MAXIMUS Federal Services

Non-HIPAA Covered Entities:
Privacy and Security Policies and Practices of PHR Vendors and Related Entities Report

Submitted to:

The Office of the National Coordinator for Health Information Technology

Office of the Chief Privacy Officer

December 13, 2012

Table of Contents

EXECUTIVE SUMMARY

As part of the Health Information Technology for Economic and Clinical Health (HITECH) Act,[1] Congress directed the Secretary of the U.S. Department of Health and Human Services (HHS) to conduct a study and submit a report to Congress on privacy and security requirements for entities that are not covered entities (CEs) or business associates (BAs) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[2] including those that are vendors of or interact with Personal Health Records (PHRs).[3] This paper uses the term "non-HIPAA PHRs" to refer to PHR vendors that are not covered entities or business associates, and which are therefore not subject to HIPAA and HIPAA regulations. This paper contributes to the development of a comprehensive report for Congress by providing an analysis of the definition and characteristics of PHRs, current legislation governing PHRs, the privacy and security practices of selected PHR vendors and related entities, and consumer views on both PHRs and PHR privacy practices.

The analysis and content of this report draw on the following:

- A review of the HIPAA, HITECH, and Federal Trade Commission (FTC) legislation and regulations that may apply to PHRs, as well as the ways these laws have been interpreted;
- A review of administrative complaints filed before an administrative law judge of the FTC and judicial complaints filed in United States district court by the FTC against companies conducting business over the Internet for alleged FTC Act violations, as well as any relevant consent agreements between the FTC and the respondent in cases where the respondent decided to settle the matter rather than contest the charges;
- A review of the stated privacy and security policies and practices of selected non-HIPAA covered PHRs, entities with which they interact, and third party service providers; and
- A review of surveys and reports on consumer attitudes and knowledge of PHRs and privacy, as well as a review of discussions at the December 2010 ONC PHR Roundtable, *Personal Health Records: Understanding the Evolving Landscape*,[4] which addressed privacy and security requirements of PHRs.

DEFINING PHRS

The study first examines the definition and characteristics of PHRs, as well as the market for PHRs. Since there is no accepted single standard definition of a PHR in general use, this paper uses the HITECH Act's definition of a PHR as the basis for discussion. The HITECH Act defines a PHR as:

---

[1] Health Information Technology for Economic and Clinical Health (HITECH) Act, § 13424(b), Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5 (codified at 42 U.S.C. Chapter 156, §§ 17901-17953). *See also* Appendix A.

[2] Health Insurance Portability and Accountability Act (HIPAA), § 264, Pub. L. 104-191 (codified at 42 U.S.C. § 1320d-2). Under HIPAA, "covered entities" are health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a covered transaction; 45 C.F.R. § 160.103; "Business associates" are those entities that provide administrative or other services to covered entities involving the creation, reception, maintenance, or transmission of PHI by the business associate; 45 C.F.R. § 160.103.

[3] HITECH Act § 13424(b).

[4] ONC convened this roundtable of privacy and security experts and providers of PHRs to discuss the evolving landscape of PHRs. Participants in the panel can be found in Appendix B. ONC Roundtable: Personal Health Records - Understanding The Evolving Landscape 34 (December 3, 2010) (transcript available at http://www.healthit.gov/sites/default/files/120310_onc_editedc.pdf) (hereinafter ONC Roundtable).

> 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.[5]

At a very general level, PHRs differ from one another based on two main attributes: the entity that offers the PHR to the consumer, and the sources of data for populating the PHR. Healthcare providers, health insurance plans, non-profit organizations, employers, and commercial entities are all major categories of entities that offer PHRs to consumers. In addition, PHRs obtain data from a number of different sources including health care provider data in electronic health records (EHRs), health insurer claims data, consumer/patient-entered data, and mobile device data. The features and characteristics of PHRs are changing and evolving, as are the business models of PHRs. The changing nature of PHRs is a factor to consider when making recommendations for privacy and security requirements for PHRs.

LEGAL BACKGROUND

The study next looks to examine different federal and state privacy and security legal requirements that apply to PHRs. PHRs offered by covered entities as defined by HIPAA, such as health care providers and health plans, or offered by business associates of covered entities are subject to the HIPAA Privacy and Security Rules.[6] All PHRs operated by commercial entities may be subject to the FTC's authority to prevent "unfair or deceptive acts or practices in or affecting commerce."[7]

The HIPAA Privacy and Security Rules[8] apply to health care providers (such as physician practices and hospitals) and health plans that are "covered entities."[9] HIPAA protects the individually identifiable health information, or protected health information (PHI),[10] held by these covered entities regardless of whether it is held in a paper record, an EHR or a PHR.[11] Covered entities directly offering PHRs must comply with HIPAA and are subject to enforcement by the Office for Civil Rights (OCR) within HHS for non-criminal violations which may

---

[5] HITECH Act § 13400(11). Under the HITECH Act "PHR identifiable health information" includes any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual. The term also includes, with respect to an individual, information that is provided by or on behalf of the individual; and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." HITECH Act § 13407(f)(2) (defining PHR identifiable health information as meaning "individually identifiable health information as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)) as well as additional specified elements).

[6] The HITECH Act made business associates directly subject to the use and disclosure restrictions of the HIPAA Privacy Rule as well as the substantive provisions of the HIPAA Security Rule. HITECH Act §§ 13401, 13404.

[7] 15 U.S.C. § 45(a)(1)–(2) (2012). The FTC has jurisdiction over all persons, partnerships, or corporations, excluding banks, savings and loan institutions, credit unions, telecommunications companies, interstate transportation common carriers, packers and stockyard operators, and the insurance industry. *Id.*

[8] 45 C.F.R. Parts 160 and 164.

[9] This study did not identify any health care clearinghouses associated with a PHR, and as a result such entities are not considered in this study.

[10] Protected health information (PHI) is the health information protected by the HIPAA Privacy Rule and is a subset of individually identifiable health information that exclude certain identifiable health information, such as information from student health clinics—which is instead covered by the Federal Educational Rights and Privacy Act. The HIPAA Security Rule covers electronic protected health information. 45 C.F.R. §§ 160.103 and 164.302.

[11] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Personal Health Records and the HIPAA Privacy Rule*. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.

result in civil penalties of up to $50,000 per violation.[12] Under HITECH, vendors who contract with covered entities to offer PHRs on their behalf are considered business associates and must comply with most of the substantive provisions of the HIPAA Security Rule and the use and disclosure limits of the HIPAA Privacy Rule.[13] The HIPAA Privacy and Security Rules establish limits on how covered entities may use or disclose protected health information, as well as administrative, technical and physical standards, and implementation specifications for ensuring that PHI is kept secure. Additionally, the HIPAA Breach Notification Rule, which was promulgated pursuant to the HITECH Act, requires covered entities and business associates to provide notification following the breach of unsecured PHI.[14] However, these rules only apply to covered entities and business associates. As a result, non-HIPAA PHRs are not subject to these regulations.

Both non-HIPAA PHRs and PHR vendors that are HIPAA- covered entities and business associates are subject to the Federal Trade Commission Act (FTC Act).[15] The FTC has the authority under section 5 of the FTC Act to prevent "unfair or deceptive acts or practices in or affecting commerce" for all persons, partnerships or corporations within its jurisdiction.[16] While the FTC has not yet specifically invoked its section 5 authorities against non-HIPAA PHRs, complaints filed by the FTC against *other* companies conducting business over the Internet for alleged FTC Act violations may offer some insight into Internet privacy and security practices that might constitute "unfair or deceptive acts." However, allegations in FTC complaints are fact-specific and do not always establish binding requirements on other entities. In addition, the FTC generally takes action to enforce potential violations only when it "sees a pattern of possible violations developing" and thus will not take action until it determines there are enough instances of possible violations.[17] PHR vendors must make their own determinations of what practices are appropriate based on the health information they collect and the way they use or disclose that information. In previous allegations of FTC Act violations against Internet based companies, the FTC has stressed the following:

- Adhering to stated privacy practices including advertised participation in self-regulatory codes of conduct or compliance programs;[18]
- Providing to the consumer, information regarding the uses and disclosures of personal information that are material to the consumer in electing to share information with the applicable person or company;[19]
- Informing consumers when third parties outside of their direct consumer relationship will collect or

[12] 45 C.F.R. § 160.404. This amount applies to violations that occurred after February 18, 2009. There is a calendar year limit of $1,500,000 for civil penalties relating to a violation of the same requirement. *Id.*
[13] HITECH Act §§ 13401, 13404, and 13408.
[14] 45 C.F.R. Part 164, Subpart D.
[15] 15 U.S.C. § 45(a)(1)-(2); FTC and HHS OCR have concurrent jurisdiction with respect to PHRs that are subject to HIPAA. The requirements for breach notification for HIPAA covered entities differ from the requirements for breach notification for non-HIPAA covered entities. Non-HIPAA covered entities are subject to the regulations at 16 C.F.R. Part 318 regarding breach notification requirements. HIPAA covered entities are subject to the regulations at 45 C.F.R. Part 164, Subpart D regarding breach notification requirements.
[16] *Id*.
[17] Letter from the F.T.C. Consumer Response Center to Michael Carome, (Sept. 21, 2012), Retrieved from http://www.citizen.org/documents/2069_ftc_letter.pdf.
[18] F.T.C. v. Toysmart.com, LLC, F.T.C. File No. X000075 (July 21, 2000) (available at http://www.ftc.gov/os/caselist/x000075.shtm); Google Inc., F.T.C. File No. 102-3136 (Oct. 13, 2011) (available at http://www.ftc.gov/os/caselist/1023136/111024googlebuzzcmpt.pdf).
[19] F.T.C. v. Echometrix, FTC File No. 102 3006 (Nov. 30, 2010), (available at http://www.ftc.gov/os/caselist/1023006/101130echometrixcmpt.pdf).

have access to their information particularly when the third party has more lenient privacy policies;[20]
- Putting in place reasonable and appropriate security measures to protect consumer data by companies that provide general assurances about the protection of personal information; and[21]
- Maintaining reasonable and appropriate safeguards by companies that collect private information to protect private information based on the type of information they maintain and the risk its exposure presents to its consumers.[22]

Non-HIPAA PHRs are required to notify consumers and the FTC in the event of a breach pursuant to the regulations the FTC promulgated under the HITECH Act. [23]

In addition to federal privacy and security protections, some states have enacted privacy laws that apply to PHRs. Two states, California and Oregon, place the same restrictions on both EHRs and PHRs.[24] Five states also have breach notification laws which specifically apply to health information and forty-six states have breach notification laws that cover data, such as social security and account numbers, which may be collected by PHRs.[25]

In conclusion, the HIPAA paradigm sets forth formal and uniform privacy and security standards across the entire class of HIPAA-regulated entities. However, these set of rules do not apply to PHRs offered by entities that are not HIPAA- covered entities or business associates. The FTC uses administrative adjudications to protect consumers from violations of the privacy and security of their personal information on a case-by-case approach. The FTC's actions tend to overlook individual cases in favor of violations that are widespread, affect a large number of people, and have a greater potential impact. Therefore, neither the FTC enforcement actions nor HIPAA regulations currently provides adequate or complete privacy and security protections for consumer information contained in non-HIPAA PHRs.

PRIVACY AND SECURITY PRACTICES

The study also presents the findings from a review conducted by the authors of this paper of privacy and security policies of selected PHRs. The authors selected 41 PHRs to review. The review was limited to publicly available information on websites of these PHRs such as "Terms and Conditions" or "Privacy Policies."[26] This

[20] *In re* Vision I Properties, LLC, et al, FTC File No. 042 3068 (April 26, 2005) (available at http://www.ftc.gov/os/caselist/0423068/050426comp0423068.pdf).
[21] *In re* Dave & Buster's, Inc., F.T.C. File No. 082 3153 (June 8, 2010) (available at http://www.ftc.gov/os/caselist/0823153/100325davebusterscmpt.pdf). *In re* DSW Inc., F.T.C. File No. 052 3096 (March 14, 2006) (available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf); *In re* BJ's Wholesale Club, Inc., F.T.C. File No. 042 3160 (September 23, 2005) (available at http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf).
[22] *In re* Twitter, Inc., F.T.C. File No.092 3093 (March 11, 2011) (available at http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf).
[23] HITECH Act § 13407(a)-(b).
[24] California Civil Code § 56.06(a); Oregon Revised Statute § 413.308(5)(b) .
[25] Arkansas Code § 4-110-103(7); California Civil Code § 1798.29(g)(4); Missouri Revised Statute § 407.1500(9); Texas Business & Commercial Code § 521.002(a)(2)(B); Wisconsin Statute § 134.98(1)(b).
[26] This study does not include HIPAA PHRs that are solely regulated under HIPAA. Eight of the PHRs included in the study are offered directly to consumers, and are also sold by vendors to providers or health plans under business associate agreements with HIPAA-covered entities. These PHR vendors are covered by HIPAA as a business associate when covered entities contract with them to offer the PHR to their patients, but they are not covered by HIPAA when they offer the PHR directly to patients. Although HIPAA PHRs and non-HIPAA PHRs may be the same in many respects—i.e., applying the same security protections both in their HIPAA and in their non-HIPAA forms—they are covered by the different legal structures described in this report's Section III and may have other different features as a result. For example, a PHR may have advertising in its non-HIPAA form, but not have advertising in its HIPAA form due to HIPAA's constraints on marketing. The data presented herein represents only the non-HIPAA versions of these PHRs.

paper focuses on these public representations because these statements may be evaluated by the FTC when determining whether the PHR has engaged in unfair or deceptive trade practices. The authors used the Fair Information Practice Principles (FIPPs) as a framework by which to evaluate these policies, and examined the policies to determine which FIPPs principles each policy did or did not include. The FIPPs basic principles are:

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing

The authors found that PHR vendors do not follow a common or standardized approach to privacy practices and consumer notifications, nor do they have a clear standard, guidance, or regulation to assist them in developing notices communicating privacy and security practices to consumers. The authors found that PHR privacy practices vary and, in many instances, do not appear to comply with the FIPPs. They also found that most of the PHR privacy notices that were reviewed did not provide clear or complete information on how data would be used or shared with others. Few PHRs seemed to provide consumers with the choice to opt in or opt out of vendors' sharing data with others. In addition, the PHRs reviewed varied considerably in their practices regarding changes, corrections, and deletion of data.

With regard to security, the authors found that non-HIPAA PHRs are not subject to clearly delineated security standards. The authors found that security policies presented on the websites were not always specific on identity management issues, such as access controls and methods for detecting unauthorized access. They also found that PHR user identity proofing often relies on data that could be known to others, such as date of birth, and that user authentication practices are generally limited to user name and passwords. Finally, they found that when selecting passwords, in most cases, users could select weak passwords (i.e., less than six characters).

Finally, the authors found that a number of PHR vendors had obtained private sector certifications to indicate that the PHR vendor meets specified privacy and security criteria. These vendors displayed a certification logo on their websites to indicate the accrediting body from which they received the certification. The most common certifying bodies associated with the PHRs reviewed were URAC (formerly the Utilization Review Accreditation Committee), TRUSTe and the Health on the Net Foundation (HON). However, the authors learned that the standards the PHR must meet in order to obtain certification vary across these certifying organizations, and less than half of the PHRs reviewed held any form of certification. All of these findings reinforce the lack of uniformity of standards for PHRs and will help to inform future recommendations for privacy and security requirements for PHRs.

CONSUMER ATTITUDES AND KNOWLEDGE

The authors also reviewed the results of numerous surveys studying consumer understanding and knowledge of PHRs and thoughts about privacy when using PHRs. Section 5 of the paper details the authors' survey findings regarding consumer attitudes and knowledge, which were conducted mainly by non-governmental organizations. The authors reviewed studies that focused specifically on PHR or health information privacy issues as well as some studies which focused on consumers and their thoughts and attitudes toward Internet privacy more generally. The findings were also informed by discussions at the ONC PHR Roundtable and by public comments submitted to ONC in response to questions it posted on its website as part of the PHR Roundtable. Based on a review of these sources, the authors found that a large majority of consumers would like to have the benefits of a PHR. They learned that privacy protections appear to be a key consideration in deciding whether to use a PHR for a similarly large percentage of consumers. Finally, they also learned that the majority of consumers may not have sufficient knowledge to understand and compare privacy policies.

CONCLUSION

This study is intended to inform ONC's preparation of a report to Congress on the privacy and security practices of health entities not covered by the HIPAA Privacy and Security Rules, including PHRs. In identifying the existing privacy and security legal framework for these PHRs and the current gaps in their privacy and security practices, this report aims to provide a foundation for the recommendations that Congress requested relating to the regulation of these specific health entities.

As further detailed below, a review of both the FTC's current enforcement activity on "unfair" and "deceptive" practices imposed upon non-HIPAA PHRs and the requirements that apply to these products under the current HIPAA regulations , demonstrates that neither regulatory regime nor a combination of the two currently provides seamless protection of the privacy and security of information held in non-HIPAA PHRs. The HIPAA regulatory structure sets standards for CEs and BAs. Those rules allow for explicit enforcement of the standards through the assessment of penalties against violators. However, these regulations do not apply to PHRs offered by entities that are not CEs or BAs. The scope of the HIPAA statute would need to be expanded before it could be applied to entities which fall outside of the current definition for CEs and BAs. The FTC's administrative enforcement authority, by contrast, allows for a more flexible approach to assessing violations. However, the FTC's enforcement authority also makes it more difficult to articulate a clear and industry-led set of standards. Regardless of the structure eventually adopted to standardize the privacy and security requirements and practices for PHRs, the comparative merits of the HIPAA and FTC regulatory structures must be carefully analyzed in order to ensure that the resulting approach effectively protects the privacy and security of consumer health information contained in PHRs.

1. INTRODUCTION AND OVERVIEW

In the United States, a wide variety of entities collect, create, maintain, use, and disclose individuals' health information. This information is increasingly automated and exchanged electronically among health care providers, consumers, and others. The automation and exchange of health information has accelerated following the implementation of the HITECH Act in 2009, which was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). The HITECH Act provides for incentive payments for providers to adopt and meaningfully use EHRs.

While health care providers are increasingly using certified EHRs, consumers have increasingly begun to use PHRs. PHRs are emerging as valuable tools which enable consumers to create, monitor, and share health-related data. As PHRs have grown in the marketplace, there has been an increased focus on the need for privacy and security protections for the data that is stored in and shared by PHRs.

A. REPORT BACKGROUND

As part of the HITECH Act, Congress directed the Secretary of the U.S. Department of Health and Human Services to conduct a study and submit a report to Congress on requirements relating to privacy, security, and notification in the case of a breach of security or privacy for non-HIPAA covered entities (i.e., entities that are not subject to HIPAA and its implementing regulations). The following non-covered entities were specifically listed to be a focus of the study: vendors of PHRs; entities that offer products of services through the website of a vendor of PHRs; entities that offer products of services through the website of covered entities that offer individuals PHRs; entities that access information in a PHR or send information to a PHR; and third party service providers used by a vendor or entity to assist in providing PHR products or services.[27] In addition, Congress directed the Secretary to study and make a "determination of which Federal government agency is best equipped to enforce such requirements recommended to be applied to such vendors, entities, and service providers" as listed above, and the timeframe for implementing regulations based on such findings.[28] This paper forms one part of the study and supports the development of the report to Congress.

B. REPORT OVERVIEW

In order to conduct the study, the authors of this paper researched and analyzed the following elements concerning PHRs: general definitions of and characteristics of PHRs; current legislation governing different types of PHRs; privacy and security practices of PHRs; and consumer attitudes toward and knowledge regarding PHRs and privacy. Although this study focused on PHRs that are not subject to HIPAA, it also examined PHRs which are subject to the HIPAA Privacy and Security Rules for comparison purposes. This paper provides a summary of the research and analysis conducted on these various elements concerning PHRs as well as findings and conclusions from the study.

[27] HITECH Act § 13424(b), *see also* Appendix A.
[28] *Id.*

The paper is organized into the following sections:

- Section 1: Introduction and Overview
- Section 2: Defining PHRs and PHR Business Models
- Section 3: Legal Background
- Section 4. Privacy and Security Practices of Non-HIPAA PHRs
- Section 5: Consumer Attitudes and Knowledge Regarding Privacy and PHRs
- Section 6: Report Findings
- Section 7: Conclusion.

2. DEFINING PHRs AND PHR BUSINESS MODELS

To begin the study, the authors examined the definitions of PHRs, the major features and characteristics of PHRs, and the market for PHRs. In order to answer the questions and requests posed by Congress, it is important to have a thorough understanding of the defining characteristics of a PHR, and the market in which PHRs are being used. This will help inform the eventual recommendations on the appropriate agency to make and enforce privacy and security requirements for PHRs.

A. DEFINING PHRS

In the evolving marketplace for health information technology, there is no single definition of a PHR. In general terms, PHRs are repositories of individually identifiable health information collected from a broad range of sources and are used by patients to maintain and manage their health information ideally in a private, secure, and confidential environment.[29] This paper will use the HITECH Act's definition of a PHR as the basis for discussion. The HITECH Act defines a PHR as:

> 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.[30]

Further, the HITECH Act defines "PHR identifiable health information" as individually identifiable health information and includes information that is provided by or on behalf of the individual and that identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[31]

Thus, when examining the HITECH definition of a PHR, it becomes clear that there are a number of key factors that make an electronic record a PHR. First, the record contains identifiable health information, which is broadly defined as information relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual. A PHR may incorporate data drawn from medical devices utilized by the individual, as well as incorporate prescription information, imaging, and test results that the individual may choose to include in the PHR. Therefore, the PHR may contain individually identifiable health information from a broad range of sources.

Second, the record includes identifiable health information created or received by a health care provider or health plan employer. It also includes individually identifiable information that is provided on the behalf of an individual. Information may be entered directly into the PHR by the individual or may be automatically pulled into a PHR from an information source to which the PHR has been connected or tethered – for example, information may be pulled into a PHR from an electronic health record for the individual generated by a health care provider, health plan, employer, or health care clearinghouse.

---

[29] U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology. (n.d.). Retrieved from http://www.healthit.gov/providers-professionals/faqs/what-personal-health-record
[30] HITECH Act § 13400(11).
[31] HITECH Act § 13407(f)(2).

Third, the information in the record must be identifiable, i.e., it must either identify the individual or there must be a reasonable basis to believe that the information can be used to identify the individual.

Fourth, and perhaps most importantly, the electronic record is managed, shared and controlled by or primarily for the individual rather than being managed by and based around the information needs of a particular provider or health plan organization.

B. PHR CHARACTERISTICS

PHRs differ from one another based on two main attributes: the entity that offers the PHR to the consumer, and the sources of data for populating the PHR.

1. Entities that offer PHRs

This study found five major categories of entities that offer PHRs to individuals:

- Healthcare providers
- Health insurance plans
- Non-profit organizations that address health issues
- Employers
- Commercial entities independent of health care organizations

Each type of entity which offers PHRs is discussed in greater detail below.

Healthcare Provider PHRs

Providers may offer patients access to PHRs directly through the provider's organization or through a contracted third party. Some PHRs offered by providers are designed for all patients to use, but others are targeted at specific patient populations to assist them with managing chronic or serious health conditions.

Health Insurance Plan PHRs

Some health insurance plans also offer their beneficiaries access to PHRs. Health insurer PHRs may be provided directly by the health insurance plan or through a contracted service. Similar to PHRs offered by providers, health insurance plan PHRs may be offered to all beneficiaries or to a specific group of members, such as those with chronic conditions. For example, Aetna provides its beneficiaries with a PHR that combines data from claims, pharmacy benefit managers, and beneficiary-entered data to provide disease management advice and health coaching.[32]

Health Related Non-Profit Organization PHRs

PHRs may also be offered by health-related non-profit organizations. For example, the American Heart Association offers a heart health management tool called Heart360. This tool allows consumers to record their heart data online, access information about heart health, and share their results with their providers.[33]

[32] *Id.* at 42-45 (comments of Dr. Gregory Steinberg, President and CEO, Aetna ActiveHealth Management).
[33] Heart360 (n.d.). Retrieved from http://www.heart360.org.

Employer PHRs

Employers may offer PHRs to their employees as a benefit. Some employers offer PHRs to all employees and others focus on employees who frequently use health care services. Often the employer offers the PHR as part of a larger wellness program. In some cases, employers link the PHR to their on-site clinics or on-site fitness centers, where data is fed to the employee's PHR from exercise equipment.[34]

Commercial Organization PHRs

Commercial organizations that do not have a relationship with any health care organization or employer also offer PHRs directly to consumers. For these types of PHRs, the consumer subscribes and generally pays a fee to use the PHR product. Commercial PHR products often can be used on a mobile device such as a smartphone or smart tablet application and allow individuals to carry out a variety of tasks related to their health such as monitor their diets, exercise habits, moods, or fertility.[35] Web-based services that allow consumers to enter health information for their own purposes, but also afford opportunities for networking with others in similar circumstances, can also be considered PHRs.[36]

2. Sources of Data for PHRs

PHRs can obtain data from a number of different sources. Initially, many products that were promoted as PHRs were simply storage vehicles for health information that acted as a flash drive or compact disc for patients to store their own health information. These PHRs have largely (but not entirely) left the market. In place of those older storage vehicles for health information, PHRs now allow users to directly access or download their information from multiple sources and apply interactive functions, such as links to health encyclopedias, receive appointment reminders, and enable individuals to graph or chart their health data over time.[37] This section describes the four most common sources of data that may be used to populate a PHR:

- Health care provider data in EHRs
- Health insurer claims data
- Consumer/patient-entered data
- Device data

PHRs may incorporate any or all of these types of data. A PHR provider may offer options to incorporate data from multiple sources, e.g., a provider-offered PHR may incorporate data from the EHR, patient-entered data, and data from devices.[38]

Health care provider data in EHRs

Some health care providers offer PHRs via portals into their EHRs. In this model, patients can log into the portal, see designated parts or all the information in their EHR, retrieve test results, schedule appointments, and communicate with their providers over secure channels. These patient PHRs are sometimes described

[34] ONC Roundtable, *supra* note 4, at 63-66 (comments of Colin Evans, CEO, Dossia).
[35] *E.g.*, Mobile PHRs. (n.d.). Retrieved from http://www.myphr.com/resources/mobile_phrs.aspx.
[36] *E.g.*, What Can You Do with HealthVault? (n.d.). Retrieved from http://www.healthvault.com/us/en/overview.
[37] *Id*.
[38] *Id.*

as PHRs that are "tethered" to an EHR. The provider may limit and control the functions and options in a tethered PHR.

Patients using non-tethered PHRs may have the option of requesting that data be downloaded from an EHR into an external non-tethered PHR outside of the provider's system. Patients can accomplish this either by authorizing the provider to upload information directly to the PHR or by receiving an electronic copy of the EHR from a provider and uploading the information into the PHR themselves.

Insurer claims data

Insurers are increasingly offering beneficiaries access to PHRs that draw data from the insurer's claims data. These PHRs may provide alert functions, education, and guidance on how the beneficiary can improve his or her health status. As with data from health care provider EHRs, claims data from health insurers may be downloaded directly to a PHR, or beneficiaries may upload an electronic copy of the claims data into their PHR.

Consumer/patient entered data

An increasing number and variety of PHRs allow consumers to enter data directly into their PHR over the Internet or through smart devices. For example, patients may directly enter weight and glucose measurements into their PHR.

Device data

Devices that record patient data may feed information to PHRs. For example, data from a glucometer could be uploaded to a PHR. These data are then incorporated into the PHR record and can be integrated with other data, graphed, and be used as a basis to provide alerts to the patient.

It should be noted that there is a great deal of variation in the function of PHRs across all entities that offer PHRs and across all sources of data for populating PHRs. Some PHRs are capable of performing multiple functions while other are more limited in the scope of functions they can perform. This variation in function will be discussed in greater detail at various points throughout this paper.

C. STATE OF THE PHR MARKET

PHRs have had to change and adapt, and continue to do so, as both the audience which uses PHRs and the methods through which PHRs earn money have evolved. Although some PHR vendors appear to have staying power in the market, others have dropped out or changed their approaches.[39] No major successful business model for PHRs has yet emerged. Although there has been an increase in interest and use of PHRs over the last several years, and "there are certainly organizations that have had success providing patients with access to portions of their health information, [but] in most communities in the United States, actual PHR use is low

[39] Health Data Management. (March 2011). *Study: Promise of PHRs Still Elusive*, HealthData Management. Retrieved from http://www.healthdatamanagement.com/news/study-phr-consumer-ehr-personal-health-record-42110-1.html; *see also* Laxor, (Aug. 27 2011). Retrieved from http://www.laxor.com; Google Health. (Aug. 27, 2011). Retrieved from http://www.google.com/intl/en-US/health/about/; *Dossia Press Releases*, Dossia Consortium, (Aug. 27, 2011). Retrieved from http://www.dossia.org/blog/news.html.

and any potential benefits are limited by the amount of clinical information available electronically."[40] These market conditions and uncertainty affect the structures of the PHRs currently offered.[41]

PHR providers potentially derive revenue from five major sources which are listed below:

- Direct product sales
- Individual subscription fees
- Advertising
- Sale of data
- Grants

Direct product sales

Large PHR vendor's primary business model is to sell their products to health plans, employers, or others interested in managing their overall health care costs. Even if these sales are not themselves profitable, they may attract customers for other services that can be sold on more profitable terms. At the PHR Roundtable, Microsoft HealthVault noted that its PHR was only one of a selection of services it offers to providers and payers.[42] HealthVault is an example of the type of PHR that vendors have developed as part of a suite of health IT products viewed as critical to achieving a market position as an overall leader in health IT.

Individual subscription fees

Subscription fees paid by individual consumers are not a significant revenue source for PHR vendors in today's market. Individual users are not willing to pay for the initial storage-type PHRs, and it does not appear that they are willing to pay for consumer portal or platform models of PHRs—at least not to the extent necessary to sustain them. Even free PHRs have had difficulty attracting users. For example, the PHR demonstration project offered by Medicare in South Carolina attracted approximately 4,000 signups and 3,000 active users, out of a population of over 700,000 Medicare beneficiaries with 100,000 targeted for outreach.[43] Consumers may be willing to pay for some commercial PHRs that allow them to enter their own health data, especially those offered as mobile apps on a smart device. Some more recent entrants into the PHR market are aiming their products toward healthy individuals who are interested in tracking wellness activities, such as exercise or diet. Consumers may be willing to pay a small amount for these services. Some PHR vendors also offer the PHR for free, but charge consumers a fee for obtaining requested medical records.

Advertising

Advertising revenue may also be a major source of revenue for PHR vendors either through use of the PHR to increase traffic on vendor websites or through advertising on the PHR itself. Consumers who use a PHR

---

[40] Computer Sciences Corporation. (2012). *Personal Health Records: A True "Personal Health Record"? Not Really ... Not Yet.* Retrieved from http://s3.amazonaws.com/rdcms-himss/files/production/public/HIMSSorg/Content/files/CSC_PersonalHealthRecords.pdf.

[41] The instability of the PHR market should be an important consideration for any proposed regulatory approach to the privacy and security of PHRs, especially for non-HIPAA PHRs.

[42] ONC Roundtable, *supra* note 4, at 73-74 (comments of George Scriban, Senior Program Manager, Microsoft HealthVault).

[43] Report prepared by the National Opinion Research Center (NORC) for the U.S. Dept. of Health and Human Services, Office of the Secretary, Assistant Secretary for Planning and Evaluation (2010). *Evaluation of the Personal Health Record Pilot for Medicare Fee-For Service Enrollees from South Carolina*, retrieved from http://aspe.hhs.gov/sp/reports/2010/phrpilot/report.pdf.

and then go to the vendor's website to log in, may click through ads, thereby generating revenue for the PHR vendor. Revenue from advertising over the Internet increases based on the amount of consumer traffic and the ability to target ads to specific users based on their profile.

Sale of Data

PHR vendors could potentially sell the information collected in the PHR as part of their business model. None of the participants at the PHR Roundtable use the sale of information in any form as a significant part of their business model. Privacy policies of a number of PHR vendors which are not subject to HIPAA, indicated plans for commercial uses of "aggregate" or "de-identified" data. Such sales are a possible source of future revenue for PHR vendors. Privacy advocates have raised the concern that PHR vendors are gaining revenue from the sale of PHR identifiable information,[44] but this study did not find evidence of this practice presently occurring.

Grants

Grants may also support vendors that design PHRs for individuals with particular health conditions such as diabetes or for at risk populations.[45] Significant PHR development has been funded by grants from organizations, such as the Robert Wood Johnson Foundation, that are interested in improving population health and the quality of health care.[46] As currently structured, grants would not provide long- term sustainable funding for PHRs.

D. CONCLUSION

The features, characteristics, uses, and audience for PHRs continue to change and evolve, and as a result, the definition and business models of PHRs also continue to develop and adapt. This evolution of PHRs should be a factor taken into consideration when making recommendations for privacy and security requirements, as it is likely that such requirements would need some type of flexibility to accommodate future changes in PHRs. Any recommendations for requirements should also take into account the variety of available PHR models to ensure that requirements can appropriately apply to any and all PHRs.

3. LEGAL BACKGROUND

Pursuant to the authority provided in HIPAA, HHS, through its Office for Civil Rights (OCR), implemented and now enforces regulations pertaining to the privacy and security of protected health information. The FTC, pursuant to its statutory authority under the FTC Act, enforces consumer protections against acts or practices that are unfair or deceptive, including, for example, enforcement actions against online entities that fail to

---

[44] *See, e.g.*, Gellman, Robert (2008). *Personal Health Records: Why Many PHRs Threaten Privacy*, the World Privacy Forum. Retrieved from http://www.worldprivacyforum.org/wp-content/uploads/2012/04/WPF_PHR_02_20_2008fs.pdf.

[45] The Robert Wood Johnson Foundation, through Project Health Design, is currently funding development of a PHR for adults with asthma and depression and an iPad touch application for youth in San Francisco with obesity and depression. *Projects*. Retrieved January 19, 2011 from http://www.projecthealthdesign.org/projects. *See also* ONC Roundtable, *supra* note 4 at 134 (comments of Stephen Downs, Assist. Vice Pres., Robert Wood Johnson Foundation). Mr. Downs indicated that Douglas Trauner, CEO of TheCarrot.com, had partnered with one of Project Health Design's current grantees. *Id.* at 135.

[46] Robert Wood Johnson Foundation. (2009). *Project Health Design: Rethinking the Power and Potential of Personal Health Records*. Retrieved from http://www.projecthealthdesign.org/media/file/Round One PHD Final Report6.17.09.pdf. *See also* ONC Roundtable, *supra* note 4 at 134 (comments of Stephen Downs).

comply with their own privacy policies or fail to properly disclose to consumers ways in which their personally identifiable information will be used. Because both HHS and the FTC play active roles in protecting consumer privacy and security and have in place statutory and regulatory frameworks for the protection of consumer privacy and security, it is important to examine the legal framework that each government entity has in place for performing these roles and carrying out its duties with regard to privacy and security. Both HHS and the FTC have a role to play in protecting the privacy and security of information contained in PHRs. PHRs may be regulated under the HIPAA Privacy and Security Rules, the FTC Act's prohibition of unfair or deceptive trade practices, state laws, or a combination thereof. This section provides an overview of the legal requirements and processes in place under HIPAA and its implementing regulations as well as requirements under the FTC Act which would apply to and are currently in place for non-HIPAA PHRs. This overview will help identify areas where non-HIPAA PHRs lack privacy and security requirements, and where current HHS and FTC requirements and processes would fail to adequately protect consumer information contained in non-HIPAA PHRs.

A. HIPAA REGULATION OF PHRS

The HIPAA Privacy Rule applies to a specific defined set of entities, known as covered entities, which are health plans, health care clearinghouses, and those health care providers who transmit any PHI in electronic form in connection with certain standard transactions, such as healthcare claims.[47] The HIPAA Privacy Rule establishes a set of standards for the protection of certain individually identifiable health information, known as protected health information (PHI), which is created or maintained by these covered entities.[48] The Privacy Rule governs how these covered entities may use and disclose an individual's PHI and grants individuals certain rights regarding their health information.[49] The HIPAA Privacy Rule addresses, among other things, requirements for notice to be provided to individuals as to how their PHI may be used and disclosed to others, an individual's right of access to inspect and obtain a copy of PHI about the individual, an individual's right to have a CE amend PHI or a record about the individual, as well as restrictions on the use and disclosure of PHI.

PHRs that are offered directly to individuals by a CE will store and maintain PHI, and are thus subject to the requirements of the Privacy Rule just as the information would be if it were maintained in an EHR or other format.[50] In addition, under the HITECH modifications to HIPAA, vendors who offer PHRs on behalf of the covered entities are considered business associates of CEs and therefore must comply with most of the substantive provisions of the HIPAA Security Rule, as well as the use and disclosure limits of the HIPAA Privacy Rule.[51] The following sections describe the primary provisions of the Privacy and Security Rules that are particularly relevant to PHI stored in a HIPAA-covered PHR.

[47] 45 C.F.R. § 160.103.
[48] 45 C.F.R. § 164.502.
[49] 45 C.F.R. § 164.502.
[50] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Personal Health Records and the HIPAA Privacy Rule*. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.
[51] HITECH Act, § 13404.

HIPAA Privacy Rule

Limits on Uses and Disclosures

The HIPAA Privacy Rule places limitations on the ways CEs and BAs may use or disclose the PHI they maintain. CEs and BAs may use or disclose PHI without needing to obtain the individual's consent in a limited number of situations: when disclosing to the individual; for treatment, payment or health care operations.[52]

Uses and Disclosures that Do Not Require Authorization

Under the Privacy Rule, CEs may generally use or disclose PHI without needing to obtain patient authorization if the PHI is being used for treatment, payment, or health care operations.[53] These uses or disclosures are generally subject to a "minimum necessary" limit if the information is not being shared for treatment purposes.[54] The minimum necessary limitation requires that CEs make a reasonable effort to limit their use and disclosure of PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[55] Thus, if a PHR is offered by a CE, the CE will likely be able to use or disclose PHI in the PHR for treatment, payment, or health care operations without needing to obtain consent from the person whose PHI is contained in the PHR. The ability of a CE to use or disclose PHI contained in a PHR in such a way would likely be of concern to consumers especially due to the fact that a PHR is generally intended to be controlled by and primarily for the benefit and use of the individual.

Use and disclosure of PHI by CEs is also permitted without authorization for certain other purposes. For example, patient authorization is not required for use and disclosure of PHI when it is required by law, such as when a CE is complying with a valid subpoena or criminal investigation, or when a CE is required under state or federal law to report domestic abuse, violence, or neglect to a government authority that is authorized to receive such reports.[56] Disclosure pursuant to a valid subpoena requires that the CE receive satisfactory assurances that reasonable efforts are made to notify the individual whose identifiable health information is in question.[57] A CE may also disclose PHI without authorization to public health authorities for activities such as surveillance, required reports of disease, vital statistics, or workplace safety investigations.[58]

---

[52] 45 C.F.R. § 164.502(a)(1).
[53] 45 C.F.R. § 164.502(a)(1).
[54] 45 C.F.R. § 164.502(b)(1),(2).
[55] *Id.*
[56] 45 C.F.R. § 164.512(a) ,(c),(e). A CE's authorization to disclose PHI in connection with such a report is limited to the extent necessary to comply with the law in question; where the CE is authorized but not required to report abuse, disclosure is allowed only where it is necessary to prevent serious harm to the patient or others, or where the authorized receiver of the report provides certain assurances regarding its necessity. 45 C.F.R. § 164.512(c). State laws vary widely as to the circumstances under which disclosure is required by law. For example, requirements to report suspected child abuse or elder abuse may differ depending on whether the reporting individual is a particular type of professional, and limitations may be placed on reporting information that is in a patient's medical record. *See, e.g.*, California Penal Code § 111657.3; Maryland Code Annotated, Health-General § 4-303; Kansas Statute Annotated § 38-2223. Additional limitations apply to disclosures of DNA, dental records, or analyses of bodily fluids or tissues. 45 C.F.R. § 164.512(f)(2)(ii). Iinformation about crime victims may be disclosed to law enforcement only with the victim's consent, or under special conditions when the victim is incapacitated or the situation is an emergency. 45 C.F.R. § 164.512(f)(3).
[57] 45 C.F.R. § 164.512(e)(1)(ii). This is a particularly important legal protection that is absent from non-covered PHRs.
[58] 45 C.F.R. § 164.512(b)(1)(i) – (ii). The public health entity to which the disclosure is made must be authorized to receive or collect such information. *Id.*

Uses and Disclosures that Require Authorization

The Privacy Rule requires CEs to obtain authorization from an individual for any specific use or disclosure of identifiable health information that is not expressly permitted by the rule.[59] However, the Privacy Rule also specifies particular uses and disclosures that require authorization. For example, CEs cannot use identifiable health information for marketing purposes without authorization, except in very limited circumstances as specified in regulation.[60] The HITECH Act specifically prohibits the sale of identifiable health information without authorization, except for nominal payments for certain public health, research, treatment, and health care operational purposes.[61] The Privacy Rule also generally requires CEs to obtain an authorization for uses and disclosures relating to research, unless a waiver has been approved by an IRB or privacy board, or the disclosure contains a limited set of information and a data use agreement exists with the researcher not to use the information for other purposes.[62] All uses and disclosures made with an authorization are limited to the "minimum necessary" standard.[63] The Privacy Rule stipulates specific standards for obtaining the authorization and special rules for particular purposes.[64] For example, an authorization for research purposes cannot generally allow the researcher to use the information indiscriminately, but must specify the particular study it is to be used for and the study's duration.[65]

Right of Access

The Privacy Rule requires CEs to give individuals access to their health information upon request in the form or format requested by the individual, or a readable hard copy if that form or format is not available.[66] Under the HITECH Act, if a CE uses or maintains electronic designated record sets, the CE must provide patients with an electronic copy of the record set directly to an entity or person designated by the patient (such as a PHR vendor).[67] Thus, in the situation of a PHR offered by a CE, patients may request access to the information maintained by the CE in their HIPAA PHR in a specific electronic form or format, and the CE must provide access in the requested format if it is available to the CE.[68]

---

[59] 45 C.F.R. § 164.508(a)(1). HIPAA also permits a set of uses or disclosures with patient notice and an opportunity to object. These uses or disclosures are those that patients would generally expect and desire in connection with their care, such as inclusion in a directory of patients treated in a health care facility, disclosures to family members or others involved in the patient's care, and authorized public or private disaster relief organizations. 45 C.F.R. § 164.510.

[60] 45 C.F.R. § 164.508(a)(3). The authorization sought must explicit indicate if the marketing involves payments to the CE from a third-party. *Id.*

[61] HITECH Act, § 13405(d).

[62] 45 C.F.R. § 164.512(i).

[63] 45 C.F.R. § 164.502(b).

[64] 45 C.F.R. § 164.508.

[65] 45 C.F.R. § 164.512(i). The use of health information in research has been an area of particular confusion and controversy. *See* Institute of Medicine. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Washington, DC: The National Academies Press, 2009. For use of identifiable health information in research, the Privacy Rule requires either an authorization or approval of a waiver by an Institutional Review Board or a special privacy board. Waivers require a finding that the research will not adversely affect the subjects' rights or welfare, the identifiable health information is required to carry out the research, and consent would be impracticable. 45 C.F.R. § 46.116(c) – (d); 45 C.F.R. § 164.512(i)(2).

[66] 45 C.F.R. § 164.524(c)(2).

[67] HITECH Act, § 13405(e)(1).

[68] *Id.* The CE may charge a fee for providing its patients with access to their data, although the fee must not be greater than the labor cost of providing that access; HITECH Act § 13405(e)(2).

Right to Amend

The Privacy Rule requires CEs to allow individuals to request an amendment to their health information held by the CEs.[69] CEs may deny the request for several reasons, including a determination that the record is accurate and complete without the amendment.[70] However, if the CE denies the request, the individual may submit a written statement of disagreement to be included with the record upon future disclosure.[71] PHRs subject to HIPAA must follow these protocols for data in the PHR created or maintained by the CE.[72]

Notice of Privacy Practices

The Privacy Rule requires that in certain circumstances, CEs must provide patients with a HIPAA notice of privacy practices.[73] The rule places specific requirements on what this notice must contain, including a description (with examples) of how the CE may use and disclose health information, both with an individual's authorization and without the individual's authorization.[74] The notice must include the individual's rights with respect to the health information maintained by the CE including the right to access and request corrections.[75] It must include notice of the individual's right to file a privacy complaint, either with the CE or with the Secretary of HHS, if the individual believes that his or her privacy rights have been violated, as well as instructions for how an individual may file a complaint with the CE. The notice must also provide a point of contact through which the individual can obtain additional information on the CE's privacy practices.[76] If the CE intends to implement changes to its notice before issuing a revised notice, it also must describe the process that the CE will use to notify individuals of changes to the privacy practices listed in the notice.[77] If a CE is providing a PHR, the CE has some flexibility in deciding whether to create a separate notice for its PHR or whether to simply apply its institutional notice to the information contained in the PHR.[78] Either way, the CE must provide individuals a notice that details the privacy practices that apply to the PHR. It should be noted that the Privacy Rule only imposes the requirement to provide a notice of privacy practices on a CE, and does not impose such a requirement on a BA.

Treatment of Business Associates under the HIPAA Privacy Rule

A CE may disclose PHI to a BA, and may allow a BA to create, receive, maintain, or transmit PHI on its behalf only once the CE has received appropriate assurances that the BA will appropriately safeguard the PHI;. These assurances must take the form of a written contract or business associate agreement between those entities.[79] A business associate agreement must lay out the uses and disclosures of PHI that the BA is authorized to

---

[69] 45 C.F.R. § 164.526(a)(1).
[70] 45 C.F.R. § 164.526(a)(2).
[71] 45 C.F.R. § 164.526(d).
[72] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Personal Health Records and the HIPAA Privacy Rule*. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.
[73] 45 C.F.R. §§ 164.520, 164.502(i). Model Notices of Privacy Practices are available from the U.S. Department of Health and Human Services website: http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html.
[74] 45 C.F.R. § 164.520(b)(1)(ii).
[75] 45 C.F.R. § 164.520(b)(1)(iv).
[76] 45 C.F.R. § 164.520(b)(1)(vi) – (vii).
[77] 45 C.F.R. § 164.520(b)(1)(v)(C).
[78] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Personal Health Records and the HIPAA Privacy Rule*. Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf.
[79] 45 C.F.R. § 164.502(e).

perform, must require the BA to report to the CE any unauthorized uses or disclosures, and must require that the same restrictions apply to any subcontractor of the BA that creates, receives, maintains, or transmits PHI.[80] A BA is subject to the same restrictions on use and disclosure as is a CE, except that, if authorized under its business associate agreement, the BA may use or disclose PHI for its own management or administration purposes or to provide data aggregation services related to the operations of the CE with which it has formed the agreement.[81] A valid business associate agreement is subject to termination by the CE if the BA is determined to have violated a material term of the contract.[82]

HIPAA Security Rule

The HIPAA Security Rule applies to all PHI electronically maintained or transmitted by CEs.[83] The HIPAA Security Rule establishes administrative, technical, and physical standards, and implementation specifications for ensuring that PHI is kept secure and aims to protect the availability, integrity and confidentiality of health information.[84] Under the HIPAA statute, Congress instructed HHS that security standards should take into account technical capabilities, costs, and the needs and capabilities of small and rural providers.[85] As a result, the Security Rule is designed to allow CEs to tailor implementation of security standards to their unique circumstances, and to take advantage of new technological developments.[86] The Security Rule is therefore structured with both required and addressable implementation specifications. If a standard includes addressable implementation specifications, a CE or BA must determine whether the implementation specification is a reasonable and appropriate safeguard in its environment.[87] If the CE or BA determines that the addressable implementation specification is reasonable or appropriate, it must implement the implementation specification. If the CE or BA determines that the implementation specification is not reasonable or appropriate, it must "document why it would not be reasonable and appropriate to implement the implementation specification and it must implement an equivalent alternative measure if reasonable and appropriate."[88]

The Security Rule specifies that a CE must have security management process in place which includes policies and procedures "to prevent, detect, contain, and correct security violations."[89] The implementation specifications for the security management process standard require an "accurate and thorough assessment of risks and vulnerabilities" to PHI held by CEs, known as a risk analysis.[90] The security management process standard also includes the requirement to implement security measures designed to reduce the risks and

[80] 45 C.F.R. § 164.504(e)(2).
[81] 45 C.F.R. § 164.504(e)(2)(i).
[82] 45 C.F.R. § 164.504(e)(2)(iii).
[83] 45 C.F.R. § 164.302. The HITECH Act applies the administrative, physical, and technical safeguards of the Security Rule directly to BAs. HITECH Act § 13401. The requirements of the HIPAA Security Rule do not apply to non-HIPAA PHRs or their associated entities, although some commentators have suggested that they are a good fit. *See* Center for Democracy and Technology. (2010). *Comments of the Center for Democracy & Technology to the Office of the National Coordinator Roundtable,* pg. 8. Retrieved from http://www.cdt.org/files/pdfs/CDT_Comment_to_ONC_PHR_Roundtable.pdf.
[84] 45 C.F.R. §§ 164.306, 164.308, 164.310, 164.312.
[85] 42 U.S.C. § 1320d-2(d)(1)(A).
[86] 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).
[87] 45 C.F.R. § 164.306(d)(3)(i).
[88] 45 C.F.R. § 164.306(d)(3)(ii).
[89] 45 C.F.R. § 164.308(a)(1)(i).
[90] 45 C.F.R. § 164.308(a)(1)(ii)(A).

vulnerabilities identified in the risk analysis to a "reasonable and appropriate" level,[91] and sanctions against workforce members who fail to act in accordance with security policies.[92] Administrative requirements also include implementing procedures to review system activity, such as audit logs, access reports, and incident tracking, as well as implementing workforce training activities, such as instruction concerning secure passwords.[93] CEs and BAs must also develop a contingency plan for responding to incidents, such as natural disasters that could damage electronic health information.[94]

Physical safeguards in the Security Rule include the implementation of policies and procedures to ensure appropriate access to areas with facilities and workstations that house identifiable health information.[95] These restrictions protect data against tampering or theft.[96] CEs and BAs must also create policies and procedures that govern access to portable electronic hardware and media that house PHI, such as laptops and mobile phones, and if applicable, their movement within or outside of a CE or BA facility.[97]

The technical safeguards in the Security Rule include access controls.[98] Required access controls include the assignment of unique user identification and a procedure for emergency access to electronic health information.[99] Addressable controls include automatic logoff after a period of inactivity, and the encryption and decryption of electronic identifiable health information while at rest.[100] The Security Rule also requires audit controls that record and examine access and other activity in information systems that contain or use electronic identifiable health information.[101] The data integrity standard requires that CEs and BAs take steps to ensure that data is not improperly altered or destroyed.[102] Entities must also have authentication procedures in place to ensure that unique user identifications are not abused to gain access to electronic PHI.[103] Finally, entities need to consider transmission security by ensuring that electronic identifiable health information transmitted over an electronic network is safe from unauthorized access.[104] HHS does not require specific encryption technologies to implement this safeguard, leaving CEs to determine the best solutions for their needs and capabilities.[105]

Breach Notification Rule for HIPAA Covered Entities

The HITECH Act requires CEs to notify affected individuals of the possibility of unauthorized access, acquisition, use, or disclosure of their identifiable health information under breach notification rules issued by HHS.[106] An example of such a breach is the loss of a laptop containing unencrypted health information. The HIPAA breach

[91] 45 C.F.R. § 164.308(a)(1)(ii)(B).
[92] 45 C.F.R. § 164.308(a)(1)(ii)(C).
[93] 45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5).
[94] 45 C.F.R. § 164.308(a)(7).
[95] 45 C.F.R. § 164.310(a)(1).
[96] 45 C.F.R. § 164.310(a)(2)(ii).
[97] 45 C.F.R. § 164.310(d)(1).
[98] 45 C.F.R. § 164.312(a)(1).
[99] 45 C.F.R. § 164.312(a)(2)(i) – (ii).
[100] 45 C.F.R. § 164.312(a)(2)(iii) – (iv).
[101] 45 C.F.R. § 164.312(b).
[102] 45 C.F.R. § 164.312(c).
[103] 45 C.F.R. § 164.312(d).
[104] 45 C.F.R. § 164.312(e).
[105] 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).
[106] HITECH Act, § 13402(a); 45 C.F.R. §164.404(a).

notification rules apply as of the first day when the CE discovers, or with reasonable diligence should have discovered, the possibility of unauthorized acquisition, access, use, or disclosure of unsecured identifiable health information.[107] The CE is required to notify local media if over 500 individuals in a State or jurisdiction are affected by the breach.[108] All breaches must be reported to the Secretary of HHS.[109] In comparison, breach notification regulations were implemented in 2009 for non-HIPAA PHRs. These regulations will be discussed in more detail later in this section, but they do contain many similarities to the requirements in the HIPAA Breach Notification Rule.

HIPAA Enforcement

HHS' Office for Civil Rights investigates complaints of HIPAA violations and conducts compliance audits.[110] The HITECH Act strengthened the Secretary's ability to enforce HIPAA and impose penalties.[111] HHS' Administrative Simplification Enforcement Rule, amended in response to the HITECH Act provisions, reflects HHS' enhanced enforcement capabilities through categories of violations that reflect increasing levels of culpability with an increased maximum dollar cap of $1.5 million per violation for violations occurring on or after February 18, 2009.[112] Penalty determinations are based in part on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.[113]

HIPAA also allows for enforcement through criminal prosecution. A person who knowingly obtains or discloses PHI in violation of HIPAA, faces a fine of up to $50,000 and a prison term of up to one year.[114] For violations committed under false pretenses, this penalty may rise to a fine of up to $100,000 and a prison term of up to five years.[115] For violations with intent to use, sell, or transfer individually identifiable health information for commercial gain, personal gain, or malicious harm, penalties may include a maximum fine of $250,000 and a prison term of up to 10 years.[116] HHS refers criminal violations for prosecution in federal court to the U.S. Attorney's office.[117]

The HITECH Act also authorizes state attorneys general to bring civil actions on behalf of residents of their states that the attorney general believes were adversely affected by HIPAA violations.[118] The state must give

---

[107] 45 C.F.R. § 164.404(a).
[108] HITECH Act § 13402(e)(2); 45 C.F.R. § 164.406(a).
[109] HITECH Act § 13402(e)(3); 45 C.F.R. § 164.408(a). Breaches involving 500 or more individuals must be reported to the Secretary via the Office for Civil Rights without unreasonable delay and in no case later than 60 days after discovery of the breach. Breaches involving less than 500 individuals must be reported no later than 60 calendar days after the end of the calendar year in which the breach was discovered. 45 C.F.R. § 164.408(b), (c).
[110] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.) *Enforcement Process*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html; 45 C.F.R. §§ 160.306, 160.308.
[111] HITECH Act, § 13410.
[112] 45 C.F.R. §160.404.
[113] 45 C.F.R. §160.408.
[114] 42 U.S.C. § 1320d-6.
[115] *Id.*
[116] *Id.*
[117] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.) *How OCR Enforces the HIPAA Privacy & Security Rules*. Retrieved December 11, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html.
[118] HITECH Act § 13410(e).

notice to the Secretary of HHS, and may not bring an action when an action by the Secretary is pending.[119] Enforcement actions by state attorneys general have more limited remedies: states may seek injunctive relief or levy civil penalties of up to $100 per violation, to a maximum of $25,000.[120] Courts also have discretion to award attorneys' fees to the state.[121]

While federal HIPAA rules do not create a private right of action for individuals to assert their rights under HIPAA, HIPAA does not preempt state laws that are not inconsistent with its terms. A private right of action may be created either under state statutory or common law.[122] HITECH mandates the establishment of a methodology to distribute a portion of civil monetary penalties or settlements collected to the individuals harmed by HIPAA violations, though this section has not yet been put into effect.[123]

HIPAA enforcement allows for informal settlement of noncompliance investigations, through means such as a corrective action plan or demonstrated compliance.[124] In more serious cases, HHS and the CE will enter into a contractual resolution agreement, generally for a period of three years.[125] Resolution agreements typically also involve payment of a monetary resolution amount.[126] Because non-HIPAA PHRs are not subject to any uniform regulatory requirements, no schema exists for which there would be enforcement which would be analogous to the HIPAA enforcement process.

Summary

In summary, HIPAA provides for a number of different requirements to protect individuals' PHI and to ensure that individuals are granted certain rights regarding their information. Entities that offer PHRs and are CEs or BAs are subject to HIPAA and its implementing regulations as described above. However, for entities that offer PHRs but are not CEs or BAs, these requirements do not apply, as discussed below.

HIPAA sets forth specific instances in which a use or disclosure of PHI does not require authorization, specifically in situations in which the PHI is being used for treatment, payment, or health care operations. For entities that offer PHRs but are not CEs, the explicit ability to disclose PHI for treatment, payment, or health care operations without needing to authorization does not exist. However, such PHRs are not subject to any uniform standard or regulation that does limit the uses or disclosures that the non-HIPAA covered PHR can make with the individual's PHI, thereby allowing such a PHR to make any number of uses or disclosures without being required to obtain authorization from the consumer.

The Privacy Rule requires CEs to obtain authorization from an individual for any specific use or disclosure of identifiable health information that is not expressly permitted by the rule. However, for entities that offer

---

[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *R.K. v. St. Mary's Med. Ctr*., 735 S.E.2d 715, 719, 724 (2012).
[123] HITECH Act § 13410(c)(3). To date no rule has been promulgated under this provision.
[124] 45 C.F.R. § 160.312(a).
[125] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *Case Examples and Resolution Agreements*. Retrieved December 11, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.
[126] *Id.*

PHRs but are not CEs, such regulatory requirements of when authorization must be obtained for a use or disclosure do not exist.

The Privacy Rule requires CEs to give individuals access to their health information upon request in the form requested by the individual or a readable hard copy if that form or format is not available. In the situation of a PHR offered by an entity that is not a CE, there would not be a requirement for the entity to provide access to the individual. However, this lack of regulation or right of access is not of great concern, given the fact that PHRs should ultimately be controlled by and for the benefit of the individual. The individual should have access to all the information in his or her PHR, regardless of the entity providing the PHR.

The Privacy Rule requires CEs to allow individuals to request an amendment to their health information held by the CEs. For entities that offer PHRs but are not CEs, such requirements to allow an individual to request an amendment to the information in the PHR do not exist. Such PHR vendors would not be required to consider amending information in the PHR if the consumer requested it. However, if an individual were able to acquire records with the correct information, such as from his or her health care provider, he or she may be able to add the record with the correct information to the PHR and note that such record contains the correct information.

The Privacy Rule requires that CEs in certain circumstances provide patients with a HIPAA notice of privacy practices. However for entities that offer PHRs but are not CEs, such a requirement to provide a notice of privacy practices does not exist.

A CE may disclose PHI to a BA, and may allow a BA to create, receive, maintain, or transmit PHI on its behalf only once the CE has received appropriate assurances that the BA will appropriately safeguard the PHI. These assurances must take the form of a written contract or business associate agreement between those entities. For entities that offer PHRs but are not CEs, the requirement to enter into an agreement with other entities prior to maintaining or transmitting information on behalf of the non-HIPAA PHR does not exist. There are no assurances or requirements in place between the parties sharing data that will ensure that the sending and receiving entities will adequately protect the transmitted information.

Finally, the HIPAA Security Rule establishes administrative, technical, and physical standards and implementation specifications for ensuring that PHI is kept secure and aims to protect the availability, integrity and confidentiality of health information. In comparison to the detailed administrative, physical, and technical standards and implementation specifications required by the Security Rule, no such security requirements are imposed on non-HIPAA PHRs.

B. FEDERAL TRADE COMMISSION JURISDICTION

This section outlines some key aspects of the FTC's authority that may be relevant with respect to PHRs. The section outlines the FTC's authority with respect to non-HIPAA covered PHRs as well as breach notification requirements under HITECH.[127]

[127] HITECH Act § 13407(a)–(b).

Section 5 of the Federal Trade Commission Act grants the FTC the authority to prevent persons, partnerships, or corporations, subject to some exceptions defined in section 5 of the FTC Act, from using, "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[128] One of the FTC's primary missions is to prevent business practices that are unfair or deceptive to consumers.[129] Unless otherwise preempted, this authority to prevent business practices that are unfair or deceptive to consumers, would extend to privacy and security policies and practices of Internet-based information technology companies that offer PHRs, when their policies and practices could be viewed as unfair or deceptive.

FTC has a limited ability to promulgate formal regulations related to its section 5 authorities. As a result, FTC has not adopted a specific set of privacy and security regulations. Instead, it relies upon its enforcement authority to establish, on a case-by-case basis, a general standard for the practices it considers to be "unfair" or "deceptive." A review of these cases demonstrates that the FTC uses its section 5 authorities to enforce a broad standard for privacy and security of consumer information held by businesses operating over the Internet.

Pursuant to its stated mission of preventing business practices that are unfair or deceptive to consumers, the FTC has expressed a great deal of interest in questions surrounding protection of consumer privacy. In 2010, the FTC issued a preliminary staff report which outlined the FTC's history of promoting consumer privacy through enforcement and policy work, as well as proposed a framework for companies to adopt to protect consumer privacy.[130] Following the issuance of the preliminary report, the FTC received over 450 comments from the public from a wide range of stakeholders. These comments expressed a broad range of viewpoints, from support of the proposed framework, to criticism of the slow pace of self-regulation and a desire for Congress to enact privacy legislation.[131] In December 2012, the FTC issued a final Report where it set forth a final privacy framework of best practices for companies that collect and use consumer data. The final Report was based on an analysis of all the public comments received in response to the preliminary 2010 report as well as developments that occurred in between the issuance of the first report and the final Report.[132] The content of the final FTC Report can serve as a useful tool for making recommendations on potential privacy policies and regulations for PHRs.

The FTC Act: Unfair and Deceptive Trade Practices

Section 5 of the FTC Act describes "unfair" acts or practices as follows: "the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[133] Thus in order to find a

[128] 15 U.S.C. § 45(a)(1)–(2).
[129] *About the Federal Trade Commission*. (n.d.).Retrieved from http://www.ftc.gov/ftc/about.shtm.
[130] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers* (2012). Retrieved from http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[131] *Id.*
[132] *Id.*
[133] Federal Trade Commission. (December 17, 1980). *FTC Policy Statement on Unfairness*, Appended to International Harvester Co., 104 F.T.C. 949, 1070 (1984). Washington, DC: Federal Trade Commission. Retrieved from http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

practice unfair, the Commission must evaluate the injury or harm that the practice has caused or may cause to consumers. The FTC has determined that the harm must in most cases be monetary or involve a health or safety risk.[134] However, as explained in this section, it will consider emotional harms when deciding to exercise its authority. In addition, the FTC Act gives the FTC discretion in evaluating the fairness of a business practice: "In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination."[135]

Although there is no specific definition in statute or regulation for what constitutes a "deceptive act or practice," the 1983 FTC Policy Statement on Deception states that "numerous Commission and judicial decisions have defined and elaborated on the phrase 'deceptive acts or practices' under both Sections 5 and 12."[136] In addition, the 1983 FTC Policy Statement on Deception summarizes the Commission's view of deceptive acts or practices and states that, "the Commission will find deception if there is a representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[137] The Act does not require the Commission to find that the person or corporation intended to deceive the consumer or that any consumer was actually deceived, in order to find an act or practice deceptive.[138]

Thus, the authority to prevent "unfair" or "deceptive" acts or practices creates two categories of actions or practices through which an entity may be subject to penalty.[139] A more detailed discussion and examination of administrative actions that the FTC has taken to enforce its authority to prevent unfair or deceptive trade practices follows later in this section. In addition, applicability of these FTC administrative actions to non-HIPAA PHRs will be discussed in those sections as well. First, however, a brief summary of FTC's investigative and enforcement authority will be provided in order to give the reader more detailed context about FTC authority.

FTC Investigative and Enforcement Authority

In carrying out its mission with respect to preventing unfair and deceptive practices, the FTC relies on specific types of authority granted by statute. The FTC's statutory authority to prevent unfair methods of competition and unfair or deceptive acts or practices affecting commerce can be divided into two main categories: investigative and enforcement authorities.

Investigative Authority

The FTC may rely on investigative powers to examine potential unfair or deceptive practices. Under section 20 of the FTC Act, only "civil investigative demands" (CIDs) may be used to investigate possible unfair or deceptive

[134] *Id.*
[135] 15 U.S.C. § 45(n).
[136] Federal Trade Commission. (October 14, 1983). *FTC Policy Statement on Deception*, Appended to Cliffdale Associates, Inc., 103 F.T.C. 110, 174 (1984). Washington, DC: Federal Trade Commission. Retrieved from .
[137] *Id.*
[138] FTC v. Verity Int'l Ltd., 443 F.3d 48, 63 (2d Cir. 2006).
[139] *See generally* Jeff Sovern, *Protecting Privacy With Deceptive Trade Practices Legislation*, 69 FORDHAM L REV. 1305, 1320, 1326–1339 (2009).

practices.[140] The scope of a CID is broader than a subpoena, with the CID capable of being used to obtain existing documents or testimony as well as to require filing of written reports or answers to questions.[141] Section 20 of the FTC Act also allows service of CIDs to entities not within the territorial jurisdiction of the United States.[142] Further, section 6 of the FTC Act provides another investigative tool and allows the FTC to require the filing of "annual or special . . . reports or answers in writing to specific questions" to obtain information about the business operations and practices of entities to whom the request is directed.[143]

It is important to note that the FTC does not investigate every complaint it receives related to unfair or deceptive practices. Instead, as described in the standard letter issued in response to the FTC receiving a complaint,

> The Commission can . . . act when it sees a pattern of possible violations developing. The decision to open up an investigative action depends on how widespread the practice is, how many consumers are hurt, how much harm is done and how much evidence we have. We must also determine how much staff and effort we can put into each case and we must concentrate on the most urgent problems.[144]

This triaging of complaints and resources stands in contrast to the procedures of the HHS Office for Civil Rights, which investigates every HIPAA complaint that fulfills a preliminary review.[145] In addition, while HIPAA regulations are oriented toward the notion that privacy and security of PHI are a per se right of individual health care consumers, FTC enforcement actions must be able to demonstrate that a cited violation of the privacy or security of a consumer's information was either "unfair" and resulted in substantial injury which was unavoidable, or was "deceptive" and misled the consumer to the consumer's detriment. As the FTC itself describes, "[t]he Commission is not concerned with trivial or merely speculative harms," and typically focuses on violations resulting in monetary harm.[146] Thus, with respect to PHRs, the FTC would most likely take action and investigate if it were to learn of numerous complaints about a particular PHR vendor or numerous similar complaints of unfair or deceptive practices by multiple PHR vendors, where consumers have been harmed in some way by the suspected unfair or deceptive practices of the PHR vendor(s).

Enforcement Authority

Following an investigation, in instances where there is "reason to believe" the law is being or has been violated, the FTC may initiate an enforcement action, generally either via administrative adjudication or judicial enforcement.[147] There are two basic types of administrative enforcement, adjudication and rulemaking, both of which will be discussed below.

---

[140] 15 U.S.C. § 57b-1.
[141] 15 U.S.C. § 57b-1(c)(1).
[142] 15 U.S.C. § 57b-1(c)(7)(B).
[143] 15 U.S.C. § 46(b).
[144] Letter from the F.T.C. Consumer Response Center to Michael Carome, (Sept. 21, 2012), Retrieved from http://www.citizen.org/documents/2069_ftc_letter.pdf.
[145] U.S. Department of Health and Human Services, Office for Civil Rights. (n.d.). *How OCR Enforces the HIPAA Privacy & Security Rules*. Retrieved December 11, 2012 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/howocrenforces.html.
[146] *FTC Policy Statement on Unfairness*, *supra*.
[147] 15 U.S.C. § 45(b).

1. Administrative enforcement: adjudication

Administrative enforcement involves the issuance of a complaint by the FTC, which a respondent can settle without admitting liability, by signing a consent agreement to be placed on the record for thirty days for public comment before becoming a final order.[148] Such final orders often require the respondent to make adjustments to its practices.

Alternatively the respondent can contest the charges in a complaint, leading to a trial-type proceeding before an administrative law judge, which results in an ALJ issuing an initial decision. This initial decision can be appealed to the full Commission by either party and then to any court of appeals.[149] Once a Commission order becomes final, which occurs sixty days after it is served, the FTC can seek civil penalties for instances where the order is violated by the respondent.[150] In such a situation, the Commission would bring suit in a District Court to enforce the Commission's order, and the District Court would assess the penalty.[151] In addition, the Commission may seek civil penalties against non-respondents once the Commission has determined in a litigated administrative adjudicatory proceeding that a practice is unfair or deceptive, and has issued a final cease and desist order. In order to seek civil penalties in this type of situation, "the Commission must show that the violator had 'actual knowledge that such act or practice is unfair or deceptive and unlawful' under section 5(a)(1) of the FTC Act."[152] The Commission would generally show that it had given the non-respondent violator a copy or summary of the Commission's determination in question in order to prove such actual knowledge on the part of the violator.[153] Most consumer protection enforcement is conducted directly in court through judicial enforcement, discussed below, rather than through administrative enforcement.

2. Administrative enforcement: rulemaking

If there is an unfair or deceptive practice occurring on an industry-wide basis, the FTC may use its authority to promulgate regulations instead of carrying out administrative adjudications against individual respondents. However, the FTC must use the procedures outlined in Section 18 of the FTC Act (Magnuson-Moss rulemaking procedures) rather than the typical government-wide notice and comment rulemaking procedures under Section 553 of the Administrative Procedures Act (APA).[154] The Magnuson-Moss procedures are more burdensome than informal rulemaking under the APA. Prior to beginning the rulemaking process, the FTC must define the conduct that it wishes to prohibit "with specificity," and must establish that it has reason to believe that the addressed practice is "prevalent" within the industry it is seeking to regulate.[155] The FTC may then initiate rulemaking by publishing an advance notice of proposed rulemaking and seeking public comment before publishing a notice of proposed rulemaking. During the rulemaking process the FTC must also provide

[148] *Brief Overview*, *supra*.
[149] *Brief Overview*, *supra*.
[150] 15 U.S.C. § 45(l).
[151] *Brief Overview, supra.*
[152] *Id.*
[153] *Id.*
[154] 15 U.S.C. § 57a.
[155] 15 U.S.C. § 57a.

opportunity for a hearing at which interested parties are given cross-examination rights.[156] Where there are numerous interested parties, the FTC must determine which parties have similar interests, group them, and have each group choose a representative for those interests in the cross-examination process.[157] These procedures are complicated and time-consuming, typically taking three to ten years to complete.[158] As a result of its complex and time-consuming rulemaking capability, the FTC has not promulgated a prescriptive set of required privacy and security practices for consumer-facing websites generally, or for PHRs specifically.

If the Commission does promulgate a regulation, however, "anyone who violates the rule 'with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule' is liable for civil penalties of up to $11,000 per violation."[159] Additionally, any person who violates a regulation, regardless of the state of knowledge, is liable for injury caused to consumers by the regulation violation, and the Commission "may pursue such recovery in a suit for consumer redress under Section 19 of the FTC Act, 15 U.S.C. Sec. 57b."[160]

Judicial Enforcement

Judicial enforcement, meanwhile, involves the FTC challenging unfair or deceptive activities in court directly, without first going through an administrative adjudication finding that the conduct is unlawful. Section 13(b) of the FTC Act authorizes the FTC to seek either a preliminary or permanent injunction to remedy "any provision of law enforced by the FTC" whenever the FTC has "reason to believe" that the law is being or is about to be violated.[161] Such judicial injunctions enable swifter enforcement, and become effective immediately pending the completion of an administrative determination as to whether the cited conduct violates section 5. This is in contrast with final orders from administrative adjudications described above, which do not take effect until 60 days after service.[162] The Commission's use of its permanent injunction authority increased during the 1980s, when the Commission "began to make widespread use of the permanent injunction proviso of Section 13(b) in its consumer protection program to challenge cases of basic consumer fraud and deception."[163] The FTC's section 13(b) authority is currently the primary mechanism by which it conducts enforcement under its consumer protection authority, including its authority against "unfair" and "deceptive" practices.[164] While judicial enforcement has become the FTC's favored mechanism for consumer protection actions, administrative proceedings do still offer important advantages. In administrative actions, the FTC is entitled to significant deference because the proceedings place the Commission in the role of interpreting its own statute and other applicable laws. A court, when reviewing an FTC's factual findings and legal standard, must uphold the FTC's findings of fact where the court finds that the findings of fact are supported by substantial evidence.[165] However, in a 13(b) suit, "the Commission receives no greater deference

[156] 15 U.S.C. § 57a(b)-(c).
[157] 15 U.S.C. § 57a(c)(4).
[158] Prepared Statement of the Federal Trade Commission on *Consumer Protection and the Credit Crisis* Before the Senate Committee on Commerce, Science, and Transportation. 111th Cong. 1 (2009). Retrieved from http://www.ftc.gov/os/2009/02/P084800creditcrisis.pdf.
[159] *Brief Overview, supra*, citing to 28 U.S.C. §2461.
[160] *Brief Overview, supra.*
[161] 15 U.S.C. § 53(b).
[162] *Brief Overview*, *supra*.
[163] *Id*.
[164] *Id.*
[165] *Id.*

than would any government plaintiff. Thus, where a case involves novel legal issues or fact patterns, the Commission has tended to prefer administrative adjudication."[166]

FTC Administrative Actions

This section will provide a summary of administrative actions that the FTC has taken to enforce its authority to prevent unfair or deceptive trade practices. A review of these enforcement actions is instructive in identifying some of the types of activities (or failures to act) that could be considered factors in determining whether a company offering a PHR service over the Internet has engaged in "unfair or deceptive acts or practices" in violation of the FTC Act. The actions reviewed below are separated into those focusing on "unfair" acts and those focusing on "deceptive" acts with respect to privacy and to security.

Administrative Actions for Deceptive Trade Practices: Privacy

The FTC has considered several acts and practices that may contribute to establishing a reason to believe that a company's actions are "deceptive" under section 5 of the FTC Act. First, several FTC enforcement actions involve companies that obtain identifiable user information over the Internet and fail to follow their own stated privacy policies in handling the information they collect.[167] In these cases, the FTC alleged that the representations made by these companies actively misled consumers as to how their personal information would be used;. Therefore, the companies' uses or disclosures of the information in direct conflict with the policy were alleged to be material to the consumer and deceptive.[168] For example, a significant factor in one FTC enforcement action was the attempted sale of customer information, including children's demographic information, in contravention of promises made in a privacy policy not to share the information with third parties.[169] In another complaint, the FTC alleged that Google's statements in its privacy policy that consumers could "opt-out" from being tracked within the Apple Safari browser were deceptive when Google actually collected information about consumer's browsing habits even if they had opted out.[170]

Similarly, the FTC has undertaken enforcement action for "deceptive" practices when a company misrepresents the extent to which it is a member of, adheres to, or complies with a privacy compliance program sponsored by the government or another entity. For example, Google stated in its privacy policy that it is a member of the National Advertising Initiative (NAI) and adheres to its Self-Regulatory Code of Conduct, which requires a conspicuous notice that describes the types of behavioral data it collects.[171] However, when Google incorrectly informed consumers that data would not be collected from users of the Apple Safari browser with certain applied settings, it also violated the NAI code of conduct. As a result, the FTC alleged that Google had engaged in a deceptive practice for its collection of information from the Safari browser on this second basis.[172]

The FTC has also filed complaints alleging deception when the practices do not involve the direct contradiction of statements in the privacy policies, but rather a failure to adequately disclose to consumers how their

[166] *Id.*
[167] FTC v. Toysmart.com, LLC and Toysmart.com, Inc. F.T.C. File No. X000075 (July 21, 2000) (available at http://www.ftc.gov/os/caselist/x000075.shtm); Google Inc., F.T.C. File No. 102-3136 (Oct. 13, 2011) (available at http://www.ftc.gov/os/caselist/1023136/111024googlebuzzcmpt.pdf).
[168] *Id.*
[169] Toysmart.com, *supra.*
[170] Google Inc., F.T.C. File No. 102-3136 (Aug, 8, 2012) (available at http://www.ftc.gov/os/caselist/c4336/index.shtm).
[171] *Id.*
[172] *Id.*

information will be collected and used. The FTC alleges that these practices can be deceptive when the omission or misrepresentation of the disclosure misleads the consumer into unwillingly sharing personal information for unanticipated and potentially harmful purposes. For example, the FTC alleged that Echometrix, a company that sold Internet parental monitoring software, was engaging in deceptive practices when it used the monitoring software to gather and sell information about children's browsing habits to third parties.[173] The FTC alleged that Echometrix had only made vague representations about this use of the information inconspicuously in its End User License Agreement, which was inappropriate because selling children's information would affect their parents' willingness to use the product.[174] In another complaint, the FTC alleged that Sears was engaging in a deceptive practice when it invited consumers to be part of an online community to give feedback to retailers without adequately informing them that by joining the community, an application would be installed on their computers that would track all of their Internet activities.[175] The FTC noted in its complaint that Sears collected information, including financial and health information, entered by consumers onto secure websites outside of the Sears website, making it particularly invasive to consumer privacy and material to the consumer's decision to participate in the online community.[176]

Overall, the FTC has emphasized, through its enforcement actions, the importance of companies following their stated privacy policies and adhering to company compliance programs. It has also shown that it believes websites must adequately describe the type and amount of disclosure of personal information that would be material to the consumer in selecting to use the product or service. These actions and decisions have implications for PHRs, as the FTC would likely hold PHRs that have a privacy policy to a similar standard, and would expect them to follow their stated privacy policy. The FTC would likely also expect PHRs to accurately describe the type and amount of personal information disclosed. However, one problem with FTC enforcement of these types of situations is the lack of a requirement for non-HIPAA PHRs to have a privacy policy in place. If a PHR vendor does not have a privacy policy in place, the FTC would have a difficult time forcing a PHR to follow a non-existent privacy policy.

Administrative Actions for Unfair Trade Practices: Privacy

The FTC has also used its authority to prevent unfair trade practices to file complaints against companies for violating consumer privacy. FTC has relied on this authority when the misrepresentation or deception by the offending company was not made directly to consumers, but through a third party.

For example, Vision I Properties, LLC operated a service called "CartManager," allowing online retailers to process payments for goods sold online.[177] When a consumer would click on their virtual shopping cart to make their purchases, the retailer would send them to a "CartManager"-run website that was styled the same way as the retailer's website, which made it unclear that consumers were entering another website.[178] While

[173] F.T.C. v. Echometrix, FTC File No. 102 3006 (Nov. 30, 2010), (available at http://www.ftc.gov/os/caselist/1023006/101130echometrixcmpt.pdf).
[174] *Id.*
[175] *In re* Sears Holdings Mgmt. Corp., FTC File No. 082 3099 (August 31, 2009) (available at http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf).
[176] *Id.*
[177] *In re* Vision I Properties, LLC, et al, FTC File No. 042 3068 (April 26, 2005) (available at http://www.ftc.gov/os/caselist/0423068/050426comp0423068.pdf).
[178] *Id.*

many retailers using "CartManager" maintained privacy policies that promised consumers that they would not share consumer information with third parties, "CartManager" did not have such a policy and sold personal information gathered during a consumer's checkout.[179] The FTC alleged that Vision I's practices were unfair because they were not forthcoming to retailers about its use of consumer information and as a result, caused substantial consumer injury that "was not offset by countervailing benefits to consumers or competition" and not avoidable by consumers.[180]

The FTC's Vision I complaint demonstrates that the Commission believes the selling of consumers' personal information, such as purchase history, name, address, and phone number, for the sake of direct marketing and without the consumers' knowledge may create "significant harm" or potential for harm. The FTC has in other cases detailed the harms that it believes this practice causes, such as emotional harm due to the subsequent harassment of telemarketing calls and monetary harm for consumers who decide to take action to prevent further privacy breaches, such as changing their phone numbers.[181] Emotional harm, therefore, may be a factor the FTC will consider when it seeks to exercise its unfairness authority in privacy cases.

This case shows that the FTC is willing to use its authority to prevent unfair trade practices to file complaints against companies that do not make deceptive misrepresentations or omissions directly to consumers, but instead use their relationship with consumer-facing companies, potentially deceiving those companies in the process, to gain access to and sell consumer information without giving the consumer an opportunity to avoid these practices. This principle could similarly be applied to PHRs if a non-HIPAA PHR were found to be selling consumer information without providing the consumer with notice and the opportunity to object to such sale of his or her personal information.

Administrative Actions for Deceptive Trade Practices: Security

The FTC has also alleged several deceptive trade practices concerning the security of personal information collected by companies over the Internet. Similar to enforcement relating to privacy practices, the FTC has filed complaints against companies on the basis that the companies failed to meet representations they made about security in policies that are publically available on their websites.[182]

For example, Twitter's privacy policy states, "Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access."[183] The FTC alleged that this statement was deceptive because, among other security failures that led to the unauthorized disclosure of private user information, Twitter failed to employ security safeguards to ensure that employees who had access to information consumers had deemed "private" (almost all Twitter employees had access to it) would not

[179] *Id.*
[180] *Id.*
[181] *See, e.g.*, FTC v. Accusearch, Inc., 570 F.3d 1187, 1193-1194 (10th Cir. 2009).
[182] *In re* Twitter, Inc., F.T.C. File No.092 3093 (March 11, 2011) (available at http://www.ftc.gov/os/caselist/0923093/100624twittercmpt.pdf); FTC v. ControlScan, Inc., F.T.C. File No. 072 3165 (Feb. 25, 2010) (available at http://www.ftc.gov/os/caselist/0723165/100225controlscanstip.pdf); *In re* Rite Aid Corp., F.T.C. File No. 072 3121 (November 22, 2010) (available at http://www.ftc.gov/os/caselist/0723121/100727riteaidcmpt.pdf).
[183] *In re* Twitter, Inc., *supra*.

purposefully or inadvertently expose the information to others.[184] The FTC specifically alleged that Twitter lacked reasonable and appropriate security measures based on the promises they made to consumers and the private nature of information they were holding, such as policies requiring strong passwords (i.e. prohibiting the use of dictionary words), policies that prohibit the storage of administrative passwords in personal e-mail accounts, and an administrative or technical means of restricting employee access to private information based on their need for that information.[185]

The Twitter case and other enforcement actions for deceptive security practices demonstrate the FTC's belief that companies that make general statements to consumers about protecting personal information collected through the Internet must take reasonable and appropriate security measures to protect that information. These protections are deemed reasonable based both on the promises made to consumers and the private nature of the information that the company has collected. Similarly, the FTC would most likely expect non-HIPAA PHRs to take reasonable and appropriate measures to protect information contained in a PHR whenever the PHR vendor makes general statements about protecting the security of consumer information.

Administrative Actions for Unfair Trade Practices: Security

In other enforcement actions related to security, the FTC has shown that it will file unfair practices complaints even in the absence of a misleading statement to consumers about security policies and practices. As noted earlier, these actions under the unfair trade practices authority of the FTC require the FTC to meet a higher bar than deceptive practices authority: it must show the practice caused or is likely to cause substantial injury to consumers that is not outweighed by the benefits of the practice, and that this injury is not reasonably avoidable by consumers.[186]

The FTC used this authority to allege unfair practices in its complaint against Dave and Buster's for failing to institute reasonable and appropriate safeguards to protect customer credit card information it collected and stored on its network.[187] Among other failures, the FTC alleged that Dave and Buster's lacked technical safeguards, such as an intrusion detection system, system traffic monitoring, and a means of restricting network access by IP addresses.[188] As a result, an intruder intercepted credit card information that was in transit between Dave and Busters' stores and its credit card processing company and fraudulently charged several hundred thousand dollars to these accounts.[189]

The Dave and Buster's case, as well as other cases in which the FTC exercised its authority to prevent unfair trade practices by pointing to companies' security failures,[190] shows the FTC's belief that even without an express promise to secure information in its public policies, companies that collect private information have a

[184] *Id.*
[185] *Id.*
[186] *FTC Policy Statement on Unfairness*, *supra*.
[187] *In re* Dave & Buster's, Inc., F.T.C. File No. 082 3153 (June 8, 2010) (available at http://www.ftc.gov/os/caselist/0823153/100325davebusterscmpt.pdf).
[188] *Id.*
[189] *Id.*
[190] *In re* DSW Inc., F.T.C. File No. 052 3096 (March 14, 2006) (available at http://www.ftc.gov/os/caselist/0523096/0523096c4157DSWComplaint.pdf); *In re* BJ's Wholesale Club, Inc., F.T.C. File No. 042 3160 (September 23, 2005) (available at http://www.ftc.gov/os/caselist/0423160/050616comp0423160.pdf).

responsibility under the FTC Act to put in place reasonable and appropriate safeguards to prevent substantial harms, such as identity theft and falsified credit card charges. For FTC enforcement under this unfairness authority, this responsibility appears to depend on the nature of the private information itself and the type of monetary or other harm its release would cause consumers.[191] With respect to PHRs, it is likely the FTC would need to find evidence of a company's potential unfair security practices and file a complaint against the company in order to give voice to its expectations for protecting information contained in PHRs. Although one can derive some idea about the expectations of the FTC from its prior settlements, there is no explicit directive from the FTC which defines what the FTC considers to be an unfair trade practice.

Summary of Administrative Enforcement Actions

The FTC has used its authority under the FTC Act to take administrative enforcement action against companies with an Internet presence that carry out unfair and deceptive practices that violate consumer privacy and/or fail to secure consumer information. While all of the cases described above were settled with a consent agreement, making the principles expressed in them non-binding to other companies, these cases may still be instructive to companies that fall under the FTC Act's jurisdiction, including companies that offer PHRs on the Internet. Statements made to consumers in privacy and security policies or omitted from these policies have proven important for enforcement determinations. However, the FTC has shown it may alternatively allege that a company has engaged in unfair practices without having made a deceptive statement or omission, but rather by violating consumer privacy, or failing to secure consumer information in a way that causes substantial unjustifiable harm. Based on the FTC's view as expressed in their enforcement decisions, companies that handle personal consumer information must secure it by applying reasonable and appropriate safeguards based on the type of information collected and the risk of harm to consumers if it were to be exposed. The security cases described above are instructive to companies in giving examples of these safeguards, but they are neither definitive nor serve as firm precedent. The individual companies must still make a determination as to what level of safeguards is reasonable and appropriate. There is no "one size fits all approach" as to which safeguards are reasonable and appropriate under different circumstances.

[191] *FTC Policy Statement on Unfairness*, *supra*.

C. FTC BREACH NOTIFICATION RULE FOR NON-HIPAA PHRS

As mentioned earlier in the section summarizing the breach notification rules for HIPAA CEs, the FTC did implement regulations for breach notification requirements for non-HIPAA PHRs. The FTC was specifically directed under the HITECH Act to issue these regulations for non-HIPAA PHR vendors and their non-HIPAA PHR associated entities, and did so in 2009.[192] These breach notification regulations will remain in place until "new legislation is enacted establishing requirements for notification in the case of a breach of security that apply to entities covered" by the temporary breach notification regulations promulgated by the FTC.[193] The temporary breach notification rule, at 16 C.F.R. §318.2(a), defines a breach of security as follows:

> Breach of security means, with respect to unsecured PHR identifiable health information of an individual in a personal health record, acquisition of such information without the authorization of the individual. Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information unless the vendor of personal health records, PHR related entity, or third party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.[194]

Under the FTC breach notification rule, a non-HIPAA PHR vendor must notify consumers of any discovered breach of identifiable health information from their non-HIPAA PHR and must also notify the FTC.[195] If the breach involves the records of fewer than 500 people, notification must be provided to both the individuals and the FTC "without reasonable delay and in no case later than 60 calendar days after the discovery of a breach of security."[196] When providing notification of a breach to the FTC, "if the breach involves the unsecured PHR identifiable health information of 500 or more individuals, then such notice shall be provided as soon as possible and in no case later than ten business days following the date of discovery of the breach."[197] If the breach involves records of 500 or more residents of a particular state or jurisdiction, the PHR must also notify the media in that state or jurisdiction and must provide the notification to the media "without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach of security."[198] These appear to be the only federal regulations that apply specifically to non-HIPAA PHRs.

D. PHR REGULATION BY STATES

In addition to federal regulations, many states also have confidentiality laws in place which may also apply to PHRs. For example, the scope of California's primary law protecting medical information, the Confidentiality of Medical Information Act (CMIA), was expanded in 2008 to expressly include businesses organized for the purposes of allowing individuals to manage their health information.[199] The CMIA holds such businesses to the same confidentiality standards as "providers of health care" and makes them subject to the same penalties

[192] HITECH Act § 13407(a),(b).
[193] 16 C.F.R. § 318.9.
[194] 16 C.F.R. § 318.2(a).
[195] 16 C.F.R. § 318.3(a).
[196] 16 C.F.R. § 318.4(a).
[197] 16 C.F.R. § 318.5(c).
[198] 16 C.F.R. § 318.4(a).
[199] California Civil Code § 56.06(a) (2009). *See also* ONC Roundtable, *supra* note 4, at 304-306 (comments of Joanna McNabb, Chief, Cal. Office of Privacy Protection).

for improper use and disclosure of medical information.[200] Oregon has established a Health Information Technology Oversight Council that has the power to ensure that PHRs, EHRs, and other forms of electronic decision support used in health care have appropriate privacy and security controls.[201] Oregon requires that data may not be used for purposes other than patient care except as permitted by law.[202] Several other states have statutes that extend privacy and security protections to persons "receiving" health records, and these statutes may also apply to PHR vendors.[203]

State Breach Notification Laws

In addition to confidentiality laws, many states also have breach notification laws in place. Within the past few years, all but four states have enacted breach notification statutes.[204] While only five of these statutes specifically protect health information, the remaining statutes protect other consumer information often held by health care-related businesses such as social security numbers, driver's license numbers and/or account number (with security code, access code, PIN or password needed to access that account).[205] Although such state breach notification laws are of less significance since there are regulations that specifically focus on breach notification requirements for non-HIPAA PHRs, it is worth noting the existence and potential applicability of such state laws as well.

E. LEGAL REQUIREMENTS THAT EMERGE WHEN DATA MOVES FROM AN EHR TO A PHR

When information is transferred from a patient's EHR to a PHR or vice versa, several changes in the legal protections for that information may occur. One such change is the loss of the provider-patient privilege: when information is disclosed by the physician or patient to a third party such as a PHR vendor.[206] Another change in legal protections or requirements occurs when information is transferred from a PHR to a HIPAA covered provider's EHR. When health information is transferred in this manner, it will become PHI under HIPAA, and will be subject to HIPAA's use and disclosure rules as well as its security requirements. Consumers should be made aware of these changes in legal protections and requirements and must understand that the presence of requirements for a PHR in one format does not guarantee that such protections will always apply to that PHR.

---

[200] California Civil Code § 56.06(b)-(c) (2009).
[201] Oregon Health Information Technology Oversight Council, About Us, (n.d.). Retrieved Dec. 4, 2013 from http://www.oregon.gov/oha/OHPR/HITOC/Pages/about_us.aspx.
[202] Oregon Revised Statute § 413.308(5)(b).
[203] These statutes do not mention PHRs, and it is unclear whether they were intended to cover only entities interacting regularly with health care providers such as claims payers, data clearinghouses, or data warehouses, or to cover any of the PHR models that receive data directly from health care providers or indirectly from claims payers. For example, Arizona, Maryland, and Minnesota have statutes of this type. Arizona Revised Statute § 12-2294(E); Maryland Annotated Code Health-Gen. § 4-302(d); Minnesota Statute § 144.293(2). Other states, such as Arizona or Florida, may have definitions of "medical record" or "health record" that include patient-created material, so long as the primary purpose of the material is the provision of health care. Arizona Revised Statute § 12-2291(5); Florida Statute § 408.051(a)(d). In these states, privacy protections governing health records may apply to such patient-created material.
[204] Forty-six states have breach notification statutes. *See State Security Breach Notification Laws*, National Conference of State Legislatures. Retrieved from http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.
[205] The states including at least some health information in these statutes are Arkansas, California, Missouri, Texas, and Wisconsin. Arkansas Code § 4-110-103(7); California Civil Code § 1798.29(g)(4); Missouri Revised Statute § 407.1500(9); Texas Business and Commercial Code § 521.002(a)(2)(B); Wisconsin Statute § 134.98(1)(b).
[206] *See* Robert Gellman, *supra*, at 5–6.

F. CONCLUSION

The legal landscape for PHRs is complex and covered by multiple Federal and state legislation and regulations. The applicability of a specific law to a specific PHR can depend on a number of different factors, such as whether the PHR is provided by a vendor that is under contract to a HIPAA-covered entity or the state in which PHR vendor activities are carried out. Because PHRs are a new and evolving healthcare information technology, it is likely that the applicability and interpretation of legislation and regulation will continue to be refined.

For the purpose of this report, however, it is important to contrast the way in which current FTC and HIPAA rules would apply to regulate the conduct of companies that offer PHRs, which may appear similar to consumers. While the FTC does possess rulemaking authority to establish prescriptive regulations related to privacy and security pursuant to its ability to regulate "unfair" and "deceptive" trade practices, section 18 of the Federal Trade Commission Act requires the use of a cumbersome and time-consuming process to make those rules. As a result of these burdensome requirements, the FTC rarely relies upon its rulemaking authority, and instead utilizes administrative enforcement actions to build a case-by-case standard for which privacy and security-related behaviors it considers to be "unfair" or "deceptive." While these cases do not form controlling precedent, they nevertheless illustrate a standard for privacy and security practices which should guide the privacy and security practices of PHRs.

The HIPAA paradigm, in contrast, adopts specific privacy and security standards that apply both to HIPAA Covered Entities and Business Associates. If a CE or BA violates those standards, it may be subject to automatic civil monetary policies assessed by HHS OCR which, unlike the FTC, is allowed to assess penalties against violators without administrative or judicial process. To apply HIPAA privacy and security standards to organizations currently offering a non-HIPAA PHR, however, the HIPAA statute would need to be expanded to grant regulatory authority over such organizations, and new regulations would need to clarify which information held by those entities is deemed PHI for the purposes of the HIPAA regulations. Since HIPAA rules have been developed to inform and regulate the practices of institutional health care actors (CEs and BAs), careful attention would be needed in order to adapt these rules for application in the patient-centric context of non-HIPAA PHRs. Further, whereas FTC enforcement can be conducted on the basis of what privacy and security practices are "reasonable" at the present time, HIPAA rules must be re-examined at different points in time to make sure that they continue to effectively safeguard the PHI held by entities subject to HIPAA and its regulations.

To summarize, while the HIPAA paradigm sets forth formal and uniform privacy and security standards across the entire class of HIPAA-regulated entities, the FTC's approach of using administrative adjudications to protect consumers from violations of the privacy and security of their personal information uses a case-by-case approach. For example, whereas HIPAA regulations require CEs to provide individuals with a notice of privacy practices describing how the CE will use and disclose those individuals' PHI,[207] no similar standard exists under

[207] 45 C.F.R. § 164.520.

FTC rules. Previous FTC cases have, however, charged companies for failing to prospectively inform consumers of uses of their information when that failure constitutes a deceptive omission.[208] A significant challenge when using the FTC enforcement authority exists due to the fact that the FTC would face a difficult process to write a regulation if they wished to uniformly require companies to prospectively inform consumers of uses of their information, and thus the FTC is unlikely to promulgate such a regulation. Another significant challenge in the FTC enforcement process is the fact that it uses a harm-based approach to investigating and assessing violations which means that individual cases will most likely be overlooked in favor of major cases with larger potential damages.

It is clear from this review that, as they currently stand, neither FTC regulatory actions nor HIPAA regulations could seamlessly apply to protect consumer information held in non-HIPAA PHRs. Careful balancing of the relative merits of these two systems will be required to establish a policy and regulatory paradigm for non-HIPAA PHRs that successfully protects the privacy and security of consumers using PHRs.

[208] *See* F.T.C. v. Echometrix *supra*.

4. PRIVACY AND SECURITY POLICIES AND PRACTICES OF NON-HIPAA PHRS

In order to more fully understand the ways in which different PHRs convey their privacy and security policies, as well as how these PHRs adhere to their privacy and security policies, the authors surveyed a number of PHR sites. This section presents the findings regarding the privacy and security practices of non-HIPAA PHRs primarily based on representations made and practices observed on publically available websites during this survey.[209] Data was collected between July 2010 and March 2011 and was accurate as of those dates. The analysis focused particularly on statements and notices provided to consumers by PHR vendors which can then be evaluated to determine if any such notices or statements convey unfair or deceptive practices. The complete set of the findings with respect to privacy is contained in Appendix C, and the complete set of findings with respect to security is contained in Appendix D. These results demonstrate the ways in which PHRs are functioning in the real world, and the ways in which they are (or are not) carrying out privacy and security policies.

A. DATA COLLECTION, SCOPE, AND METHODS

To gather data for this report, the authors reviewed the privacy and security practices of selected non-HIPAA PHRs; the privacy and security practices of the entities with which non-HIPAA PHRs interact; and the privacy and security practices of third party service providers. [210] The authors selected 41 PHRs to review from the American Health Information Management Association (AHIMA) consumer PHR information website,[211] Medicare PHR demonstration projects,[212] and the 2008 Chilmark market analysis of PHR vendors.[213] The 17 smart device (e.g., iPhone, Android, and iPad) applications (apps) reviewed were selected for review based on popularity rank in the Apple and Android app stores, sensitivity of health conditions represented, and likely size of the audience. The review was limited to publicly available information collected from the websites of PHR vendors and related entities, such as website "Terms and Conditions" or "Privacy Policies," and publicly available information about smart apps. Report authors did not purchase fee-based PHRs, although they did establish test versions of no-cost PHRs. The analysis did not independently validate whether the publically available statements and policies by non-HIPAA PHRs are being implemented as described.

---

[209] This study did not include PHRs that are covered under only HIPAA. Eight of the PHRs included in the study are offered directly to consumers, and are also sold by vendors to providers or health plans under business associate agreements with these HIPAA-covered entities. These PHR vendors are regulated by HIPAA when covered entities contract with them to offer the PHR to their patients, but are not regulated by HIPAA when they offer the PHR directly to patients. Although HIPAA PHRs and non-HIPAA PHRs may be required to comply with the same requirements in many circumstances—for example, applying the same security protections both in their HIPAA and in their non-HIPAA forms—they are covered by different legal structures and may have other different privacy and security protections as result. For example, a PHR may have advertising in its non-HIPAA form, but not have advertising in its HIPAA form due to HIPAA's constraints on marketing. The data presented represents *only* the non-HIPAA versions of these PHRs. *See* section III *supra*.

[210] Appendices C and D include the complete privacy and security study findings, respectively.

[211] MyPHR brought to you by AHIMA, AHIMA Foundation. (n.d.). Retrieved from www.myphr.com.

[212] U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services. (n.d.). *CMS Personal Health Record Pilots in South Carolina, Arizona, and Utah*, Retrieved from https://www.cms.gov/Medicare/E-Health/PerHealthRecords/PHR_Pilots.html.

[213] Chilmark Research. (2008). *2008 iPHR Market Report*, *Analysis & Trends of Internet-based Personal Health Records' Market.* Retrieved from https://www.chilmarkresearch.com/chilmark_report/iphr-market-report-2008-analysis-trends/.

Non-HIPAA PHRs privacy and security policies were assessed against the Fair Information Practice Principles (FIPPs), NIST security standards, and numerous other frameworks and recommendations for privacy and security practices. The FIPPs basic principles are:

- Transparency
- Individual Participation
- Purpose Specification
- Data Minimization
- Use Limitation
- Data Quality and Integrity
- Security
- Accountability and Auditing[214]

Appendix E provides a mapping of the FIPPs to other privacy and security regulations and recommendations.

B. PRIVACY FINDINGS

The study found considerable variation in privacy policies publicly displayed by non-HIPAA PHR vendors. Some vendors appear to have adopted strict privacy guarantees (beyond those required by HIPAA). Others appear to offer more limited protections for privacy. The privacy review examined privacy policies to determine how well they comply with the following FIPPs:

- Transparency: availability of privacy policies and the language of the privacy policies;
- Use Limitation, Individual Participation, and Purpose Specification;
  - Consent to changes in privacy policies;
  - Advertising, commercial uses, and behavioral tracking;
  - Data retention;
  - Uses for law enforcement or response to subpoena; and
- Data quality and integrity: ability to correct or delete data to ensure continued accuracy.

The privacy review also identified and assessed special considerations related to smart devices and apps. The table found in Appendix C documents the observations made of the selected PHRs and apps in each of the above categories. The following sections summarize these findings.

Transparency – Availability of Privacy Policies

Out of the 41 PHR vendor websites reviewed, 37 of them had links to privacy policies on the home page of the PHR vendor. All of the sites with links to privacy policies provided access to the policy within one or two clicks by the user. Two sites, of the 37 with links to privacy policies, had "beta" or "test" versions of PHRs that allowed consumers to enter personal information, but had links to privacy policies that were broken. Some PHRs did not have privacy policies that were readily visible. Some of the sites had links to privacy policies that were in small type or located at the bottom of the website where they could not be easily seen. Other PHR

[214] While many versions of FIPPs have been published, all versions stem from the principles set forth in: U.S. Dept. of Health, Education, and Welfare. (1973). *Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems.* Retrieved from http://epic.org/privacy/hew1973report/.

vendor websites required browsing through multiple pages to find the policy. Some PHR vendor websites scattered information about privacy in documents that were not clearly labeled as "privacy" policies, such as an FAQ. Some privacy policies could be located only after scrolling past advertisements.

Transparency – Language of Privacy Policies

The study examined PHR vendors' privacy policies (as well as terms and conditions and FAQs where available) and identified several commonly-used phrases that may be confusing to consumers, such as the following:

- References to HIPAA
- Assertions regarding the use of individually identifiable information
- Liability waivers and damage limitations.

The paragraphs that follow describe these phrases and ways in which these phrases are ambiguous and may be confusing to consumers.

References to HIPAA**:** HIPAA is treated in three ways by non-HIPAA PHR privacy policies. The first group of PHR websites studied did not mention HIPAA at all. In the second group of PHR websites studied, privacy polices clearly state that the PHR is not covered by HIPAA and the information in the PHR does not receive the same legal protections as information held by covered entities. In the third group of PHR websites studied, the privacy policies indicate that the PHRs follow HIPAA, the PHR is "HIPAA-compliant," the PHR "adheres to" or "follows" HIPAA standards, or the PHR "uses HIPAA as a guideline." The use of these phrases raises concerns with regard to the transparency principle, because they do not fully explain to consumers that the PHR vendor is only voluntarily following the HIPAA standards and is not subject to the same enforcement procedures as HIPAA covered entities.

Assertions regarding use of individually identifiable information**:** On the PHR websites reviewed for this study, several of the PHR privacy policies use the terms "aggregated" or "anonymized" to indicate to consumers that although the operators of the website may perform many different activities with information in the PHRs, including research, analysis of consumer interests or activities, and analysis designed to improve PHR performance, consumers will not be individually identified. Seventeen of the 41 PHRs reviewed did not specify their policies regarding the use of aggregated and anonymized data. Ten of the PHRs reviewed did provide specific statements regarding the use of aggregated and anonymized data. Four of the ten PHRs with specific statements did not provide definitions on aggregated and anonymized data. Two of the PHRs' policies refer to aggregation with other data but do not indicate what the sources are for this other data. This lack of comprehensive explanations around use of aggregated and anonymized data practice raises concern with transparency because there are multiple methods which can be used to "anonymize" or "aggregate" data and there is considerable debate about which of these different methods protect patient privacy by mitigating the risk that the data can be re-identified and connected to individuals.

Liability waivers and damage limitations: Twenty-four of the PHRs studied present waivers or limits that required consumer agreement in order to use the PHR. Some disclaim liability for any information posted on the site. Some, such as CapMed and TeleMedical, indicate that the site will not be liable for loss or destruction

of information. Some waivers simply state that use of the site is at the consumer's own risk and the consumer waives liability for anything that happens to his or her information.[215] In these cases, it may be unclear to consumers for what specific actions the site is intending to disclaim responsibility. It may also be unclear to consumers whether such waivers disclaim damages in cases of medical identity theft.

Use Limitation, Individual Participation, and Purpose Specification – Consent to Changes in Privacy Policies

PHR vendors generally reserve the right to change their privacy policies. Twenty-five of the PHR vendors reviewed post changes to their privacy policies on their websites and provide no further notification to consumers. Twelve vendors notify consumers by email of changes in their privacy policies. Three vendors indicate that they can change policies without notification.

Generally the PHR vendor considers continued use of the PHR to constitute consent to the policy change whether or not the consumer is aware of the change. Although this is a far less common practice, several PHRs inform consumers that changes in the privacy policy will be effective immediately even if they have not been previously posted on the PHR website.

Only four vendors require that consumers affirmatively agree to changes to privacy policies. One of these vendors (TeleMedical) only allows the consumer to opt out if they do not agree to changes in the privacy policy. PHRs that do not allow consumers the possibility of opting in to material changes in the privacy policy effectively present consumers with only two choices: continue to use the PHR with the changed policy, or close the PHR and request deletion of their information.

Use limitation, Individual participation, and Purpose Specification – Advertising, Commercial Uses, and Behavioral Tracking

PHRs differed in their approaches to advertising on their sites, tracking of user behavior, and links to external sites.

Advertising – Many PHR privacy policies inform consumers when there may be advertising on the PHR website and also state that use of the site constitutes consent to this advertising. Two of the vendors reviewed allow the consumer to opt out of receiving advertisements when using the PHR. dLife allows consumers to opt out of advertising. NoMoreClipboard allows users to purchase an upgraded account that does not have advertising.

Tracking of Users – PHRs also vary with respect to the use of devices that enable tracking of the user on the site and disclosures made about these uses. One example of a tracking device is a "cookie." In its simplest form, a web cookie is a general mechanism a server can use to store and retrieve information from a website user. Cookies can have many beneficial functions, including authentication, storing site preferences, shopping cart contents, session management, or other timesaving functions that can be accomplished through storing

[215] Such waivers would not affect the website's liability to federal enforcement actions under the FTC Act. In cases of unfair or deceptive acts or practices with respect to which the FTC has issued a final cease and desist order, and in which the act or practices is one a reasonable person would have judged dishonest or fraudulent, the FTC may seek consumer damages in court. 15 U.S.C. § 57b(a)(2), (b). State unfair or deceptive trade practice laws may also allow suits for consumer damages and it would be a matter of state law whether rights under these statutes can be waived. *See, e.g.*, California Business and Professional Code § 17204; 73 Pennsylvania Consumer Statute § 201-9.2.

text data. Generally, a website's full functionality will be lost to an end-user if all cookies are disabled within a web browser. The dLife PHR specifically references this type of tracking in its policies explaining that they may collect anonymous and aggregated information by using cookies, action tags and other methods. The EMRy Stick and Google PHR policies indicate that they capture this type of data, but only retain it for two weeks, after which it is used only in aggregated form. Other PHR policies are more general when discussing tracking of users, and state that they will be, "logging information about the consumer's use of the PHR."

Links to External Sites – When the PHR site offers links to third- party service providers, customers may click on the link and follow it to locations off the PHR site. Many of the non-HIPAA PHRs surveyed offer links within the PHR to information that may be helpful to consumers. Some of these links are to information services, such as medical dictionaries, also located within the PHR, so that the patient does not leave the actual PHR environment. Others link to off-site medical reference services such as the National Library of Medicine or the Mayo Clinic. There are also links on PHRs to third party service providers that may be interested in collecting health information from the consumer who visits their site.

Thirty of the PHR vendors surveyed advertised products on their homepage or offered services that require consumers to click through to an external site from the PHR homepage. In some cases, these links suggest to consumers that they will be receiving medical information. The privacy policies that apply while on the PHR website do not apply to activities on these home pages of the external products or advertisements. Consumers visiting the PHR website may follow links on the PHR home page without receiving a notification that they may be going to other websites outside of the PHR website. They also do not receive notification that while these other websites may ask for personal information, the sites may provide different privacy protections from those provided by the PHR website. The privacy policies of non-HIPAA PHRs regarding the collection of patient identifying information by third party sites vary considerably and have raised concerns of privacy advocates.[216]

Use limitation, Individual participation, and Purpose Specification – Data Retention

None of PHR privacy policies reviewed address what will happen to the information in PHRs that is left unused for a lengthy period of time. Four of the PHRs reviewed keep backup copies of deleted information for a set period of time or without any stated time limit.

Use limitation, Individual participation, and Purpose Specification – Uses for Law Enforcement or Response to Subpoena

Twenty-five of the PHR vendor websites surveyed indicated that the sites would disclose information if they believed they were required to do so by law or in response to a subpoena. The non-HIPAA PHR sites do not indicate how they would determine their response to a subpoena request or reference the variety of state law reporting requirements.[217] A few PHR vendors, including Juniper Health and MyMedicalRecords, indicated

[216] Center for Democracy and Technology. (2010). *Comments of the Center for Democracy & Technology to the Office of the National Coordinator Roundtable*, pg. 17. Retrieved from http://www.cdt.org/files/pdfs/CDT_Comment_to_ONC_PHR_Roundtable.pdf.

[217] In contrast, HIPAA requires covered entities to obtain adequate assurances that the patient has been notified of the request and has been given an opportunity to object in court, or that a protective order has been sought to prevent further disclosure of the information during or after the case prior to disclosing health information in response to a subpoena without patient authorization. 45 C.F.R. § 164.512(e).

that if the customer's data were transferred as a result of a legal requirement, the vendor would provide the customer with notice.

Thirty of the PHR vendors surveyed indicated that they would disclose data for treatment, payment, and health care operations. Juniper Health and myMediConnect's policies indicated that they would disclose information to prevent harm.

Data quality and integrity – Data Correction or Deletion

Data accuracy is particularly important for information in PHRs that may be used for treatment by health care providers, such as individually identifiable health information that is transferred from an EHR to a PHR, that the patient shares with other providers or the direct transfer of lab test results into the PHR. Physicians and other providers have expressed concerns that if patients can alter or delete information in PHRs, the information in the record may be incomplete or inaccurate and relying on it for care decisions may subject providers to liability.[218] For PHRs used by providers for treatment purposes, it is important to maintain the integrity of the record and to clarify sources of information. However, one benefit for patients who download treatment information from their providers to their PHRs, comes from the patient's ability to detect errors in the patient's medical records. If treatment decisions are made based on records downloaded to PHRs, it is also important for patients to be able to point out possible inaccuracies to their treating providers.

Non-HIPAA PHRs vary significantly in their practices regarding changes, correction or deletion of information. Our report identified examples of the following practices:

- Allowing individuals to make notations about information in the PHR that they believe to be incorrect.
- Allowing the consumer to make changes, corrections or deletions. Twenty-four of the vendors surveyed allowed users to correct or delete data.
- Requiring consumers to submit any requests for changes, corrections, or deletions in writing. One of the vendors surveyed, dLife, required that users submit corrections or deletions in writing either by email or regular mail.
- Not permitting the deletion of information in the PHR. One vendor reviewed in the survey, EMRy Stick, did not allow users to change data.
- Delaying requested deletions for periods as long as 180 days, even when the consumer is requesting to terminate use of the PHR.

[218] *National Committee on Vital Health Statistics, Subcommittee on Privacy, Confidentiality, and Security. Hearings on Personal Health Records,* 111th Congress. (2009) (statement of Dr. Matthew Wynia, Director, the Institute for Ethics at the American Medical Association) Retrieved from http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090521p6.pdf.

Special Considerations Related to PHRs Offered on Smart Devices and Apps

Smart devices, such as phones or tablets which give consumers access to the Internet as well as other multimedia functionality, apply privacy policies to all applications or "apps" available through their operating systems. Apps may also have their own privacy policies. This report reviewed the device privacy policies of the two current market leaders for smart device applications, Apple and Google.

Apple offers apps through the iTunes store. Apple's terms of use for apps incorporate the general privacy policy that covers consumers' use of iTunes. Apple reserves the right to share personal information about its customers to affiliates and third parties to improve its services and for advertising purposes, and defines personal information as information that could be used to uniquely identify or contact a single person.[219] If the information is considered non-personal, then Apple has wide latitude to use the data "for any purpose."[220] The Apple terms of service make it clear that Apple provides no warranty, and disclaims any liability for the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality, or any other aspect of third-party apps.[221] Apple specifically states that third parties providing services through apps are governed by their own privacy policies. Apple also reserves the right to remove or disable access to any apps from an Apple device at any time and without notice.[222]

Google developed the Android operating system, which contains searching functions from the Google platform. The privacy policy of the parent company Google applies to most of its products, services and websites.[223] Google, as required by its enforcement agreement with the FTC, agrees to ask for the explicit consent of its users if it should ever propose to use personal information in new ways that were not previously agreed to by the user. Google also requires any affiliates accessing users' personal information to agree to comply with Google's privacy policy, although it is unclear whether or not Google directly monitors their affiliate privacy and security practices.[224] The Android operating system has its own device-specific privacy policy.[225] The Google privacy policy does not apply to third-party apps that are merely offered through a device operating the Android system. In these cases, the individual app developer's privacy policy will apply to the specific data the app collects.

Many non-HIPAA PHRs are offered both as websites and smart device apps with the same privacy policy used for both environments. Other PHRs are offered only as apps and in such cases may have their own privacy policies outside of the device operating systems they are offered on. These policies vary greatly. Some rely only on the privacy policy of the smart device. Some feature very short statements about the privacy policies that apply to the data that the app obtains and stores.

---

[219] *Mac App Store, App Store, and iBooks StoreTerms and Conditions*, (n.d.). Retrieved from http://www.apple.com/legal/itunes/us/terms.html#APPS.
[220] *Apple Customer Privacy Policy,* (n.d.). Retrieved from http://www.apple.com/privacy.
[221] *Licensed Application End User License Agreement*, (n.d.). Retrieved from http://www.apple.com/legal/itunes/appstore/dev/stdeula/.
[222] *Terms and Conditions*, *supra*.
[223] *Google.com Privacy Policy*, Retrieved from http://www.google.com/policies/privacy/archive/20111020 (Note: this is the Google Privacy Policy which was in place prior to March 1, 2012).
[224] *Id.*
[225] *Privacy Policy, Droidcellphone.com* (n.d.). Retrieved from http://droidcellphone.com/privacy-policy.

Several additional privacy issues particular to smart apps are worth noting. First, smart devices have the capacity for geolocation[226] and body sensing.[227] Apple encourages apps to link to a user's contacts and geographic location.[228] In the materials given to developers that are publicly available, Apple tells app developers that they can access the user's list of contacts to get "information relevant to your application's needs."[229] Apple also tells developers that they can obtain the user's location "to tailor information for the user's current location [to] make for a compelling user experience."[230] This function may add value to the app, including information relevant to health, such as local air quality. It is unclear whether consumers would be aware, however, of the possibility that PHR identifiable information could be linked with their geographic location in real time and potentially their first and last name as provided on their iTunes account.

Second, apps may function both on the smart device and as tools on a website for the consumer to access. Apps examined for the report do not always tell the consumer whether information is being provided, stored, or used locally through the app, or whether the app is linking the consumer to a website.

Of the 17 smart device apps reviewed, only four had privacy policies (BodyMedia, iMensies, iTriage, motionPHR). All of these policies could be accessed with a single click by the user. In addition to a privacy policy, the BodyMedia app did not support advertising and allowed users to correct data in writing on their website.

C. SECURITY FINDINGS

Security policies and practices address the need to protect data and ensure its integrity. The policies and practices guard against unauthorized access and thus against unexpected disclosures or uses. Security practices also provide oversight and accountability for data collection and management practices.

While technical, administrative, and physical safeguards all form a basis for data security,[231] this study focuses mainly on technical safeguards as reported by these non-HIPAA PHR vendors because they can be examined through a website content-based assessment.[232] However, this study also evaluates administrative and physical security policies when they appear in the PHR's overall privacy practices statement.

---

[226] Smartphones can be tracked in real-time through each mobile phone's Unique Device ID (UDID), for example. The UDID is a serial number associated with each phone and traceable to the individual consumer.

[227] For example, BodyMedia's $249 SenseWear arm-band sensors can now communicate with smartphone devices such as iPhone and Droid via Bluetooth technology, including collecting and monitoring over 9,000 measurements. Liden, Craig B. et al., *Characterization and Implications of the Sensors Incorporated into the SenseWear Armband for Energy Expenditure and Activity Detection.* (2010). Retrieved from http://www.bodymedia.com/site/docs/papers/Sensors.pdf.

[228] *Apple.com iOS Reference Library*, Retrieved from http://developer.apple.com/library/ios/#referencelibrary/GettingStarted/Creating_an_iPhone_App/index.html%23//apple_ref/doc/uid/TP40007595.

[229] *Id*.

[230] *Id*.

[231] HIPAA Security Rule, 45 C.F.R. §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards). *See also* U.S. Department of Health and Human Services, Office for Civil Rights. (March 2007). *HIPAA Security Series: Security 101 for Covered Entities.* Retrieved from http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf.

[232] Administrative safeguards ensure that the right policies are in place to protect information, including, for example, password management policies and security training and termination procedures for employees. Physical safeguards include physical facility and workstation access controls and policies and procedures to ensure the appropriate protection of data from loss, disaster, theft, or other means of destruction or alteration. The study found that privacy and security policies typically did not describe administrative and physical safeguards, and therefore this study does not address them in a comprehensive fashion.

The report addresses the FIPPs principles of Data Quality and Integrity and Security by assessing the following security features of non-HIPAA PHRs:

- Consumer registration and identity proofing
- Authentication, password strength, encryption
- Administrative security policies
- Physical security policies
- Statements about risk assessment or audit capability

The table found in Appendix D documents the observations made of the selected PHRs and apps in each of the above categories. The following sections summarize these findings.

Consumer Registration and Identity Proofing

"Consumer registration" means the process of subscribing to a PHR, and "identity proofing" means validating sufficient information for unique identification of the subscriber.[233] Identity proofing requires the PHR vendor to have some way of determining whether a person establishing a PHR is who they say they are, and not an imposter. If users' identities are not "proven" when establishing the PHR, anyone accessing the information in it could mistakenly believe that information was entered by the users or their representatives at their request. In addition, an impersonator registering for a PHR that is tethered to an EHR may be able to request transfer of his or her health records to the PHR, and thus gain unauthorized access to health information through the PHR.

Most non-HIPAA PHRs use basic methods for registration and identity proofing.[234] Table 1 presents the type of identity information requested by the PHRs reviewed for this report.

TABLE 1: IDENTITY INFORMATION REQUESTED BY PHRS

Identity Information	Frequency
Name	26
Date of Birth	24
Email Address	24
Address	12
Gender	12
Zip Code (without address)	6
Phone	6
State	1
None requested till purchase	5

[233] National Institute of Standards and Technology. (2006*). NIST Special Publication 800-63 Version 1.0.2, Electronic Authentication Guideline, Information Security*. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf.
[234] *Id*.

PHR sites request different combinations of identifying information. Users subscribing to non-HIPAA PHRs typically enter their name, email address, and date of birth. In a few cases, a name and email address will suffice. In other cases, subscribers may be requested to enter additional information such as sex, phone number, address (or aspects of location such as time zone, country, state, county or city, or zip code), race, height and weight, or employer. For example, Health Butler requests name, date of birth, address, email, gender, height, weight, and race while Revolution Health requires only an email and date of birth. All of this information may be known by others who could impersonate the user.

Individuals who want to establish a PHR from any of the vendors surveyed for this study create their own usernames, passwords, and security questions and answers. Unlike PHRs that are offered by a health care provider, PHRs offered by non-HIPAA PHRs (and health plans) are less likely to offer in-person identification proofing because of the lack of an opportunity to do so. Health plans that offer PHRs may offer other means for identity proofing, as they have existing individual data from verifying their enrollment for participation in the plan. It appears to be much more difficult for non-HIPAA PHRs to identity-proof an individual user, and the study of the non-HIPAA PHR security policies reflects this.

Authentication

"Authentication" means a method for establishing confidence in user identity.[235] The methods by which an individual may authenticate himself or herself for the PHR fall into three categories based on the factors used to verify identity:

- Something the user knows (such as a password)
- Something the user has (such as a token or an ATM card)
- Something the user is (i.e., that is biometrically unique [such as a fingerprint]).

Single-factor authentication consists of the use of one of these factors. It is used in situations where the risk level is low and when using multiple factors would be overly burdensome. For example, many websites allow subscribers to login using just a user name and password.

Multi-factor authentication requires two or more of these factors. Because multi-factor authentication provides a higher level of identity assurance, it is used in situations where the risk is higher. An example of multi-factor authentication is the ATM machine, which requires both an ATM card (something the user has) and a password (something the user knows). Multi-factor authentication solutions can have greater costs associated with them in terms of procurement, implementation, and continuing maintenance and administration.

This report found that all of the PHRs used single-factor authentication for accessing an established PHR. This authentication was in the form of a username and password created by the individual establishing the PHR. Microsoft HealthVault authenticates users through their Windows Live log-in credentials. Similarly, Google Health relies on the log-in and authentication practices used across the Google platform. The

[235] *Id.*

RingfulHealth PHR takes the additional step of sending a password to the registered email address (the user can subsequently change the provided password).

Password Complexity

Password strength measures the effectiveness of a password in preventing unwanted access to the information in the PHR through password-cracking attacks. In its typical form, password strength estimates how many trials an attacker who knows a username but does not know the password would need, on average, to guess the password correctly. The strength of a password is a function of its length, its complexity, and its randomness. Weak passwords have features that make them very easy to guess, such as repeating the user's name, using an expected phrase (for example, "health" or "healthrecord"), or being very short.[236] Users may find weak passwords easier to remember than strong passwords.

The risks posed by weak passwords are greater depending on whether additional safeguards are in place. Locking out access after a limited number of failed attempts can interrupt password cracking attacks and thus reduce their effectiveness. Requiring individuals to change passwords on a regular basis reduces the time available for password cracking attempts. Multi-factor authentication makes password cracking more difficult, as the individual must also have the additional authenticating element in hand (such as an ATM card). Additional factors limiting access may also reduce risks. For example, online banking may require users to supply additional security information when they log in from an unfamiliar computer. ATM withdrawals typically include additional limiting factors, such as the amount or frequency of withdrawals.

The analysis informally tested the password complexity required by the PHR sites that mandated authentication. Table 2 below shows the password minimum length required by the PHRs reviewed.

TABLE 2: MINIMUM PASSWORD STRENGTH REQUIRED BY PHRS

Password Minimum Length	Frequency
0	1
1	2
4	2
5	1
6	16
7	1
8	5

A few sites allowed users to create passwords with a single character. The majority of websites required passwords to have a minimum of six characters but did not have additional complexity requirements. Five of the PHRs examined required passwords with at least eight characters.

[236] *Id*.

Five PHRs required at least one additional complexity feature (such as a number or at least one uppercase letter). Table 3 below shows the complexity factors used by the PHRs reviewed and the number of PHRs using each factor.

TABLE 3: COMPLEXITY FACTORS REQUIRED BY PHRS

Additional Complexity Factor	Frequency
Letter	3
Lower Case Character	2
Upper Case Character	2
Number	5
Not First or Last Name	1

In conjunction with single factor authentication and the lack of other reducing factors, limited password complexity requirements may raise security concerns.

Encryption

Encryption protects security by using an algorithm to make data unreadable so that someone else cannot understand it without a de-encryption key.[237] An important distinction regarding encryption concerns data in motion or data at rest. Data in motion is data as it is being transmitted back and forth, for example, from the user to the PHR vendor. Encryption of data in motion is a best practice accepted by most websites that collect identifiable data from users, because data in motion is vulnerable to interception by a third party. Data at rest is stored data. In some cases, a risk assessment may determine that data at rest, particularly when it is stored on a server, is adequately protected by other types of security and therefore encryption is not needed for security protection. However, even if the stored data is not accessible remotely on a network, it may still be subject to unauthorized access if it is stored on portable media, such as a flash drive or a laptop. In such cases, the risk of a breach is high and encryption likely necessary.

Encryption of data in motion is a security feature that is easily identifiable in a website review.[238] Ten of the sites reviewed encrypted users' connections to the web server hosting its services. Eighteen additional sites encrypted information that the individual sent to the service provider as part of the authentication process. In addition, sites encrypted the transmission of health information after successful validation of the authorized user. This report verified through the URL review that all but four of the 41 PHRs studied used encryption for data in motion. One site, SparkPeople, had no encryption, which was not consistent with their posted privacy

[237] National Institute of Standards and Technology. (2011). NIST Interagency Report (IR) 7298 Revision 1, Glossary of Key Information Security Terms. Retrieved from http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf.
[238] An analyst can determine whether a website is encrypted by viewing the Uniform Resource Locator (URL) by looking for the "S" in the "HTTPS" of the URL. The "S" shows that encryption using either Secure Socket Layer (SSL) or Transport Layer Security (TLS) is being used. SSL or TLS are cryptographic protocols that force the data through an encrypted channel.

policy that stated that passwords were encrypted. Given its scope limitations, this review could not verify encryption of data at rest in PHRs.[239]

Physical and Administrative Security Policies

During this survey, the authors searched PHR websites for posted security policies or information about security in "Privacy Policies," "Terms and Conditions," or other posted materials such as "Frequently Asked Questions (FAQs)."

Thirty of the PHR sites reviewed made some reference to the importance of security. Some references were general statements such as "the security of your information is important to us." Some websites made more specific statements about security, stating for example that data would be encrypted. Ten of the sites reviewed had a separate security policy document. Sixteen of the sites addressed security in their privacy policy documents. Eight of the sites had scattered information about their security policies and practices. Six of the sites had no information about their security policies and practices.

Physical security measures described in security statements included redundant storage, storage on servers located within the United States, facility surveillance, and limited access to facilities.

Some of the administrative security measures described included role-based access to information, personnel training, and measures for disciplining employees for violations of security or privacy policies. Google Health's policy specifically references role-based access control. The Juniper and Keas PHRs indicate that data is limited to employees with a need-to-know and that there are sanctions for violations of access restrictions. The NoMoreClipboard and People chart PHRs have policies that specify that employees and contractors are bound by confidentiality agreements that restrict access to personal health information.

Instead of storing the PHR information on their own internal servers, some PHRs store data in the "cloud," meaning that they use secure Internet connections to move the data to multiple servers owned and operated by other entities who sell server space, such as Amazon. Of the PHRs reviewed, only the security policy of My doclopedia states that no information is stored offshore. All other PHRs reviewed online were silent on the issue.

Risk Assessment and Audit Capability

HIPAA requires CEs to conduct periodic assessments of risks to identifiable health information in their possession.[240] While this is recognized as a good security practice, non-HIPAA PHRs are not required by law to conduct these assessments. Only a few of the PHR websites surveyed for this report made any reference to whether the vendor engaged in efforts to assess risks or review security policies.

---

[239] Absent a full-scale security assessment against the website, the study could not assess for encryption of data at rest (the data in the PHR vendor's database). This is because the "S" in the "HTTPS" only shows the encryption for the data as it is being sent over the Internet. The "S" does not show how the data is encrypted once it is in the PHR vendor's database.

[240] 45 C.F.R. §§ 164.308(a)(1)(ii)(A),164.306(e), 164.316(b)(2)(iii).

The HITECH Act requires non-HIPAA PHR vendors and associated entities to notify consumers and the FTC of breaches of PHR individually identifiable information.[241] However, the Act does not require FTC to promulgate regulations to require the technological capacity to detect breaches when they happen. Only five of the PHR vendors surveyed referenced audits, access logs, or other methods to detect unauthorized access to identifiable information in PHRs.

Security Considerations Related to PHRs Offered on Smart Devices and Apps

Smartphone or smart tablet vendors are third- party service providers to vendors of apps. This section reviews the security of smart device PHRs by considering both the security of the smart devices and the security of the apps themselves. Security of a smart device can vary based on the method of communication it uses: for example, smart phones are offered through a variety of cell phone services with differing security practices.[242]

Smart devices offer many different security protections to consumers. For example, the iPad offers consumers the option to set a passcode that activates the device's data protection function, including encryption of data at rest.[243] Consumers who set up this function and then forget their password, however, will need to re-install all software on the device in order to be able to use it again.[244]

Some health apps function by allowing an individual to store information locally on the hard drive of the smart device. Others use the smart device as an interface to the Internet. Both types of apps may have their own security policies, apart from that of the smart device.

For apps storing information on the local hard drive of the device, security issues include the possibility that the device may be lost, stolen, or tampered with. Encryption of data stored in the app can be used to protect against these risks, and some PHR apps offer this capability. However, without a secure password recovery process, the data in an encrypted app becomes inaccessible if the user forgets his or her password. This would create a frustrating scenario in which the consumer would need to re-populate all of his or her information into the app under a new account.

Other apps use remote access to the PHR vendor's server infrastructure for information storage and use. In these cases the smart app is functioning as a vehicle through which the consumer accesses the Internet. The security review identified 14 apps that send data to remote storage without any indication that information in transit is encrypted. This presents a security risk to users if hackers gain access to the stream of information through the Wi-Fi connection used by the device or an intermediary in the chain of data transfers on the Internet.

D. CERTIFICATION

Some PHR vendors obtain private sector certifications that allow them to post a certification logo on their websites as a way of demonstrating that they follow accepted industry privacy and security measures.

---

[241] HITECH Act § 13407.
[242] National Institute of Standards and Technology. (2008). *NIST Special Publication 800-124, Guidelines on Cell Phone and PDA Security.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf.
[243] *iPad User Guide*. (n.d.). Retrieved from http://manuals.info.apple.com/en_US/ipad_2_user_guide.pdf.
[244] *Id*.

Certifying organizations such as URAC,[245] HON,[246] and TRUSTe[247] certify websites after reviewing them to ensure they meet their required guidelines. These certification programs primarily address the Fair Information Practice Principles for transparency and purpose specification. The sections below provide a high level description of the standards in each of these areas.

Transparency—Posting Privacy Policies: URAC,[248] HONcode,[249] and TRUSTe[250] require that the website post a privacy policy.

Transparency—Contact Information: All three certification programs require websites to post contact information.

Purpose Specification – Advertising: URAC, TRUSTe and HONcode have different requirements regarding advertising. While TRUSTe does not address advertising, URAC and HONcode require websites to have editorial and advertising or sponsorship policies.

Purpose Specification – Offsite Links: HONcode and TRUSTe do not have requirements that address offsite linkages. URAC Accreditation requires disclosures regarding offsite linking and requires websites to meet four standards for linking, including notification about the relationship between the website and the linked site.[251]

Individual Participation – Consent to Changes to Privacy Policies: URAC, TRUSTe and HONcode have different requirements regarding consents to changes in privacy policies. URAC Accreditation requires that the website not use personally identifiable information or personal health information for any purposes outside the scope of the original opt-in without first obtaining additional opt-in (unless required by law).[252] Under the TRUSTe Program Requirements, TRUSTe must approve any material changes[253] in the participant's privacy statement or privacy practices. Participants are required to post prominent notices on their website for thirty days before implementing any material change. Participants also need to explain how users may exercise their opt-in and opt-out choices with respect to material changes to the privacy policy.[254] HONcode does not address changes to a site's privacy policy.

---

[245] URAC. (n.d.). About URAC. Retrieved from https://www.urac.org/about-urac/about-urac/.
[246] Health on the Net Foundation Non Governmental Organization. (n.d.). The HON Code of Conduct for medical and health websites (HONcode). Retrieved from http://www.hon.ch/HONcode/Conduct.html.
[247] TRUSTe Powering Trust in the Data Economy. (n.d.). About TRUSTe. Retrieved from http://www.truste.com/about-TRUSTe/.
[248] URAC. (n.d.). *Health Web Site Standards*. Retrieved from http://www.urac.org/docs/programs/URACHW2.1factsheet.pdf.
[249] Health on the Net Foundation Non Governmental Organization. (n.d.). *HONCode Principles*. Retrieved from http://www.hon.ch/HONcode/Guidelines/hc_p8.html.
[250] TRUSTe Powering Trust in the Data Economy. (n.d.). *Web Seal Program Requirements*, Retrieved from http://www.truste.com/privacy-program-requirements/.
[251] *Health Web Site Standards*, *supra* note 225.
[252] URAC, Health Content Provider Accreditation Guide, Version 3.0, at 61 (Aug. 2008) (explaining that it is not adequate for a website to change its privacy policy without actively notifying a user of substantive changes in the scope of the privacy policy related to personal health information).
[253] TRUSTe *Web Privacy Seal Program Requirements*, *supra*. Section I(H) defines "material change" as "a change that relates to Participant's 1. Practices regarding notice, disclosure, and use of Personally Identifiable Information and/or Third Party Personally Identifiable Information; 2. Practices regarding user choice and consent to how Personally Identifiable Information and/or Third Party Personally Identifiable Information is used and shared; or Measures for data security, integrity, or access . . . ." *Id.*
[254] Section III(E)(2)(g) explains the requirements for posting the notice, and section III(E)(2)(b) discusses requirements relating to exercising opt-in, opt-out choices. *Id.*

Because each organization establishes its own criteria, the standards vary across certifying bodies. URAC, for example, requires health websites seeking accreditation to notify users before collecting health information or selling health information to third parties. It also requires the health website to certify that its security protocols are sufficient to maintain the privacy of the information it collects. Appendix F describes these certification standards more fully and includes a table showing which PHRs surveyed for this report are certified by each organization. -

Eighteen of the 41 PHR sites surveyed indicated that they were certified by at least one organization. Twelve PHRs were certified by HON, five were certified by TRUSTe, and only one site had URAC certification. HealthString and Microsoft Health Vault were certified by both HON and TRUSTe. WebMD held certifications from all three bodies.

E. CONCLUSION

The survey of privacy and security policies of PHR websites described above finds a great deal of variation in privacy and security policies and practices. The privacy and security policies surveyed do not all cover the same principles or touch on the same requirements, and many remain silent on principles or requirements. As a result, PHRs establish different privacy and security requirements and policies for themselves and provide different protections to consumers. Some PHRs acquire certifications from private certifying bodies to demonstrate to the public that they comply with industry policies or practices. However, each certifying body has somewhat different criteria and requirements to obtain a certification, and thus the acquisition of a certification from one certifying entity does not necessarily mean compliance with the same privacy and security requirements as acquiring a certification from another entity. The variation and differences observed in the privacy and security policies and practices are helpful for establishing a baseline measure of the ways in which PHRs currently operate with regard to privacy and security policies and practices. This baseline measure can help identify common weaknesses in PHR privacy and security practices as well as highlight areas where there is a strong need for uniform policies and/or regulations on privacy and security practices to be implemented.

5. CONSUMER ATTITUDES AND KNOWLEDGE REGARDING PHRs AND PRIVACY

In order to gain a better familiarity with consumer understanding and knowledge of PHRs and consumers' thoughts on privacy when using PHRs, the authors of this study reviewed the results of multiple different surveys on consumer views of these topics. This section draws on the results of surveys conducted by the Markle Foundation and the California Health Care Foundation. The findings are also drawn from the discussions at the ONC PHR Roundtable during which four panels of experts addressed privacy and security requirements of PHRs.[255] ONC also carefully reviewed over 300 public comments it received in response to questions it posted on its website as part of the PHR Roundtable.[256] This section also discusses the results of some general studies of consumers and their thoughts and attitudes toward Internet privacy (i.e., not specific to health information) which may help inform an understanding of consumer attitudes and concerns regarding PHRs. All of these survey results and findings can help identify places where the public believes that gaps exist in current privacy and security requirements for PHRs and the actions or trends that occur with regard to use of PHRs as a result of these perceived gaps. These survey results and findings can also help focus future recommendations for privacy and security requirements so that they align with and help alleviate consumer concerns.

A. CONSUMERS CONSIDER PRIVACY A KEY CONSIDERATION IN PHR USE

A number of different surveys have been conducted to learn the extent to which consumers know about PHRs as well as to determine the reasons that consumers choose not to use PHRs. According to a Markle Foundation study, patients understand the benefits of PHRs but believe that adequate privacy protections are very important.[257] A Markle survey conducted in June 2003 found that over 70% of those surveyed believe that PHRs would improve the quality of health care.[258] In that same survey, however, over 90% of consumers expressed concerns about privacy protections for their data and indicated that privacy protections are key to their willingness to use a PHR.[259] In a June 2008 survey also conducted by the Markle Foundation, 91% of respondents agree that "how my health information is handled online is so important to me that the online services should always require my express agreement for each use."[260]

A survey by the California Health Care Foundation also found that 68% of the 1,849 consumers surveyed between December 18, 2009 and January 15, 2010 were "very concerned" or "somewhat concerned" about

---

[255] ONC Roundtable, *supra.*

[256] *Id.* The four sets of questions and their responses are on file with ONC and with the study authors.

[257] *See, e.g.*, Markle Connecting for Health. (2003) *Americans Want Benefits of Personal Health Records*. Retrieved from http://www.connectingforhealth.org/resources/phwg_survey.pdf; Markle Foundation. (2006). *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care*. Retrieved from http://www.markle.org/sites/default/files/research_doc_120706.pdf; Markle Foundation. (2011). *The Public and Doctors Overwhelmingly Agree on Health IT Priorities to Improve Patient Care*, retrieved from http://www.markle.org/publications/1461-public-and-doctors-overwhelmingly-agree-health-it-priorities-improve-patient-care.

[258] Markle Connecting for Health, *Americans Want Benefits of Personal Health Records*, supra.

[259] *Id.*

[260] Markle Foundation. (2008). *Americans Overwhelmingly Believe Electronic Personal Health Records Could Improve Their Health*. Retrieved from http://www.markle.org/publications/401-americans-overwhelmingly-believe-electronic-personal-health-records-could-improve-t.

the privacy of their health information.[261] Many of those who expressed concern about the privacy of their health information were worried that their health information could be used employers, health insurance plans, or others.[262] In a joint 2008-2009 survey conducted by the American Medical Association and the Markle Foundation, patients and physicians expressed concern about privacy with use of PHRs. "Of those surveyed, 87 to 92 percent of consumers said that privacy protection would factor into their decision to use an online PHR. Similarly, 70 percent of physicians agreed that PHRs may not have adequate privacy protections."[263]

A recurring theme in the PHR Roundtable discussion and the public comments was that PHRs, whether covered under HIPAA or non-HIPAA covered, must be trustworthy enough for individuals to use them in greater numbers.[264]

In addition to their own concerns about privacy, physicians are also concerned that consumers may not fully trust the privacy of PHRs. A survey indicated that although nearly half of physicians thought PHRs would be beneficial to their patients, they were worried about potential inaccuracies in information contained in PHRs due to patient lack of trust in PHRs, resulting liability risks, and additionally they were concerned about the lack of reimbursement for reviewing information in PHRs. [265]

B. THE SOURCE OF A PHR OFTEN DETERMINES CONSUMER TRUST

While individuals are concerned about the privacy and security of their personal health information, many do not fully understand the privacy and security policies for the information in their PHRs.[266] As a result, they may turn to trusted sources such as their health care provider for advice in making a decision about using a PHR based on the assumption that a PHR offered by or recommended by trusted sources will adequately protect their information.[267] With respect to electronic records generally, survey data gathered in late January 2011 from 1000 American adults who had visited a physician or hospital in the past 18 months indicated that consumers trust physicians more than other entities to protect their health care information. However, 49% of those surveyed also felt that EHRs would have a somewhat or significantly negative impact on privacy protections.[268] In terms of PHRs, consumers were most positive about those offered by their local health

---

[261] California HealthCare Foundation. (2010). *New National Survey Finds Personal Health Records Motivate Consumers to Improve Their Health*. Retrieved from http://www.chcf.org/media/press-releases/2010/new-national-survey-finds-personal-health-records-motivate-consumers-to-improve-their-health.

[262] *Id.*

[263] Markle Foundation. (2010). *AMA & Markle Foundation Present PHR Survey Research at HIMSS*. Retrieved from http://www.markle.org/news-events/media-releases/ama-markle-foundation-present-phr-survey-research-himss.

[264] ONC Roundtable, *supra*.

[265] *AMA & Markle Foundation Present PHR Survey Research at HIMSS*, Markle Foundation (Mar. 3, 2010), http://www.markle.org/news-events/media-releases/ama-markle-foundation-present-phr-survey-research-himss; Wynia, Matthew & Kyle Dunn. (2010). *Dreams and Nightmares: Practical and Ethical Issues for Patients and Physicians Using Personal Health Records*. Journal of Law, Medicine and Ethics, 38. Retrieved from https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&doctype=cite&docid=38+J.L.+Med.+%26+Ethics+64&srctype=smi&srcid=3B15&key=75d20d8d53f5c95eb540069b7876b718 National Committee on Vital Health Statistics, *supra*.

[266] *See* ONC Roundtable, *supra*.

[267] *See* ONC Roundtable, *supra*.

[268] Dolan, Pamela Lewis. (March 15, 2011). *Patients trust physicians most to protect personal data*, American Medical News. Retrieved from http://www.amednews.com/article/20110315/business/303159997/8/.

providers, and 58% of the California HealthCare Foundation survey respondents said they want to use a PHR provided by their physicians.[269]

At the PHR Roundtable, Dr. Matthew Wynia, Director of the Institute for Ethics for the American Medical Association, stated that the ethical framework around privacy may be clearer than the legal framework.[270] Dr. Wynia suggested that patient reliance on physicians to provide advice or guidance about PHRs created ethical obligations regarding information they provide that goes beyond HIPAA or FTC regulations.

Consumers may not understand that different privacy protections and policies govern a PHR depending on the entity that provides the PHR. As a result, consumers may assume that a non-HIPAA covered PHR provides the same privacy protections as a PHR provided by a HIPAA covered entity. Consumers may benefit from a common legal framework for privacy and security that is applicable to all PHRs regardless of source.

C. CONSUMERS HAVE GENERAL CONCERNS ABOUT SPECIFIC USES OF THEIR PERSONAL INFORMATION

The FTC has identified several concerns that consumers hold about the privacy of their information.[271] These concerns include:

- Entities tracking consumer behavior: sources of information on consumers and their behaviors have grown. Consumer Internet searches, geographic locations, and purchasing activities can be tracked and combined to both provide services to consumers and to target them for advertising.
- Indefinite storage of information: the rapid reduction in cost of storage and the increase in storage capacity has led to longer retention of data and expanded uses of the data.
- Third-party access to consumer information, especially when proposed uses are commercial: consumers may not understand that the sharing of data with "affiliates" cited in company privacy practices may involve sharing data with a large number of organizations.

D. CONSUMERS MAY NOT UNDERSTAND PRIVACY PRACTICES

PHRs increasingly offer a variety of functions accessed over the Internet, which brings privacy and security concerns about PHRs into the realm of broader-ranging concerns about privacy and security on the Internet. A 2010 study of consumer knowledge of information privacy conducted by University of California's Berkeley Center for Law and Technology suggests that consumers lack knowledge about what it means for a website to have a privacy policy.[272] In a telephone survey of a random sample of American adults, the researchers found that only a small percentage (14%) read privacy policies often, just over a third (36%) read them sometimes, and half of the respondents read them hardly ever or never. Over half (55%) reported being more concerned about Internet privacy now than they were five years ago, largely because they believed they knew more about privacy risks online (48%), had more to lose if their privacy were violated (30%), or had had an experience

[269] *New National Survey Finds Personal Health Records Motivate Consumers to Improve Their Health*, *supra*.
[270] ONC Roundtable, *supra* at 264 (comments of Matthew Wynia, Director, the Institute for Ethics at the American Medical Association).
[271] Federal Trade Commission. (2012). *Protecting Consumer Privacy in an Era of Rapid Change: a Proposed Framework for Businesses and Policymakers*. Retrieved from http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.
[272] Hoofnagle, Chris et al., *How Different Are Young Adults From Older Adults When It Comes To Information Privacy Attitudes & Policies* (Working Paper, 2010). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

that had changed their mind about privacy (17%). These perceptions, however, did not translate into actual knowledge about existing privacy protections. Overall, 75% of respondents were able to correctly answer only two or fewer of the following five true-false questions about legal rights to privacy protection:

- If a website has a privacy policy, it means that the site cannot share information about you with other companies, unless you give the website your permission.
- If a website has a privacy policy, it means that the site cannot give your address and purchase history to the government.
- If a website has a privacy policy, it means that the website must delete information it has about you, such as name and address, if you request them to do so.
- If a website violates its privacy policy, it means that you have the right to sue the website for violating it.
- If a company wants to follow your Internet use across multiple sites on the Internet, it must first obtain your permission.

This lack of knowledge was even more pronounced among young adults; 88% answered two or fewer of the questions correctly and 42% answered none correctly.[273]

This study demonstrates that consumers may believe that the existence of a privacy policy on a website means that their privacy is protected and that they have legal rights to sue if it is not. They may not understand that the policy is a statement of what the company will or will not do with respect to information. This lack of knowledge about what it means to have a privacy policy may explain why some consumers fail to read policies—they believe that the policies protect them, when in fact all that the policies do is explain to them the extent to which they will or will not be protected. For these and other reasons, the 2010 FTC Staff Report on consumer privacy questions the reliance on consumer notice and choice as a primary method for protecting privacy.[274]

While many people place significant value on privacy, and express a desire to protect it, Internet users of all ages often fail to protect their privacy. Cognitive biases, responses to peer pressure, immaturity, lack of transparency in the website's practices, Internet illiteracy, the failure to understand privacy policies, and shifting social norms about online relationships and identities all may play a role in explaining this paradoxical behavior.[275] Default privacy settings that favor uninhibited information uses or disclosures unless individuals opt out, may disproportionately affect consumers who are less familiar with the Internet and thus less adept at changing the default settings.[276] For users of PHRs this lack of understanding may lead individuals to assume that there are privacy protections in place for their health information, when in reality, the data may be disclosed.

---

[273] *Id*.
[274] Federal Trade Commission, *supra*.
[275] *See* Nordberg, Patricia A., Daniel R. Horne & David A. Horne. (2007). *The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors*. Journal of Consumer Affairs, 41. Retrieved from http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2006.00070.x/abstract.
[276] Boyd, Danah & Eszter Hargittai. (August, 2, 2010). *Facebook Privacy Settings, Who cares?*, First Monday, 15. Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/3086/2589.

E. CONCLUSION

In the results of multiple surveys, consumers consistently cite privacy as an important precursor for trusting others with their health information. They also consistently express trust in their own providers when placing their health information in a PHR. Consumers have different levels of understanding of the Internet and of the significance of privacy policies. As a result, the posting of Internet privacy policies is not uniformly effective in informing consumers about ways in which information they submit on websites will be used and disclosed. All of these findings are informative and should be kept in mind when developing future recommendations for privacy and security requirements that can help meet the needs of consumers and adequately protect their privacy.

6. SUMMARY OF FINDINGS AND CONCLUSION

The research described in this paper is part of the work that will be carried out in response to Congress' request in the HITECH Act for the Secretary of HHS, in consultation with FTC, to conduct a study and submit a report on the privacy and security requirements for entities not covered by HIPAA. This research analyzed many different aspects of PHRs. It examined the various definitions and characteristics of PHRs, as well as the legal protections and requirements that apply to both HIPAA and non-HIPAA PHR vendors. It also surveyed the privacy and security practices of non-HIPAA PHR vendors and related entities and identified difficulties for consumers in understanding privacy and security policies as well as privacy concerns that are especially important to consumers. The next paragraph summarizes the findings of this research.

A. SUMMARY OF FINDINGS

The non-HIPAA PHRs reviewed for this survey appear to vary considerably in their approaches to privacy and security. Based on an examination of privacy and security policies listed on the websites reviewed as part of this survey, many of those non-HIPAA PHRs reviewed appear to deviate from FIPPs. The analysis of PHR privacy and security policies and practices identified the following issues:

- Most non-HIPAA PHRs have a notice of privacy practices. Non-HIPAA PHR privacy notices vary in form and clarity, making it difficult for consumers to use privacy practices as a factor in determining which PHR to choose.
- Most of the PHR privacy notices that were reviewed did not provide clear or complete information on how data would be used or shared with others.
- Few PHRs provide consumers with the choice to opt in or opt out of the PHR vendor sharing their data with others.
- PHRs vary considerably in their practices regarding changes, corrections, and deletion of data.
- Security policies are not always specific on issues, such as access controls and methods for detecting unauthorized access.
- PHR user identity proofing relies on data that could be known to others, e.g., date of birth. User authentication practices are limited to user name and passwords and in most cases users could select weak passwords (e.g. less than six characters).
- Consumers may not be alerted when they navigate away from the PHR site to other linked sites with their own privacy and security policies and practices.

Certification through private entities such as URAC, TRUSTe and HON imposes some degree of uniform privacy and security standards on participants and may help assure consumers that their information is protected. However, these organizations vary in their standards, and less than half of the PHRs reviewed held any form of certification. As the standards of the HIPAA Privacy and Security Rules only apply to HIPAA PHRs, these privacy and security certification requirements could play a role in creating uniform requirements and standards for non-HIPAA PHR practices. Based on previous FTC enforcement actions, it is possible that an entity's failure to adhere to the standards of a certifying body by which it has been certified may be considered to be a deceptive practice under section 5 of the FTC Act.

It appears that the privacy and security practices of non-HIPAA PHRs are of concern to consumers. Although a large majority of consumers would like to have the benefits of a PHR, consumers expressed concerns about

privacy in deciding whether to use a PHR. Given that consumers would like to have the benefits of a PHR and believe privacy protections are important when choosing a PHR, the inconsistent privacy and security practices of non-HIPAA PHRs may be a factor inhibiting more widespread use of PHRs.

B. CONCLUSION

This study is intended to inform ONC's preparation of a report to Congress on the privacy and security practices of health entities not covered by the HIPAA Privacy and Security Rules, including PHRs. In identifying the existing privacy and security legal framework for different types of PHRs and the current gaps in both the privacy and security policies of non-HIPAA PHRs and requirements placed on non-HIPAA PHRs, this study aims to provide a foundation for the recommendations that Congress requested relating to the regulation of these specific health entities.

Appendix A
HITECH Provision for a Study and Report on Application of Privacy and Security Requirements to Non-HIPAA Covered Entities HITECH Act §13424(b)(1)[277]

> [T]he Secretary, in consultation with the Federal Trade Commission, shall conduct a study, and submit a report . . . on privacy and security requirement for entities that are not covered entities or business associates . . . including—
>
> (A) requirements relating to security, privacy, and notification in the case of a breach of security or privacy (including the applicability of an exemption to notification in the case of individually identifiable health information that has been rendered unusable, unreadable, or indecipherable through technologies or methodologies recognized by appropriate professional organization or standard setting bodies to provide effective security for the information) that should apply to---
>
> (i) vendors of personal health records;
>
> (ii) entities that offer products or services through the website of a vendor of personal health records;
>
> (iii) entities that are not covered entities and that offer products or services through the websites of covered entities that offer individuals personal health records;
>
> (iv) entities that are not covered entities and that access information in a personal health record or send information to a personal health record; and
>
> (v) third part service providers used by an vendor or entity described [above] to assist in providing personal health record products or services;
>
> (B) a determination of which Federal government agency is best equipped to enforce such requirements recommended to be applied to such vendors, entities, and services providers . . . and
>
> (C) a timeframe for implementing regulations based on such findings.

[277] 123 Stat. 115, 276 (2009) (codified as 42 U.S.C. § 17953(b)(1)).

MAXIMUS Federal Services

Appendix B
Roundtable Participation

ROUNDTABLE: PERSONAL HEALTH RECORDS
UNDERSTANDING THE EVOLVING LANDSCAPE

December 3, 2010: Moderators and Panelists

A full transcript of the PHR Roundtable discussions can be found at: http://www.healthit.gov/policy-researchers-implementers/personal-health-records-phr-roundtable

Panel 1: PHR Origins, Developments, Privacy and Security Practices	
Kathy Kenyon, Moderator	Senior Policy Analyst Office of the National Coordinator for Health Information Technology
Colin Evans	Chief Executive Officer Dossia
Tim McKay, Ph.D., CISSP	Director of Digital Identity Services Kaiser Permanente
Lori Nichols	Director HInet
George Scriban	Senior Program Manager Microsoft HealthVault
Gregory Steinberg, M.D.	President and Chief Executive Officer ActiveHealth Management (Aetna)
Panel 2: New Forms, New Audiences, and the New Challenges of PHRs	
Wil Yu, Moderator	Special Assistant of Innovations and Research Office of The National Coordinator for Health Information Technology
Stephen Downs,	Assistant Vice President, Robert Wood Johnson Foundation (RWJF)
Darcy Gruttadaro, J.D.	Director National Alliance on Mental Illness (NAMI) Child And Adolescent Action Center
John Moore	Chilmark Research
Gail Nunlee-Bland, M.D., F.A.C.E., F.A.C.P.	Interim Chief of Endocrinology Director of Diabetes Treatment Center Howard University
Douglas Trauner	Chief Executive Officer TheCarrot.com

Panel 3: Privacy and Security of Identifiable Health Information in PHRs and Related Technology, the Expectations and Concerns	
Joy Pritts, Moderator	Chief Privacy Officer U.S. Department of Health and Human Services
Robert Gellman, J.D.	
Josh Lemieux	Director of Personal Health Technology Markle Foundation
Lee Tien, J.D.	Staff Attorney Electronic Frontier Foundation
Tresa Undem	Vice President Lake Research Partners
Matthew Wynia, M.D., M.P.H.	Director The Institute for Ethics American Medical Association

Panel 4: Perspectives on Privacy and Security Requirements for PHRs and Related Technologies	
Leslie Francis, Ph.D., J.D., Moderator	Distinguished Professor of Law and Philosophy Alfred C. Emery Professor of Law University of Utah
Loretta Garrison, J.D.	Senior Attorney Bureau of Consumer Protection Federal Trade Commission
Adam Greene, J.D., M.P.H.	Senior Health IT and Privacy Specialist HHS Office for Civil Rights
Robert Hudock, J.D.	Counsel Epstein Becker & Green, P.C.
Frank Pasquale, J.D.	Schering-Plough Professor in Health Care Regulation and Enforcement Seton Hall Law School
Nicolas P. Terry, B.A. (Hons.) Law, LL.M.	Chester A. Myers Professor of Law Saint Louis University School of Law

Appendix C
Privacy Study Findings

PHR VENDORS – PRIVACY STUDY

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
Access My Records	Non-HIPAA; $30/year; $50/ year/couple	Y; 1 E , O, P	TPO=Y LR=Y	N	N	Y	Y	Y	YTW	NR	http://www.accessmyrecords.com/
myActiveHealth	HIPAA and DTC version (offered through Microsoft HealthVault)	Y; 1 P	LR=Y	Y=TCL	N	Y (directed at the HIPAA version, though)	N	Y	YCD YT	NR	https://www.myactivehealth.com/consumer/
CapMed (acquired by Metavante in 2009)	Non-HIPAA; $19.95	Y; 1 CNN	TPO=Y LR=Y	Y=TCL	N	N	N	Y	YCD	NR	http://www.capmedphr.com/
dLife	Non-HIPAA	Y; 1 P	TPO=Y LR=Y	Y=TCL	HONcode	N	Y; may opt out but may take some time to be effective	Y	YCW (by mail or email)	YN YH	http://www.dlife.com/
Dr. I-Net	Non-HIPAA	N (although statements about the importance of confidentiality and privacy are scattered in various documents on the site)	TPO=Y	N	HONcode	N	Y	Y	YCD(except for lab results; some information must be entered by medical professionals)	NR	http://www.drinet.com/
EMRy Stick	Non-HIPAA V2.0 still free, is in Beta	Y; 1, but link is broken (3/19/11)	No statement, but the link to the Privacy Policy is broken (3/19/11)	N, but Privacy Policy link is broken (3/19/11)	N	N	N	N	N, but the link to the Privacy Policy is broken (3/19/11)	YN (Automatically records log information about the users' use of the PHR. Two weeks later it is aggregated with" other data" and is no longer associated account. Does not explain what "other data "is.)	http://phr.emrystick.com/

[278] Y=has a privacy policy; 1=visible with one click from home page; 2=visible with 2 clicks from home page; D=difficult to find, scattered among several documents. CNN=may change with no notice required; E=email notice of material change in privacy policy; P=posted notice of material change in privacy policy; O=consumer must agree to material change in privacy policy before the change becomes effective.

[279] TPO=may use or disclose without consent for treatment, payment or health care operations; PH=may use or disclose without consent for public health purposes; LR=may use or disclose without consent if legally required in the judgment of the PHR vendor. Y=yes, may so use; N=no, may not so use. If the privacy policy stated that any use or disclosure requires consent, this was scored as "N+" for each of these possibilities.

[280] Y=Yes, TCL=in Terms and Conditions/Terms of Service/Legal Disclaimer.

[281] YC=yes with independent consent; Y=yes; N=no.

[282] YCD=may correct or delete information, YCW=correction or deletion must be in writing, YT=may terminate PHR, YTW=terminations must be in writing, K=vendor keeps a copy of deleted information or terminated PHR.

[283] YD=may collect aggregate/anonymized data and defines terms; YN=may collect aggregate/anonymized data but does not defines terms; NR=No Reference to the collection of aggregate/anonymized data; YH=may collect aggregate/anonymized data and explains how data is collected.

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
FollowMe	HIPAA/non-HIPAA	Y; 1 P Note: signup links are broken	N+	Y=TCL	No	Y	Y	Y	No statement	YN	http://www.followme.com/
GlobalPatientRecord	Non-HIPAA; $49.99 plus $19.99 per person/year	Y; 1 P	TPO=Y LR=Y	Y=TCL	N	Y	Y	N	YCD K	NR	http://www.globalpatientrecord.com/
Google Health	Non-HIPAA; many partners	Y; 1 P, O	TPO=Y LR=Y	Y=TCL	N	Y	N	Y	YCD YT	YN(Automatically records log information about the users' use of the PHR. Two weeks later it is aggregated with" other data" and is no longer associated account. Does not explain what "other data "is.)	http://www.google.com/intl/en-US/health/about/
HealthAtoZ (now myOptumHealth)	Non-HIPAA	Y; 1 E, P	TPO=Y	Y=TCL	HONcode	N	Y	Y	YCD	YN	http://myoptumhealth.com
Health Butler	HIPAA/non-HIPAA $15/year Can link to Google Health	Y; 1 CNN	TPO=Y LR=Y	N	HONcode	N	N	Y	YCD	YN	http://healthbutler.com/
Healthe*Tracks*	Non-HIPAA, $24.95	Y; 1 CNN	LR=Y	Y=TCL	N	N	N	Y	No statement	NR	http://www.healthetracks.com/
HealthString	HIPAA/Non-HIPAA	Y; 1 E, P	TPO=Y LR=Y	N	HONcode TRUSTe	N	N	Y	YCD	NR	https://www.healthstring.com/
Juniper Health	Non-HIPAA; also SNS	Y; 1 E, P	TPO=Y LR=Y; also if needed to prevent harm or threats. Will make reasonable efforts to notify unless would violate law or court order	Y=TCL	TRUSTe	N	N	Y	YCD YT	YD	https://juniperhealth.org/

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
Keas	Non-HIPAA (currently free during beta testing) Works with Microsoft Health Vault and Google Health	Y; 2 E, P	TPO=Y LR=Y	Y=TCL	N	N	N	N	YC YT	YD	https://www.keas.com/
LifeOnKey	Non-HIPAA	Y; 1 P	TPO=Y LR=Y	Y	HONcode	Y	Y	Y	No statement	NR	http://www.lifeonkey.com/Solutions/Default.aspx
MedeFile	Non-HIPAA: Premier Plan $249/year	Y; 1 E, P	TPO=Y LR=Y	Y	TRUSTe	Y	Y	Y	YCD	YD (Aggregate definition)	http://www.medefile.com/
MedicalSummary.com	Non-HIPAA; $30. Subscription	Security Policy only; 1	No info	No info	N	No info	No info	No info	No info	No info	https://www.medicalsummary.com/main1.cfm?CFID=3393121&CFTOKEN=22519817
MediKeeper	Non-HIPAA	Y; 1 P	TPO=Y LR=Y	Y	HONcode	N	N	Y	YCD K for 180 days if individual deletes (Privacy Policy) and for 2 years if MediKeeper terminates account (Terms)	NR	http://www.medikeeper.com/healthvault/
MedsFile.com	HIPAA and non-HIPAA	Y; 1 E	TPO=Y LR=Y	Y	N	Y (but appears directed to its HIPAA form)	Y	Y	YCD	NR	http://www.medsfile.com/
Microsoft HealthVault	Non-HIPAA	Y; 1 P	TPO=Y LR=Y	Y	HONcode TRUSTe	N	N	N	YC YT	YN	http://www.healthvault.com/personal/index.aspx
My doclopedia PHR	Non-HIPAA	Y; 1 P	TPO=Y LR=Y	N	N	Y	Y	Y	YCD	YD	https://www.doclopedia.com/Login.aspx

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
MyLife HealthRecord	Non-HIPAA $30.00/year	Y; 1	TPO=Y	Y=TCL	N, but the privacy policy states the website subscribes to the HONcode Principles. However, when the user clicks on the HONcode link, the user is informed the site is not a bona fide HONcode member.	N	Y	Y	YCDW; information must be kept 10 years per NZ and Australian law	NR	http://www.doctorglobal.com/index2.asp
MyMedicalRecords	Non-HIPAA Family $9.95/ month or $99.95/year	Y; 1 P, O	TPO=Y LR=Y	Y=TCL	N	Y	Y	Y	YCD K	YN	http://www.mymedicalrecords.com/
myMediConnect; Passport MD	Non-HIPAA	Y; 2	TPO=Y LR=Y; if subpoena will attempt to notify before disclosing information; may also disclose information if threat of imminent harm to self or others	N	N	Y	N	Y	YCD	NR	http://www.mymediconnect.net/index.php
MyMediList	Website links broken(3/19/11)	None referenced.	Links broken (3/19/11)	Link to Terms of Use broken (3/19/11)	N	Contains a link to CMS's HIPAA website.	Site links will not work, cannot tell (3/19/11)	None referenced	Site links will not work, cannot tell (3/19/11)	NR	http://www.mymedilist.org/

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
NoMoreClipboard	HIPAA and non-HIPAA Fees range from free to $119.95 for Concierge Account for a Family	Y; 1 P	N	N	N	Y	Y for free accounts N for upgraded accounts	Y	YCD	Does not sell patient data, even in aggregate form. From time to time, may collect and summarize non-personal information for internal use, in order to continuously improve service.	http://www.nomoreclipboard.com/
Peoplechart	Non-HIPAA; $29.95/month individual; $69.95 family (up to 4 members)	Y; 1 E, P	TPO=Y LR=Y	N	N	Y	N	Y	YTW	NR	http://www.peoplechart.com/
RelayHealth	HIPAA and non-HIPAA functions	Y; 1 P	N	N	N	N	N	N	Not mentioned	NR	https://www.relayhealth.com/
RememberItNow!	Non-HIPAA	Y; 1 E, P	TPO=Y LR=Y	Y=TCL	N	N	N	Y	YCD	YD (Aggregate)	http://www.rememberitnow.com/
Revolution Health	Non-HIPAA	Y; 1 P	TPO= Y LR=Y	Y	HONcode	N	Y	Y	YCD K	NR	http://www.revolutionhealth.com/
Ringful PHR	Non-HIPAA may be available over the Internet through apps	No privacy information on the site	No info	No info	No info	No info	No info	No info	No info	NR	http://www.ringfulhealth.com/apps/
SmartPHR	Non-HIPAA; subscription price varies with plan; iPhone app version Works with Microsoft Health Vault and Google Health	Y; 1 (Site indicates that a further fact sheet about privacy may be available for plan purchaser)	LR=Y	N	N	Y	N	Y	YCD	NR	http://www.smartphr.com/
SparkPeople	Non-HIPAA	Y; 1 E, P	TPO=Y LR=Y	Y=TCL	N	N	Y	Y	YCD K	YD YH	http://www.sparkpeople.com

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
SynChart	Non-HIPAA; $9.95 (Single); $39.95 (Family)	Y; 1	TPO=Y LR=Y	N, but FAQ link is broken (3/19/11)	HONcode	Y: In disclosure statement: Disclosure as required by HIPAA	N	N	No statement	NR	https://www.synchart.com
TeleMedical.com	Non-HIPAA Registration screen takes you to Relay Health sign-in page. (See RelayHealth row above)	Y; 1 O (but only choice is to terminate use of service)	LR=Y	Y	N, but the site says it subscribes to the HONcode Principles, but when the user clicks on the link to HONcode, the site is not verified as a HONcode-certified site	N	Y	N	YTW	NR	http://www.telemedical.com/
TheCarrot.com	Non-HIPAA This website has changed since the initial review	Y; 1	TPO=Y	Y	N	Y	N	N	No statement	NR	http://thecarrot.com/
VitalChart	Non-HIPAA Website is currently under reconstruction so initial findings cannot be confirmed	Y; 2 P	LR=Y	Y=TCL	N	N	N (As of 3/19/11, all links to pharmaceutical information were being reconstructed)	Y	No statement	YD	https://www.vitalchart.com/
WebMD	HIPAA/non-HIPAA	Y; 1 E, P	TPO=Y LR=Y	Y=TCL	HONcode TRUSTe URAC	N	Y	Y	YCD	NR	http://www.webmd.com/phr
YourHealthRecord	Non-HIPAA Works with Microsoft Health Vault, Google Health	Y; 1 E, P	TPO=Y	Y=TCL	HONcode	N	N	N	No statement	YD	http://www.yourhealthrecord.com/

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
Smartdevice Apps											
ADHD Allies self-assessment tool	Non-HIPAA; on Facebook. Because this is hosted on Facebook, it inherits all of Facebook's privacy settings	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	http://www.facebook.com/ADHDAllies?v=app_17037175766
BodyMedia	Body sensors available for purchase $6.85/month with annual subscription	Y; 1 P Short reference to security practices on the Privacy Statement of the site	TPO=Y LR=Y Registration requires Name, country, e-mail, and DoB	Y=TCL	TRUSTe	No info	N– this is a shopping site for related items and does not appear to advertise	Y	YCW and through web site	NR	http://www.bodymedia.com/Professionals/Reports/Characterization-and-Implications-of-the-Sensors-Incorporated-into-the-SenseWear
Capzule PHR	Non-HIPAA; iPhone app. Website is non-functional.	N – not for the PHR app on the smart phone.	No info	No info	No info	No info	No info	No info	No info	NR	http://capzule.com
Fit-ify calorie tracker	Non-HIPAA; because on Facebook, inherits Facebook's privacy policies.	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	Facebook policies only	http://www.facebook.com/apps/application.php?id=8209307103&v=app_6261817190
HealthFile Plus	Non-HIPAA; iPhone app.	N	No info	No info	No info	No info	No info	No info	No info	NR	http://www.wakefieldsoft.com/healthfile/features.html
HeartWise Blood Pressure Tracker	Non-HIPAA; iPhone app.	N	No info	No info	No info	No info	No info	No info	No info	YN	http://itunes.apple.com/us/app/heartwise-blood-pressure-tracker/id311716888?mt=8
iMensies	Non-HIPAA; iPhone app costs $1.99	P; 1 "iMensies respects your privacy. We never sell, rent, or give away your name, email, address or any other information to anyone. All information provided is used exclusively by iMensies.com."	TYO=Y	Y=TCL	N	No info	No info	No info	No info	NR	http://www.imensies.com/

PHR Vendor	Comments	Privacy Policy; Visibility; notice of change[278]	Use/ Disclosure TPO, PH, LR[279]	Liability Limitation[280]	Certification	HIPAA Mention	Advertising on PHR site	Offsite Links[281]	Correction/ deletion[282]	Aggregate or Anonymized Data Collection[283]	Link to website
iTriage	Non-HIPAA	Y, 1	No info	Y=TCL	No info	No info	Y	No info	No info	YN	http://www.itriagehealth.com/
LiveStrong Calorie Tracker Lite	Non-HIPAA app	Stores locally on the device	No info	No info	No info	No info	No info	No info	No info	No info	https://itunes.apple.com/us/app/livestrong.com-calorie-tracker/id502317923?mt=8?mt=8
MyDS	Non-HIPAA app	Stores locally on the device	No info	No info	No info	No info	No info	No info	No info	No info	No URL link
motionPHR	Non-HIPAA; iPhone app.	Y, 1, CNN Looks like data stored only on handheld	No info	No info	No info	No info	No info	No info	No info	No info	http://motionphr.com/privacy.html
My MS Manager	Non-HIPAA for MS patients	Registration establishes a Ringful PHR; see above	No info	No info	No info	No info	No info	No info	No info	No info	No URL link
My Medical Pro for BlackBerry	Not listed in appworld. No info available online for this.	No info available at all for this.	No info	No info	No info	No info	No info	No info	No info	No info	http://appworld.blackberry.com/webstore/content/9079
Patient Power, Global TeleImaging, LLC	Non-HIPAA, iPhone app.	N	No info	No info	No info	No info	No info	No info	No info	No info	http://gtipatientpower.com/
Ringful Health	Non-HIPAA; smartphone apps.	N	No info	No info	No info	No info	No info	No info	No info	No info	http://www.ringful.com
STAT Depression Screener	No info	No info	No info	No info	No info	No info	No info	No info	No info	No info	http://itunes.apple.com/us/app/stat-depression-screener/id348793894?mt=8
WaveSense Diabetes	Non-HIPAA; iPhone app.	N	No info	No info	No info	No info	No info	No info	No info	No info	http://itunes.apple.com/us/app/wavesense-diabetes-manager/id325292586?mt=8

Appendix D
Security Study Findings

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
Access my Records	Referenced on the privacy page	Request the following: Name, Address, Date of Birth (DoB), e-mail.	Yes, required	Cannot test because it costs money to create an account.	Yes, for registration.	No info	No info	http://www.accessmyrecords.com/
myActiveHealth	Referenced on its own page. Reviewed annually.	Request the following: Name, Gender, zip code, DoB, e-mail.	Username becomes your e-mail address.	Password must be between 6-20 characters and must not contain any spaces. Password must contain at least 1 lowercase, 1 uppercase and 1 number. Password cannot contain your first or last name.	Yes, for registration.	A security statement was available on the site that included reference to access control, encryption, and physical security.	"Among the safeguards that ActiveHealth has developed for this site are administrative, physical and technical barriers that together form a protective firewall around the information stored at this site."	http://www.myactivehealth.com/Portal/Security.aspx
CapMed (acquired by Metavante in 2009)	No reference.	No identification on site until you attempt to purchase a PHR. Billing information is requested.	Cannot create an account without a purchase.	Cannot create an account without a purchase.	Encryption for data in motion not documented Encryption is available when an individual attempts to purchase the online PHR.	No info	No info	http://www.capmedphr.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
dLife	No reference.	Site registration requests Name, DoB, and e-mail.	Required after registering.	6 characters only. No special characters required.	In place for registration and authentication	"We care about the safety and security of your PII. While we take commercially reasonable precautions to safeguard PII provided to us, we cannot guarantee that such information will not be lost, disclosed or accessed by accidental circumstances or by the unauthorized acts of others."	No info	http://www.dlife.com/
Dr. I-Net	Limited. Makes notice of the fact that the site is encrypted using VeriSign SSL.	Site registration requests Name and e-mail address only.	Required after registering.	Created an account with a 1 character password, although security statement says "Elaborate password protection systems are used to prevent any intrusion on your privacy."	In place for registration and authentication.	Limited reference to the site encryption, SSL. Security statement reads: "This site has security measures in place to protect against the loss, misuse, or alteration of the information stored on our database."	Security statement reads: "Dr. I-Net's experience and reputation for thorough user training and responsive technical support also provides an added layer of security.	http://www.drinet.com/
EMRy Stick	Privacy Policy is on a web page that is broken and the error handling is porous at best. (3/19/11)	Site registration requests Name, Gender, DoB, and e-mail.	Required after registering.	8 character minimum password required. The site returned a verbose error message when the creation of a 1 character password was attempted.	In place for registration and authentication.	No security info; link to privacy policy broken.	No info; link to privacy policy broken.	http://phr.emrystick.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
FollowMe	Makes reference to the use of SSL for registration.	Site registration requests Name, DoB, address, and e-mail.	Required after registering.	Cannot tell. Site is broken and returns error when attempting to register.	Encryption is in place for registration, but not authentication.	Makes reference to encryption used during registration, but it doesn't protect authentication after registration has occurred. Security statement reads, "The servers we use to store personally identifiable information are located in a professionally managed co-location facility with state of the art security measures."	No info	http://www.followme.com/
Global Patient Record	Security referenced in the Privacy Statement; makes mention to encryption, but it must be for data at rest, because there is not encryption for data in motion on this site.	Site registration requests Name, DoB, address, employer information, and e-mail.	Yes, required.	Site states that required password length is 0 characters.	None used at all on the site.	"CareData has implemented appropriate security measures in our physical facilities to protect against the loss, misuse or alteration of information that we have collected from you at our site."	Only disclaimers, "CareData has implemented appropriate security measures in our physical facilities to protect against the loss, misuse or alteration of information that we have collected from you at our site."	http://www.globalpatientrecord.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
Google Health	Security controls are referenced on the "Google Health and HIPAA" page. The Google Privacy Center also explains that Google is a "responsible steward of the information we hold." The Google Privacy Policy also references information security.	This site inherits the Google domain's security policy for identification and authentication.	Required after registration.	The complexity requirements that are implemented are the same across all Google platforms.	Yes, entire session is encrypted.	Security control implementations are referenced in the privacy policy. E.g., "We have extensive backup systems in place to protect the integrity of this information. Google's servers are protected by strong physical security at our facilities, including pass codes, locks, and security personnel."	"Procedural safeguards are also in place to secure the health information users store with us. Within Google, only the people who are operating and improving Google Health have access to user information, and they are bound by strict policies to not disclose this information to others, either within Google or to the outside world."	http://www.google.com/intl/en-US/health/about/
HealthAtoZ (now myOptumHealth)	Documented Security Policy on the site.	Site registration requests Name, DoB, address, and e-mail.	Yes, required.	The password must be 8 - 15 characters, including 1 number and no spaces (case sensitive).	Yes, for registration and authentication.	"We have appropriate security measures in place in our physical facilities to protect against the loss, misuse, or alteration of information that we have collected from you at our Site."	No info	http://myoptumhealth.com
Health Butler	No reference.	Site registration requests Name, DoB, address, Gender, height, weight, race and e-mail.	Yes, required.	The password must be 6 characters and contain a number.	None used at all on the site (includes data in motion).	No info	No info	http://healthbutler.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
HealtheTracks	Security policy reads: "You are entering a secure, SSL encrypted website. Whenever you see the padlock at the bottom of a page, secure encryption is being employed for your protection."	Site registration requests Name, DoB, address, payment information and e-mail.	Yes, required.	Cannot test because it costs money to create an account.	Yes, for registration and authentication.	No info	No info	http://www.healthetracks.com/
HealthString	Security policy is presented on the privacy statement.	Site registration requests Name, DoB, address, and e-mail.	Required after registration.	Password must be between 6 and 30 characters.	Yes, entire session is encrypted.	States that uses geographically redundant servers to protect against data loss.	States that limits number of employees with access to information	https://www.healthstring.com/
Juniper Health	Security is referenced in the Privacy Statement.	Site registration requests e-mail and time zone.	Required after registration.	Passwords must be between 6 and 20 characters long.	Yes, entire session is encrypted.	The privacy statement has a security section that references encryption at rest. "We store the personal information you provide encrypted on computer servers with limited access that are located in controlled facilities."	"We restrict access to personal information to Juniper Health employees, contractors, and agents who need to know that information in order to operate, develop, or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations."	https://juniperhealth.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
Keas	The security policy is referenced in the Privacy Statement.	Site registration requests Name, Gender, DoB, and e-mail.	Required after registration.	Password minimum 8 characters, at least 1 letter and 1 digit.	Yes, entire session is encrypted.	The privacy statement has a security section that references encryption at rest. "We store the personal information you provide encrypted on computer servers with limited access that are located in controlled facilities."	"We restrict access to personal information to Keas employees, contractors, and agents who need to know that information in order to operate, develop, or improve our services. These individuals are bound by confidentiality obligations and may be subject to discipline, including termination and criminal prosecution, if they fail to meet these obligations."	http://keas.com
LifeOnKey	The security policy is referenced in the Privacy Policy.	Site registration requests Name, Gender, and State.	Required after registration.	Cannot test because you need to provide billing information to create an account.	Yes, entire session is encrypted.	States that encryption is used; "websites and servers are protected both physically and technologically"	No info	http://www.lifeonkey.com/Solutions/Default.aspx
MedeFile	Formal security policy.	Site registration requests Name, DoB, phone number and e-mail.	Required after registration.	Cannot test because it costs money to create an account.	Yes, for registration and authentication.	Security references to communications security, authentication, and access control. States uses biometric controls for physical access to site.	"site-wide restrictions on resource availability and authentication control for all MedeFile users, staff and support personnel."	http://www.medefile.com/
Medical Summary.com	There is a security link on the page that references their use of encryption.	Cannot test because it costs money to register.	Required after registration.	Cannot test because it costs money to create an account.	Yes, entire session is encrypted.	"[f]irewall protected, dedicated database server which is totally separate from our web hosting server." Access to data server is limited to certain specific IP addresses.	No info	https://www.medicalsummary.com/main1.cfm?CFID=3393121&CFTOKEN=22519817
MediKeeper	Formal security policy.	Site registration requests Name, Gender, email address, a security question and answer, DoB and Zip code.	Required after registration.	6 character minimum.	Yes, for registration and authentication.	Extensive physical protections, e.g. intrusion detection, references.	Extensive administrative security referenced.	http://www.medikeeper.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
MedsFile.com	There is a HIPAA Readiness file on the page that describes how the site complies with the Security Rule.	Site registration requests Name, DoB, phone number and e-mail.	Required after registration.	Password minimum 6 characters.	Yes, for registration, but not authentication.	States "industry standard best practices" and maintain "physical safeguards."	States industry standard best practices with respect to procedural safeguards	http://www.medsfile.com/
Microsoft HealthVault	Security policy is outlined on the site under the Privacy Statement.	Registration is accomplished through the use of a Windows Live ID, which is also used for all other MSN services (i.e. hotmail).	Required after registration.	6-character minimum; case sensitive.	Yes, for various actions, including registration and authentication.	The Privacy Statement speaks to various controls built into the site that allows the user to see access of their records (consent management) Information stored on computer servers with limited access in controlled facilities.	No info	http://www.healthvault.com/personal/index.aspx
My doclopedia PHR	Referenced in the FAQ section.	Site registration requests Name, address, DoB, phone number and e-mail.	Required after registration.	The password must be at least 4 characters long.	Yes, entire session is encrypted.	States will never send information offshore.	No info	https://www.doclopedia.com/Login.aspx
MyLife HealthRecord	Security Policy has its own dedicated page on the site.	Site registration requests Name, Gender, DoB, e-mail, city of residence, and country of residence.	Required after registration.	User Name and Password minimum 6 characters, maximum 32 characters. Letters, numbers and special characters are acceptable.	Yes, for registration and authentication.	The security policy references corporate technical, administrative, and physical safeguards.	No info	http://www.doctorglobal.com/index2.asp

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
MyMedical Record	Security policy is referenced in the Privacy Policy.	Site registration requests Name, e-mail, and payment information.	Required after registration.	Cannot test because it costs money to create an account.	Yes, for registration and authentication.	To prevent loss of information, all data is backed up periodically The security statement references security measures in place to protect the loss, misuse, and alteration of information on the website.	Employees do not have any access to stored data without being given password access.	http://www.mymedicalrecords.com/
myMediConnect; Passport MD	Security is referenced in the FAQ section.	Registration requires name, DoB, address, Gender, and phone number.	Required after registration.	Password must be at least 6 characters and contain no spaces, at least one letter, and at least one number or special character.	Yes, whole session is encrypted.	"All information is kept in a highly secure US based facility, guarded 24 hours a day by armed guards, security sensors, cameras, and multiple levels of security measures."	No info	http://www.mymediconnect.net/index.php
MyMediList	No reference.	Site won't allow registration due to functionality issues.	Site won't allow registration due to functionality issues.	Site won't allow registration due to functionality issues.	Site references 128-bit Security, but since the web server isn't receiving requests for registration, it cannot be determined.	No reference.	No info	http://www.mymedilist.org/
NoMore Clipboard	Security controls are referenced in the Privacy Policy.	Registration requires name, DoB, address, and phone number.	Required after registration.	Passwords and usernames must be between 5-16 characters.	None required for creating a free account.	No reference.	No info	http://www.nomoreclipboard.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
Peoplechart	There is a Security Overview link that outlines an internal security policy.	Registration requires name, DoB, address, Gender, e-mail and phone number.	Required after registration.	Cannot test because it costs money to create an account.	Yes, for registration and authentication.	The Security Overview page references processes and solutions in place to protect the CIA of PII/ PHI. Statement about physical security: "Our "live" or production servers and database are guaranteed 99.9% uptime and protected by a professional and secure data storage facility that is located in disaster-free zone state. The facility includes video surveillance cameras, motion and temperature detectors, and continuously monitoring for online intrusions."	"Ability to assign specific user roles and privileges to each authorized user"	http://www.peoplechart.com/
RelayHealth	Security controls are referenced in the Privacy Policy.	Registration requires Name, DoB, Gender, e-mail, Zip code.	Required after registration.	At least 6 characters, no spaces.	Yes, for registration and authentication.	No info	No info	https://www.relayhealth.com/
RememberIt Now!	Security controls are referenced in the Privacy Statement.	Registration requires Name, DoB, Gender, and e-mail	Required after registration.	Password must be at least 6 characters.	Yes, for registration and authentication.	The security section makes references to secure servers and network firewalls "to help prevent interference from outside intruders."	No info	http://www.rememberitnow.com/
Revolution Health	Security controls are referenced in the Privacy Policy.	Registration requires e-mail address and DoB.	Required after registration.	Passwords must be 8 - 15 characters, including at least 1 letter and 1 number.	Yes, for registration and authentication	None referenced outside of SSL.	No info	http://www.revolutionhealth.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
RingfulHealth	No security policies are posted	Registration requires Name, e-mail	Required after registration	Registrant is sent password to email; allowed to change password, with recommendation of at least 7 characters	No info	No info	No info	http://www.ringfulhealth.com/apps/
Smart phr	The site references a Security Policy Fact Sheet, but the study authors could not locate it.	Cannot test because it costs money to create an account.	Cannot test because it costs money to create an account.	Cannot test because it costs money to create an account.	Yes for purchasing.	No reference.	No info	http://www.smartphr.com/
SparkPeople	Security controls are referenced in the Privacy Policy.	Registration requires DoB, Country, and Zip code.	Usernames must be 6 - 15 characters, no spaces, and authentication required after registration.	6 - 10 characters, no spaces.	No encryption used for any transmissions on the site, but the Privacy Policy indicates the website encrypts the user's password when it is submitted to the website.	The use of multiple network firewalls and other physical safeguards is referenced on the Privacy Statement.	No info	http://www.sparkpeople.com
SynChart	Security controls are referenced in the Privacy Policy.	Cannot test because it costs money to create an account.	Cannot test because it costs money to create an account.	Password must be at least 6 characters long. You must include at least one uppercase letter, lowercase letter, and number.	Yes, entire session is encrypted.	No reference.	No info	https://www.synchart.com
TeleMedical.com	Security controls are referenced in the Privacy Policy.	Registration requires name, DoB, e-mail, Gender, and Zip code.	Required after registration.	At least 6 characters, no spaces.	Yes, for registration and authentication	No reference.	No info	http://www.telemedical.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
TheCarrot.com	Security section makes reference to the use of encryption, but the browser session didn't support any encrypted communi-cations.	Registration requires Name and e-mail.	Required after registration, but you can stay logged in for 2 weeks by checking a box.	Passwords must be 4 - 12 characters.	No encryption used for any transmissions on the site.	References are made to security controls, but the lack of encryption while registering raises concerns about the presence of other security controls. "TheCarrot uses only dedicated servers that are kept locked in a 24-hour-a-day, secure facility in the United States." Also states daily site backups.	No info	http://thecarrot.com/
VitalChart	Security posture is referenced on the privacy Statement.	Registration requires Name and e-mail.	Required after registration.	A 1 character password could be created.	Yes, entire session is encrypted.	References made to technical, contractual, administrative and physical steps to protect against unauthorized access to and disclosure of personally identifiable information. States "We uses security measures to protect against the loss, misuse, and alteration of the information under our control. We store the information in a database in a secure data center." [sic]	"We take technical, contractual, administrative and physical steps to protect against unauthorized access to and disclosure of personally identifiable information."	https://www.vitalchart.com/
WebMD	An extensive Security Policy can be found on the site with multiple sections related to varying processes.	Registration requires an email address, username (can use email address as user login), password, two security questions, Name, DoB, Gender, and Zip code.	Required after registration	Password must be at least 8 characters or numbers; special characters are allowed.	Yes, for registration and authentication	References made to internal security controls on the Privacy Statement page. Geographic redundancy of servers.	Monitors number of employees with access. Also will discipline employees for unauthorized access.	http://www.webmd.com/phr

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
YourHealth Record	Brief encryption statement on the Privacy Policy	Site registration requires Country, State, and DoB.	Required after registration.	Password must be at least 6 characters long.	Yes, for registration and authentication	No references, other than firewall to protect from hackers.	No info	http://www.yourhealthrecord.com
Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps	Smartdevice apps
ADHD Allies self-assessment tool	No info	No info	No info	No info	No info	No info	No info	http://www.facebook.com/ADHDAllies?v=app_17037175766
BodyMedia	Short reference to security practices on the Privacy Statement of the site.	Registration requires Name, Country, e-mail, and DoB	Site appears to be broken. Won't allow for registration as a popup keeps appearing asking you to identify your country of origin. Poor web design.	Unable to test because of non-functional registration process.	Yes for registration but not for authentication	Short reference to the use of network firewalls.	No info	http://www.bodymedia.com/Professionals/Reports/Characterization-and-Implications-of-the-Sensors-Incorporated-into-the-SenseWear
Capzule PHR	No info	No info	No info	No info	No info	No info	No info	http://capzule.com/
Fit-ify calorie tracker	No info	No info	No info	No info	No info	No info	No info	http://www.facebook.com/apps/application.php?id=8209307103&v=app_6261817190
HealthFile Plus	No info	No info	No info	No info	No info	No info	No info	http://www.wakefieldsoft.com/healthfile/features.html
HeartWise Blood Pressure Tracker	No info	No info	No info	No info	No info	No info	No info	http://itunes.apple.com/us/app/heartwise-blood-pressure-tracker/id311716888?mt=8
iMensies tracks periods and moods	No reference	Registration requires Name, e-mail, and password	Required after registration.	1 character password was created.	No encryption used to safeguard password or registration info	No references.	No info	http://www.imensies.com/
iTriage	No reference	No info	No info	No info	No info	No info	No info	http://www.itriagehealth.com/

PHR Vendor	Security Policy	Initial Identification	Authentication	Password Strength	Encryption	Physical Security	Administrative Security	Link to website
LiveStrong Calorie Tracker Lite	Stores all data locally on the device, and has whatever protection the device provides	No info	No info	No info	No info	No info	No info	https://itunes.apple.com/us/app/livestrong.com-calorie-tracker/id502317923?mt=8?mt=8
MyDS	Stores all data locally on the device and has whatever protection the device provides	No info	No info	No info	No info	No info	No info	No URL link
motionPHR	No info	No info	No info	No info	No info	No info	No info	http://motionphr.com/privacy.html
My MS Manager	Registration activates Ringful Health PHR (see above)	No info	No info	No info	No info	No info	No info	No URL link
My Medical Pro for BlackBerry	No info	No info	No info	No info	No info	No info	No info	http://appworld.blackberry.com/webstore/content/9079
Patient Power, Global TeleImaging, LLC	No info	No info	No info	No info	No info	No info	No info	http://gtipatientpower.com/
Ringful Health	No info	No info	No info	No info	No info	No info	No info	http://www.ringful.com
STAT Depression Screener	No info	No info	No info	No info	No info	No info	No info	http://itunes.apple.com/us/app/stat-depression-screener/id348793894?mt=8
WaveSense Diabetes	No info	No info	No info	No info	No info	No info	No info	http://itunes.apple.com/us/app/wavesense-diabetes-manager/id325292586?mt=8

Appendix E
Fair Information Practice Principles

FAIR INFORMATION PRACTICE PRINCIPLES COMPARISON

Fair Information Practice Principles (FIPPs) are a standard framework for analyzing privacy protections. There are different versions of FIPPs, however. The table below summarizes selected FIPPs principles from several versions of FIPPs relevant to this report.

FIPPs Comparison						
Basic Principle	**D-HEW (1973)[284]**	**ONC (2008)[285]**	**FTC Preliminary Staff Report (2010)[286]**	**Department of Commerce Green Paper (2010)[287]**	**Markle[288]**	**Reflected in HIPAA**
Openness and Transparency	There should not be any personal-data record-keeping systems whose very existence is secret	There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.	Notice of what information is collected from consumers and it will be used	Promote increased transparency through simple notices	Communicate policies to participants and individuals. Provide privacy notices to consumers. Involve stakeholders in developing information sharing policies.	Notice of privacy practices under 45 C.F.R. § 164.520
Individual Access	There should be a way for an individual to find out what information about him is in a record and how it is used	Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format	Consumers should have access to data collected about them	N/A	Allow individuals to find out what data have been collected and who has access, and exercise meaningful control over data sharing.	Right to request designated record set under 45 C.F.R. § 164.524. However, may refuse psychotherapy notes; any information if reason to believe harm to patients or others also under 45 C.F.R. § 164.524

[284] U.S. Dept. of Health, Education, and Welfare. (1973). Records, Computer*s, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems. Retrieved from h*ttp://epic.org/privacy/hew1973report/.
[285] U.S. Department of Health and Human Servces, Office of the National Coordinator for Health Information Technology. (2008). Nationwide Privac*y and Security Framework For Electronic Exchange of Individually Identifiable Health Information.* Retrieved from http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__privacy___security_framework/1173.
[286] Federal Trade Commission, sup*ra*.
[287] U.S. Department of Commerce, National Telecommunications & Information Administration. (2010). Commercial Data *Privacy and Innovation in the Internet Economy: a Dynamic Policy Framework.* Retrieved from http://www.ntia.doc.gov//reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf.
[288] Markle Foundation. (2006). The Architecture for Privacy in a Networked Health Information Environment. Retrieved *from http://www.markle.org/sites/default/files/P1_CFH_Architecture.pdf.*

FIPPs Comparison						
Basic Principle	**D-HEW (1973)[284]**	**ONC (2008)[285]**	**FTC Preliminary Staff Report (2010)[286]**	**Department of Commerce Green Paper (2010)[287]**	**Markle[288]**	**Reflected in HIPAA**
Individual Participation and Control	There should be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent	Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information. Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.	Consumers should be given choice about how information collected from them may be used	Clearly articulated purposes for data collection, commitments to limit data uses to fulfill these purposes	Specify the purpose of the data collection effort clearly and make it narrowly suited to the need. Assure that only data needed for specified purposes are being collected and shared. Establish processes to ensure that data are only used for the agreed upon and stated purposes. Establish what data access is permitted for each user.	Distinction between required disclosures, uses and disclosures not requiring authorization, uses and disclosures requiring authorization; limited consumer rights under 45 C.F.R. § 164.522.
Data Quality and Integrity	There should be a way for an individual to correct or amend a record of identifiable information about him	Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.	Consumers should have access to data collected about them [this access may be used by the consumer to check the accuracy of the data]	N/A	Give individuals access to information about them, and the ability to request corrections and see audit logs. Provide that data are relevant, accurate, complete and up-to-date.	Right to request amendment under 45 C.F.R. § 164.526; covered entities need not agree

FIPPs Comparison						
Basic Principle	**D-HEW (1973)[284]**	**ONC (2008)[285]**	**FTC Preliminary Staff Report (2010)[286]**	**Department of Commerce Green Paper (2010)[287]**	**Markle[288]**	**Reflected in HIPAA**
Security	Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data	Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner. Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.	Businesses should take reasonable steps to ensure the security of the information they collect from consumers	Expanded use of robust audit systems to bolster accountability	Establish tools and mechanisms to provide that data are secured against breaches, loss or unauthorized access. Establish tools and approaches for user authentication and access. Establish who monitors compliance with policies and procedures for handling breach. Produce and make available audit logs. Establish mechanisms for complaints. Establish remedies for affected parties to compensate for harm caused by breach.	Security Rule 45 C.F.R. § 164.306.

Appendix F
Certification
PRIVATE SECTOR CERTIFICATIONS AND COMPLIANCE BY PHR VENDORS

Some PHRs reviewed in this report participated in URAC, TRUSTe, and HONcode certification programs. The table below lists the PHR vendors that had received each type of certification.

URAC Accredited as a Health Web Site[289]	TRUSTe-certified[290]	HONcode-certified[291]
WebMD[292]	HealthString[293]	dLife[294]
	Juniper Health[295]	Dr. I-Net[296]
	MedeFile[297]	Health Butler[298]
	Microsoft HealthVault[299]	HealthString[300]
	WebMD[301]	LifeOnKey[302]
		MediKeeper[303]
		Microsoft HealthVault[304]
		myOptumHealth [formerly Health A to Z][305]
		Revolution Health[306]
		SynChart[307]
		WebMD[308]
		YourHealthRecord[309]

[289] URAC (Feb. 15, 2011), http://www.urac.org.
[290] TRUSTe (Feb. 8, 2011), http://www.truste.com/index.html.
[291] HONcode indicates that it subscribes to the principles of the Health On the Net Foundation Code of Conduct. When the user clicks on the link, the user is informed that the site is not a bona fide HONcode member. HONcode, Health on the Net Foundation (Feb. 9, 2011), http://www.hon.ch/HONcode. Another of the surveyed sites, TeleMedical, also states that it subscribes to the HONcode Principles, but when the user clicks on the HONcode seal, the user is taken to a list of the HONcode principles, not to a verification of the HONcode seal. TeleMedical (Mar. 15, 2011), http://www.telemedical.com/principles.htm.
[292] WebMD (Feb. 5, 2011), http://www.webmd.com.
[293] HealthString (Mar. 10, 2011). http://www.healthstring.com.
[294] dLife (Mar. 10, 2011), http://www.dlife.com.
[295] Juniper Health (Mar. 10, 2011), http://www.juniperhealth.com.
[296] Dr. I-Net (Mar. 10, 2011). http://www.drinet.com.
[297] MedeFile (Mar. 10, 2011), http://www.medefile.com.
[298] Health Butler (Mar. 10, 2011), http://healthbutler.com.
[299] Microsoft HealthVault (Feb. 5, 2011), http://www.healthvault.com/personal/index.aspx.
[300] HONcode, supra note 266.
[301] TRUSTe, supra note 265.
[302] LifeOnKey (Mar. 10, 2011), http://www.lifeonkey.com.
[303] MediKeeper (Feb. 5, 2011), http://www.medikeeper.com/home/aboutus/privacy.aspx.
[304] Microsoft HealthVault, supra note 274.
[305] myOptumHealth (Feb. 5, 2011), http://www.myoptumhealth.com/portal.
[306] Revolution Health (Feb. 5, 2011). http://www.revolutionhealth.com/ (site links to everydayhealth.com).
[307] SynChart (Mar. 10, 2011), https://www.synchart.com/.
[308] WebMD, supra note 267.
[309] YourHealthRecord (Mar. 10, 2011), http://www.yourhealthrecord.com/.

These certification programs[310] primarily address the Fair Information Practice Principles for openness and transparency and limited purpose: consumer autonomy. The sections below discuss how the certified PHRs address these requirements.

Openness and Transparency—Posting Privacy Policies

URAC,[311] HONcode,[312] and TRUSTe[313] require that the website post a privacy policy. All of the sites with URAC, HONcode certification or TRUSTe certification are in compliance with this requirement.

Openness and Transparency—Contact Information

All three certification programs require websites to post contact information.

URAC requires a user feedback and complaint mechanism, such as an email address, phone number or postal address, as well as the implementation of a policy for processing the feedback.[314] URAC also requires that a website disclose its practices for users and response times for emails, electronic messages, and other communications transmitted via the website.[315] WebMD offers its users a contact form with which to email the website, a mailing address, and a phone number.[316]

HONcode requires the websites provide a way for visitors to obtain further information in the clearest possible manner and to provide contact forms or email addresses.[317] The website is required to promptly answer inquiries from the website's visitors.[318] Of the twelve HONcode-certified sites, two (dLife and Revolution Health) have an email address for a privacy contact, one (HealthString) has a postal address and phone number for the Chief Compliance & Privacy Officer, and one (SynChart) has an email address for the website's Webmaster. The remaining eight sites have general web forms and/or email addresses users can use to contact the website.

Under TRUSTe, the Privacy Statement must explain how users of the website can contact the certified entity and TRUSTe. The certified entity is required to provide users with reasonable, appropriate, simple, and effective means to submit complaints and express concerns regarding the entity's privacy practices.[319] All of the five TRUSTe certified sites have links to TRUSTe. One of the websites (MedeFile) provides a contact name, postal address, and phone number for questions and concerns regarding the privacy statement and the other TRUSTe certified PHRs provide web forms or email addresses for contact.

---

[310] TeleMedical.com (Mar. 10, 2011), http://www.telemedical.com/. This site indicates HONcode certification. However, for purposes of the analysis in this Appendix, TeleMedical.com is not considered a HONcode certified site as the certification status of the site is not shown on the link to the HONcode website from TeleMedical's posted privacy policy. *See Principles and Policies of Your Telemedical Office*, TeleMedical.com (Mar. 10, 2011), http://www.telemedical.com/principles.htm.
[311] *Health Web Site Standards*, URAC (Feb. 16, 2011), http://www.urac.org/docs/programs/URACHW2.1factsheet.pdf.
[312] *HONcode Principles*, Health on The Net Foundation (Feb. 16, 2011), http://www.hon.ch.HONcode/Guidelines/hc_p8.html.
[313] *Web Seal Program Requirements*, TRUSTe (Feb. 16, 2011), http://www.truste.com/privacy-program-requirements/.
[314] URAC, Health Content Provider Accreditation Guide, Version 3.0 (Aug. 2008).
[315] *Id*.
[316] WebMD, *supra* note 267.
[317] HONcode, *supra* note 266.
[318] *Id.*
[319] TRUSTe, *supra* note 265.

Limited Purpose: Consumer Autonomy—Advertising

URAC, TRUSTe and HONcode have different requirements regarding advertising. While TRUSTe does not address advertising, URAC and HONcode require websites to have editorial and advertising or sponsorship policies.

URAC requires that a website disclose its editorial policy on health content as well as its advertising and sponsorship policies. The website also needs to disclose a sponsor's involvement in selecting or preparing health content that appears on the website.[320] WebMD is in compliance with URAC website standards for advertising and editorial policies.[321]

Under HONcode, advertising policies must explain how the website distinguishes between editorial and advertising content.[322] The site must also explain which advertisements are accepted and any conflict of interest.[323] Of the twelve websites with HONcode certification, four have advertising and editorial policies (WebMD, Revolution Health, myOptumHealth, and dLife). Seven of the sites (LifeOnKey, Microsoft HealthVault, Health Butler, HealthString, MediKeeper, SynChart, YourHealthRecord)[324] do not appear to contain advertising and therefore do not need to have any advertising policies. One site (Dr. I-Net) provides information for potential advertisers but no advertising or editorial policies are provided on the web site for potential members.[325]

Limited Purpose: Consumer Autonomy—Offsite Links

URAC imposes specific transparency requirement regarding offsite linkages. HONcode and TRUSTe do not have requirements that address offsite linkages.

URAC Accreditation requires disclosures regarding offsite linking and requires websites to meet four standards for linking, including notification about the relationship between the website and the linked site.[326] WebMD is in compliance with the URAC linking requirements.[327]

---

[320] URAC, *supra* note 264.
[321] WebMD, *supra* note 267.
[322] HONcode, *supra* note 266.
[323] *Id.*
[324] The following websites indicate that they do not sell advertising space: Health Butler (Mar. 10, 2011), http://healthbutler.com; LifeOnKey (Mar. 10, 2011), http://www.lifeonkey.com; YourHealthRecord, (Mar. 10, 2011), http://www.yourhealthrecord.com.
[325] Dr. I-Net, *supra* note 271.
[326] URAC, *supra* note 264.
[327] WebMD, *supra* note 267.

Limited Purpose: Consumer Autonomy—Consent to Changes to Privacy Policies

URAC, TRUSTe and HONcode have different requirements regarding consents to changes in privacy policies.

URAC Accreditation requires that the website not use personally identifiable information or personal health information for any purposes outside the scope of the original opt-in without first obtaining additional opt-in (unless required by law).[328] WebMD appears to be in compliance with this URAC standard by requiring the user to expressly authorize opt-in for material changes to the privacy policy that involve the use of personal health information.[329]

Under the TRUSTe Program Requirements, TRUSTe must approve any material changes[330] in the participant's privacy statement or privacy practices. Participants are required to post prominent notices on their website for thirty days before implementing any material change. Participants also need to explain how users may exercise their opt-in and opt-out choices with respect to material changes to the privacy policy.[331] The privacy policies of five of the TRUSTe certified sites (HealthString, Juniper Health, MedeFile, Microsoft HealthVault[332] and WebMD[333]) explain how changes to the website's privacy policy can be communicated to the user. WebMD requires the user to expressly authorize opt-in for material changes to the privacy policy that involve the use of personal health information, but does not require the user to expressly opt-in for material changes that expand the permissible uses or disclosures of personally identifiable information allowed by the prior version of the privacy policy.[334] HealthString, Juniper Health, MedeFile, and Microsoft HealthVault[335] do not require express opt-in for any material changes.[336]

HONcode does not address changes to a site's privacy policy. However, examination of the nine sites that are HONcode-certified but not TRUSTe-certified determined that seven of the sites (dLife, Dr. I-Net, LifeOnKey, MediKeeper, myOptumHealth, Revolution Health, and YourHealthRecord) advise users how they will be notified of changes to the privacy policy.

---

[328] URAC, *supra* note 264.
[329] WEBMD, *supra* note 267.
[330] TRUSTE, *supra* note 265.
[331] *Id*. Section III(E)(2)(g) covers the posting of a notice, section III(E)(2)(b) covers the requirements for consumers to exercise opt-in or opt-out choices.
[332] *Privacy*, MICROSOFT HEALTHVAULT (Feb. 9, 2011), http://www.healthvault.com/privacy-policy.aspx.
[333] WEBMD, *supra* note 267.
[334] *Id.*
[335] *See* HEALTHSTRING, *supra* note 268; JUNIPER HEALTH, *supra* note 270; MEDEFILE, *supra* note 272; MICROSOFT HEALTHVAULT, *supra* note 274.
[336] *Privacy*, MICROSOFT HEALTHVAULT, *supra* note 307; *Web Seal Program Requirements*, TRUSTE, *supra* note 288.