and give consumers a right to opt out of some information sharing.[121] The GLBA also contains a prohibition against "pretexting," or obtaining customer information under false pretenses.[122]

Computer Fraud and Abuse Act

---

[115] See Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042-43 (N.D. Ill. 1998).
[116] 18 U.S.C. §2702(a)(2)(B).
[117] 18 U.S.C. §2703.
[118] Orin Kerr, Surveillance Law: Reshaping the Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208 (2004). A diverse coalition of companies, think tanks and privacy advocates has also recommended updating ECPA, http://www.digitaldueprocess.org.
[119] Pub.L. 106-102, 113 Stat. 1338, (Nov. 12, 1999).
[120] Federal Trade Commission, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm.
[121] 15 U.S.C. §§6801-6803; see FTC, In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act.
[122] 15 U.S.C. §6821.

The Computer Fraud and Abuse Act[123] is another federal statute potentially applicable in the context of PHRs. Broadly speaking, the CFAA criminalizes the unauthorized access to and use of protected computers. The definition of "protected computers" is expansive, and includes any computer "used in interstate or foreign commerce or communication."[124] Among the actions proscribed is unauthorized access to a computer and thereby obtaining "information from any protected computer if the conduct involved an interstate or foreign communication."[125]

At the very least, the CFAA makes it a crime to break into a computer system hosting PHRs and obtain information, but it is not entirely clear what are the outer limits on what constitutes accessing a protected computer "without authorization or exceed[ing] authorization." The potential reach of the concept was illustrated in the widely publicized prosecution and conviction of Lori Drew. Drew was charged under the CFAA with accessing a protected computer without authorization or in excess of authorization and thereby obtaining information from that computer. The charge was based upon Drew's violation of the terms of service of the social networking site MySpace. The conviction was set aside by the district court judge on the ground that Drew's violation of the terms of service did not constitute a crime under the Act, but the decision is not binding nationwide and the full scope of the Act remains unresolved.[126]

FDCA

In addition to regulating food, drugs, and cosmetics, the Food Drug and Cosmetic Act regulates medical "devices." A device can be, among other things, an "instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article," which is "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease…."[127] Part of the promise of PHRs is that they can be used for disease, diagnosis, treatment, and prevention; thus, they are at least candidates to be "devices" under the statute. At present, the FDA has convened a working group to determine whether electronic health records (including PHRs) should be considered "devices" under the law. One commentator suggests that the decision could turn on whether the FDA sees the records as mere electronic equivalents of paper records, in which case they are less likely to be considered devices, or it sees them as having "clinically directive functions," in which case they are more likely to be considered devices.[128]

State Laws

A variety of state laws could apply to PHRs. Many states have consumer fraud protection statutes, similar to the FTC Act, that prohibit deceptive trade practices. Unlike the FTC Act, these may create private causes of action and may provide

---

[123] 18 U.S.C. §1030.
[124] 15 U.S.C. §1030(e)(2).
[125] 15 U.S.C. §1030(a)(2)(C).
[126] *U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009).
[127] 21 U.S.C. §321(h).
[128] FDA Creates Working Group on Regulation of Electronic Health Record Systems, Apr. 2, 2009, http://www.ropesgray.com/fdaregulationofelectronichealthrecordsystems/.

for treble damages. There are also state laws specifically applying to health data, and these may apply to PHRs. California, for example, has a Confidentiality of Medical Information Act, a Patient Access to Health Records Act, and an Insurance Information and Privacy Protection Act.[129] State laws that are more stringent than HIPAA are not preempted; that is, HIPAA creates a floor of protection rather than a ceiling. [130] And where PHRs are provided by non-HIPAA covered entities, preemption is not an issue; the state law applies.

[129] Calif. Civil Code §56 et seq., Calif. Health & Safety Code § 123110 et seq., Calif. Insurance Code § 791 et seq. See California Office of Information Security and Privacy Protection, Your Patient Privacy Rights: A Consumer Guide to Health Information Privacy in California, http://www.oispp.ca.gov/consumer_privacy/consumer/documents/html/cis7english.asp.

[130] Institute of Medicine, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research (National Academies Press, 2009), p. 187-88.