Review of the Personal Health Record (PHR) Service Provider Market

Privacy and Security

January 5, 2007

HS691.001.001-01
R. Lecker
D. Armijo
S. Chin
J. Christensen
J. Desper
A. Hong
L. Kneale

Review of Personal Health Record (PHR) Service Provider Market

Privacy and Security

January 5, 2007

Altarum
3520 Green Court, Suite 300 • Ann Arbor, Michigan 48105 • (734) 302-4600

Corporate Headquarters	Alexandria, VA	San Antonio, TX
734 • 302 • 4600	703 • 575 • 1200	210 • 832 • 3000

Preface

This report was developed for the Office of the National Coordinator for Health Information Technology (ONC) by Altarum Institute, a nonprofit research organization. Work was performed under the American Health Information Community (AHIC) Program Support contract; Prime Contract No. GS-10F-0034N, Order No. HHSP233200500217U.

Technical Questions should be directed to:

Mr. Robert Lecker
Director, Health Informatics
Altarum Institute
Tel: (703) 575-1691
E-Mail: robert.lecker@altarum.org
http://www.altarum.org
"Systems Research for Better Health"

Table of Contents

1.0 Statement of Problem

Trust in the privacy and security of the PHR is essential for its successful adoption by consumers. As noted by the National Committee on Vital and Health Statistics:

> "public support … depends on public confidence and trust that personal health information is protected. Any system of personal health information collection, storage, retrieval, use, and dissemination requires the utmost trust of the public. The health care industry must commit to incorporating privacy and confidentiality protections so that they permeate the entire health records system."

Therefore Office of the National Coordinator for Health Information Technology (ONC), in support of the American Health Information Community (AHIC) Consumer Empowerment (CE) Workgroup, requested a thorough review of existing privacy policies to understand what is currently being stated, where improvements could be made, and what outstanding areas of uncertainty still exist around privacy concerns.

2.0 Methodology

2.1 Review of Privacy Policies

Altarum obtained via Web site research 30 privacy policies from current PHR vendors. All privacy policies were retrieved between December 1, 2006 and December 18, 2006. Each policy was then reviewed for content, readability, and other factors. In this report, no individual vendor will be directly identified and identification has not been released to the government.

We sought privacy policies with the following goals in mind:

- Is there a "model" privacy policy—with broad coverage of essential topics—that can then be modified and considered for general adoption and use;
- Are there particular areas of privacy and confidentiality that all PHR vendors should describe in their offerings; and
- Are there some areas that no vendor currently addresses?

While we continue to believe that a model privacy policy is a desirable goal, we find little consensus existing today as to its content, particularly on disclosure of secondary use of data, definition of terms, and ultimate disposition of personal health data should the PHR vendor go out of business.

A descriptive summary of our findings is contained in sections 3.0–3.3. Proposals for elements in a model PHR are described in Section 3.4. A discussion of unresolved policy areas is in Section 3.5.

2.1.1 Definition of Confidentiality, Privacy, and Security

Here we briefly distinguish among "privacy," "confidentiality," and "security." This document uses definitions from the Institute of Medicine publication, *Disposition of the Air Force Health Study* (2006).

Health information **privacy** is an individual's right to control the acquisition, uses, or disclosures of his or her identifiable health data. **Confidentiality**, which is closely related, refers to the obligations of those who receive information to respect the privacy interests of those to whom the data relate. **Security** refers to physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.

Privacy therefore is a right that, if broken, has been violated. Security, by comparison, is a product that may be bought and sold under business contracts. Meaningful levels of security are also wholly dependent on the business rules surrounding the confidentiality and privacy of the data they protect. Data can be completely secure from unauthorized breach, but if authorization allows unlimited duplication and dissemination of underlying data then that security has no meaningful interpretation.

For these reasons, we have focused in this analysis on privacy policies and transparency of business rules regarding secondary use of data, rather than on security features as such. Wide-ranging and in-depth efforts in security, authentication and authorization are already well underway in the healthcare technology and general information technology realms; we direct the interested reader to those studies.[1]

2.1.2 Limitations of the Study

There are several potential gaps in our methodology. First, we reviewed only those privacy policies that were available publicly. The rationale for this is simple: a privacy policy that first requires provision of private data (name, email address, or other contact information) has missed the principle of informed consent. We note that some PHR vendors are not information aggregators; instead they already own the clinical or administrative data presented in the PHR as a Health Insurance Portability and Accountability Act of 1996 (HIPAA)-covered entity and are therefore already restricted in what they can and cannot do with individually-identifiable data. Still, the lack of universal discussion on the use of de-identified data by PHR vendors is notable.

Second, we did not attempt to verify the contact information supplied in each reviewed policy, to determine if the phone number or email address remains current, or to determine how much time is required to receive direct response from a human rather than automated response from a computer or interactive voice recognition system to resolve any questions regarding the policy.

Finally, we make no assertions regarding the general applicability or external validity of this analysis. We attempted to ensure that the major PHR vendors were contained in this analysis, but we do not know how many individuals are in turn covered by these vendors. The growing availability of claims data from insurer portals, for example, means that potentially many millions of consumers have access to these kinds of PHRs, which were not the focus of the analysis in this report.

[1] See, for example, the Liberty Alliance Project for open, federated identify management (www.projectliberty.org), the Initiative for Open Authentication (http://www.openauthentication.org/), the Homeland Security Presidential Directive-12 Interoperability Consortium (http://www.hspd-12.org/), the emerging HITSP Privacy and Security Standards (http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3), and the AHIC Privacy and Security work group, for example the statement of John Macaulay from September 29, 2006 describing identify management and authentication issues (http://www.hhs.gov/healthit/ahic/materials/meeting09/cps/P2-PHR-Macaulay.pdf)

3.0 Data Analysis

Altarum developed a scoring tool for examining all privacy policies. This tool consisted of "yes/no" questions that could be applied against any privacy policy to check for completeness and coverage. Readability was scored from "1" (poor) to "3" (good). We examined a total of 30 policies against 31 criteria in 8 major categories. These categories are detailed in Exhibit 1.

The eight categories are:

- Communication with vendor;
- Readability;
- Coverage;
- Gathering non-personal data;
- Bundled with security policies;
- Detail how/if information is shared;
- Definition of critical terms; and
- Data guidelines or compliant with privacy codes.

These categories are intended to be descriptive of the kinds of information expected in a Privacy Policy, with a particular focus on transparency and informed consumer consent.

Exhibit 1: Evaluation Criteria and Categories

Category	Criteria
Communication with Vendor	Contact Info
	Effective date
	Notification of change in policy
	Opt-in to changes
Readability	Alternative Languages
	Readability (1-3)
	FAQ
Coverage	De-activated accounts?
	Buy/Sell of Company
Gathering non-personal data	Cookies
	Solicit voluntary participation (surveys, etc)
	Web service logs
	Opt-out option, on one or more ways to gather non-personal data
Bundled with security policies?	n/a
Detail how/if information is shared?	Different policy for identifiable vs. de-identified
	Business Associates
	Family Members
	Clinical Trials
	Research
	Marketing
	Law Enforcement
	Other
	Consent Prior to sharing?
Definition of Critical Terms	Personal Health Information
	De-identified
Data guidelines or compliant with privacy codes?	HIPAA
	URAC
	European Union (EU) Safe Harbor Guidelines
	American Medical Association (AMA)
	Health on the Net Foundation (HON)
	VeriSign®

A longer description of each category is provided in Appendix A.

3.1 Coverage by Included Privacy Policy

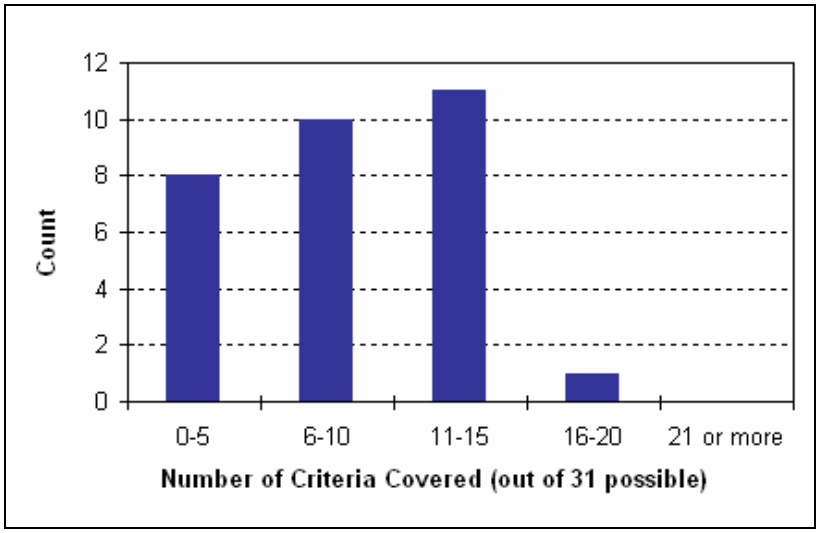
Of the thirty privacy policies reviewed, none covered more than 18 of the 31 criteria we used for review. A criteria was deemed covered if it was mentioned at all in the policy, regardless of the level of detail or whether affirming or denying the relationship to that criteria. Readability was counted as covered if it scored at least a "2" (fair) in assessment. All 29 of the remaining policies (97%) covered 15 or fewer criteria, or less than half of the criteria used. This distribution of criteria covered is shown in Exhibit 2. The average number of criteria covered by the 30 policies reviewed is 8.7; the median number is nine. A complete review of the coverage of all 30 policies is provided in Appendix B.

Exhibit 2: Distribution of Privacy Policies by Number of Criteria Covered

Number of Criteria Covered	Number of Privacy Policies
1	1
2	1
3	2
4	3
5	1
6	3
7	1
8	3
9	0
10	3
11	2
12	4
13	3
14	1
15	1
16	0
17	0
18	1

While the criteria are not equally important, it is clear that no reviewed privacy policy is even approximately complete, and further, there is wide variation in the scope and breadth of the reviewed policies. These data are shown in graphical form as a frequency distribution, in Exhibit 3. The mode (highest point) of this distribution is the range of 11–15 criteria covered. There is a very steep drop off after that point.

Exhibit 3: Distribution of Privacy Policies Reviewed, by Number of Criteria Covered



The analysis of the breadth of each policy thus shows a wide range of interpretation of what constitutes a privacy policy and adequate informed consent to that policy. However, not every criteria or every category is equally important. Therefore, in a second analysis, we reviewed how well individual criteria and categories were covered by the 30 reviewed policies. This distribution is shown in Exhibit 4.

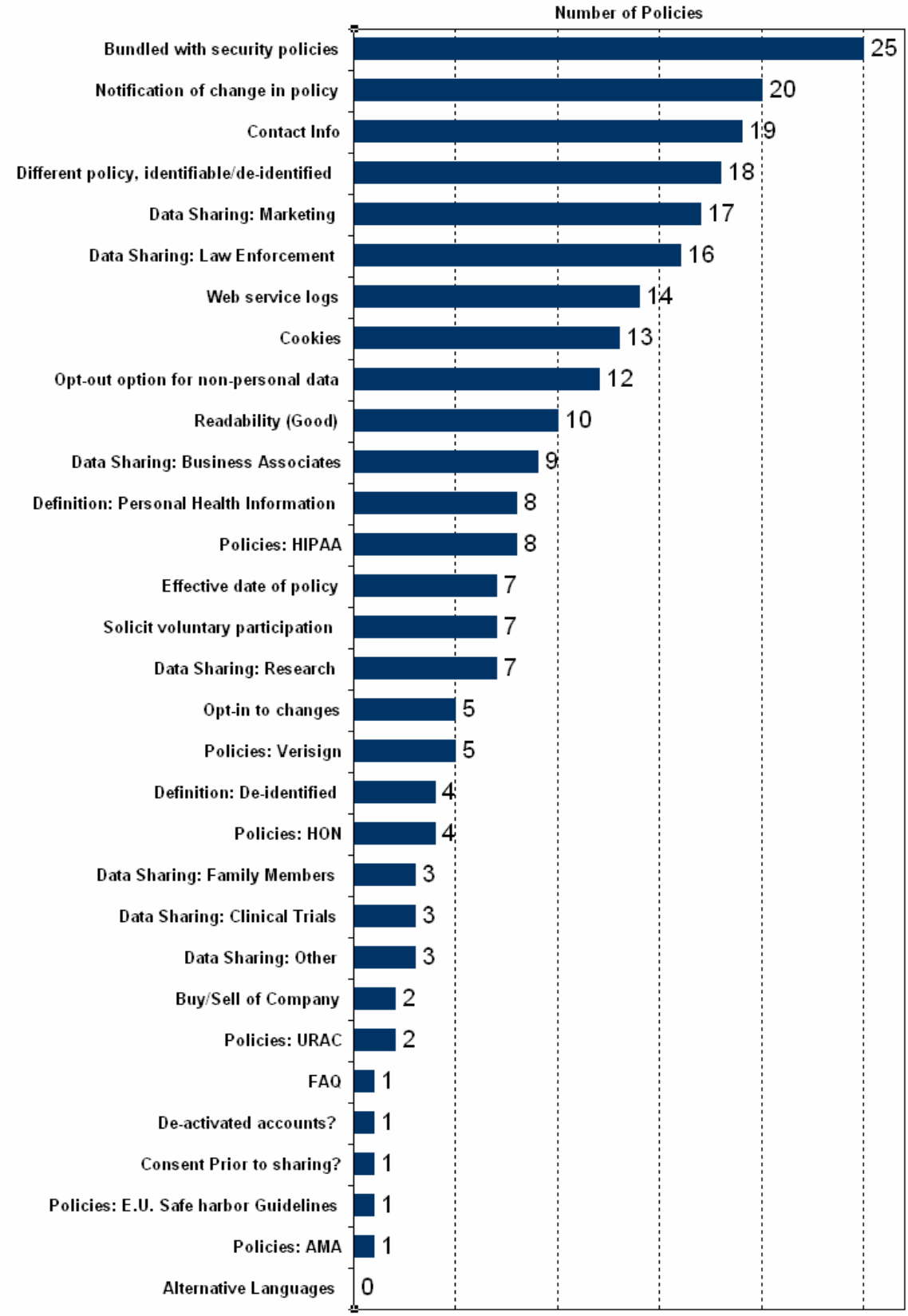
Security was covered by the most policies, with 25 out of 30 (83%) of the reviewed policies bundling security policies into the privacy document. The use of alternative languages was covered by the fewest, with none of the 30 (0%) privacy policies reviewed offering the document in a language other than English.

Surprisingly, only one policy (3%) stated that explicit consumer consent was necessary prior to the vendor sharing any of the data in the PHR (an "opt-in" only approach).

No policies named the vendor's existing data partners, third-parties or other secondary users of the PHR data, whether de-identified or not, nor were data elements that might be shared explicitly described in any of the reviewed policies.

Two vendors (7%) described the ultimate disposition of data should the vendor be sold or go out of business, and one (3%) described their policy with respect to de-activated accounts. The disposition of PHR data is a critical area of trust, as there is substantial turnover in the PHR market and uncertainty regarding the ability of the organization or its debtors to sell assets such as the database of customer information, up to and including identifiable clinical data.

Exhibit 4: Coverage of 31 Criteria by Reviewed Policies



Data sharing also lacks transparency among reviewed policies. Generous scoring criteria were used, so that any discussion of potential data sharing or of policies enabling or explicitly prohibiting third-party sharing was counted as coverage. Even so, only:

- Seven policies (23%) discussed research use of data;
- Three (13%) discussed use of data in clinical trials; and
- Three (13%) discussed access to data by family members.

Sixteen privacy policies (53%) discuss possible release of data to law enforcement; although this is the largest category covered, it is not clear what possible alternative is contemplated by the 14 policies (47%) that did not discuss this potential for compelled release of data.

3.2 Coverage by Criteria

We also examined data at the category level; this is summarized in Exhibit 5. If at least one criterion in any category was covered, then that category was considered to be covered by that reviewed policy. Even with this generous scoring, we find far less than 100% coverage of the relevant categories.

Exhibit 5: Coverage of Categories by Reviewed Policies

Category	Total Policies That Cover This Category	Percent of Total
Communication between vendor and user	22	73%
Coverage of inactive accounts	2	6%
Collecting user data	19	63%
Sharing of user data with non-health care entities	23	76%
Definition of terminology	11	36%
Adherence to published guidelines or codes	14	46%
Bundled with security policies	25	83%

As Exhibit 5 shows, and as noted in Exhibit 4, the Bundling of Security and Privacy was covered by the largest number of vendors, with over 83% indicating some coverage of this concept. Sharing of User Data was second with 76%, while Communication Between User and Vendor was third.

3.2.1 Communication Between Vendor and User

This category addresses communications between vendor and user as specifically applied to the privacy policy. For example, does the policy provide a specific contact for additional questions; does it provide the date the policy went into effect; and does it describe how the users are notified if the privacy policy changes? At 73%, most vendors we reviewed touched on some aspect of communications with the user regarding privacy policy. While that is a high percentage, we would expect all

vendors to provide a mechanism for answering users' questions and to be very clear about how users are notified of changes.

3.2.2 Coverage: Inactive Accounts or Vendor Ceases Operations

As noted elsewhere, the PHR market is immature and rapidly evolving. As has been witnessed in the EHR space as well as other evolving technology markets, some vendors will not survive and will merge with other vendors or leave the business. Likewise, customer loyalty will likely be low especially in the early, formative stages and many accounts will become inactive as users move to other vendors or allow their accounts to lapse. These are two situations that create additional unwanted exposure of personal health data. As seen in Exhibit 5, only 6% of the vendors we reviewed address the issue of user data residing in either inactive accounts or with organizations no longer doing business.

3.2.3 Collecting and Sharing of User Data

That "Collecting and Sharing of User Data" were topics addressed by such a high percentage of vendors is positive and an indication that they are aware of how much these issues resonate with users. As service providers, there may be good reasons to collect certain non-personal data to aid in systems administration. Of the vendors' privacy policies we reviewed, 63% indicate that they do collect non-personal user data, examples of which include IP addresses, demographic and profile data. There appears to be some confusion here by vendors, who describe Internet privacy policies for information collected by interaction with the Web site (cookies, Web logs) rather than privacy policies for the PHR data, however collected.

More problematic and central to privacy and confidentiality is the "Sharing of User Data with Non-Health Care Entities." At issue here is whether or not the service provider makes user data available to third parties (e.g., sponsors, business partners) for secondary purposes. In our analysis, 76% of the vendors addressed third-party data sharing in some form in their published privacy policies.

The largest categories of named third parties for data sharing are Law Enforcement and Marketing. While it remains unclear whether PHR data is discoverable under the law, most vendors recognize that they can be compelled by subpoena or court order to release user data to law enforcement. The large number in the Marketing category is a strong indicator of the evolving nature of business models for PHR vendors. As there is no clear technology or market share leader in the PHR market, it is too soon to tell whether subscription or license fee models will generate enough revenue to support service providers. As a result, vendors may see sales or lease of user data in some form as a source of additional revenue. One vendor's policy addressed this issue directly:

> To defer the costs of bringing you the service, we may at times distribute aggregate information about our members to sponsors, advertisers or business associates, but we will never personally identify you.

A second vendor also addressed the issue directly but with a different perspective:

> [Vendor] understands that the security of your medical and personal information is our highest priority. [Vendor] will continually strive to ensure that any and all information on this website will remain secure. [Vendor] will never sell, lease, rent or share your personal information, except in a case where the law might demand it.

Sharing of user data, even for purposes of advancing public health, present at least two major privacy challenges. First, the data in PHR repositories is most likely not stored in a de-identified form. The service provider must take steps to create a de-identified and aggregated database before it leaves their data center. For those service providers who are not covered entities under HIPAA, there is no requirement that they take those steps. They may find it more cost-effective to send their PHR database to one of their business partners or sponsors under a sell or lease arrangement with the understanding that the third party will extract and use only aggregated and de-identified data. And second, since these are personal health records that likely contain data entered by the user, data quality and accuracy issues may reduce the value of the data for scientific analysis. This second issue serves to reinforce the Marketing category as the most likely third party source of revenue from sharing user data and help explain why the Marketing category in Exhibit 4 is more than twice as large as the Research category.

3.2.4 Definition of Critical Terminology

Healthcare and privacy terminology often contains language with precise technical meanings but imprecise general use and interpretation. At the most basic level a common understanding of "personal health information," as defined by HIPAA, is critical to informed consumer consent to the PHR vendor's privacy policy. As shown in Exhibit 6, only 26% of vendor privacy policies defined "personal health information," and only 13% defined "de-identified personal health information." The general lack of technical glossaries and Frequently Asked Question sheets among reviewed privacy policies is notable.

Exhibit 6: HIPAA Referenced as an Industry Standard

Vendor Privacy Policy	Number of Vendors	Percent of Total
Provides a definition of "personal health information"	8	26%
Provides a definition of "de-identified personal health information"	4	13%
Specifically references HIPAA	8	26%

3.2.5 Adherence to Published Guidelines or Codes

Referring back to Exhibit 5, the 46% coverage of this category appears deceptive. One of the published guidelines included in this category is HIPAA, and the 14 vendors that did mention some guideline include the 8 that referenced HIPAA (Exhibit 6). Of the remaining vendors, 4 referenced HON and 5 mentioned VeriSign, neither of which are privacy guidelines.

Covered entities under the HIPAA statute are required to protect personal health information, but many PHR service providers are not covered entities and there is no statute or standard that defines PHR service providers' legal responsibilities. Even less clear are the legal restrictions on third parties who are the business partners with the PHR service provider. As a final area lacking clarity, it is entirely unknown what requirements may be placed on offshore or non-US based companies.

The National Committee for Vital and Health Statistics (NCVHS) has stated that "privacy measures at least equal to those in HIPAA should apply to all PHR systems, whether or not they are managed by covered entities." HIPAA provides a usable baseline and starting point for privacy protection of individually identifiable health data in the PHR, as it is in common usage and implementation throughout the healthcare industry.

However, in our examination of PHR vendors' privacy policies we note with interest that only eight vendors (26%) specifically reference HIPAA. The following quote is illustrative:

> While [Vendor] is not required to comply with HIPAA, [Vendor] has used the HIPAA regulations as a guideline for its own policies and procedures with respect to your protected health information, as such term is defined in the FAQ's.

We would have expected more vendors to at least reference HIPAA in a way similar to the vendor quoted above. Since the legal landscape is so unclear on the privacy requirements of PHR service providers, it would make sense that many of them would use HIPAA as a guideline in formulating their policies. In addition there could be significant marketing advantages from referencing HIPAA, as many users, providers and payers are familiar with it.

3.2.6 Bundled with Security Policies

This is the category with the highest coverage among those reviewed with 83% of vendors publishing a bundled privacy and security policy. As detailed earlier in this document, privacy and security are different concepts and should be treated separately. Simply put, the security tactics (tools and technologies) that are implemented by a PHR service provider should be driven by the privacy policies that detail an individual user's rights to control his or her personal health data. These results are another indication to us that the vendors we reviewed either do not fully understand the difference between privacy and security or have chosen not to clearly explain the difference in their published policies.

3.3 Summary of Descriptive Analysis

The descriptive analysis provides interesting insights into the privacy policies of the PHR vendors examined. First, the reviewed privacy policies are incomplete. No policy covered more than 18 of the 31 criteria used for evaluation, and twenty-nine of 30 policies reviewed (97%) covered 15 or fewer criteria—less than half the total number of criteria. The least descriptive policy covers only 1of these criteria. Furthermore, a number of highly important criteria, including whether or not any

identifiable or de-identified data are provided to business associates, are very poorly covered by the privacy policies we reviewed. Out of 30 policies, only nine (30%) directly addressed secondary use of data by business associates, even if only to say that there is no secondary use, and only slightly more than half (16, or 53%) note that the PHR data may be released to law enforcement.

Second, we note some confusion among privacy policies among three related concepts: the privacy policy of the PHR vendor's Web site, the privacy policy of the PHR vendor with respect to PHR data, and the security procedures used to protect those data. Seventeen of the 30 policies reviewed (57%) describe the use of cookies or Web logs on the vendor's Web site. Such policies properly cover only those personal data received over the Internet via customer interaction with the vendor Web site, as described by Fair Information Practices or Federal Web site privacy policies mandated by the Office of Management and Budget.[2] While Internet privacy policies are important, they are separate from, and largely secondary to, privacy policies regarding the personal health data held in a PHR. The conflation of the two may create confusion in the mind of the consumer, intentionally or not.

Security procedures are also widely covered by the reviewed policies, and in some cases are the only content of the privacy policy. This is also a potential source of confusion to consumers, who may believe that their personal health data are protected from any release, when in fact no such privacy policy may be in place. Security policies should be clearly separated and held distinct from the business rules describing who may be authorized to view or use the data held in the PHR.

Lastly, we note some substantial gaps in all reviewed privacy policies:

- No privacy policy we reviewed named any business associates who might receive identifiable or de-identified health information.
- No privacy policy provides for a notice to be sent to the PHR customer when identifiable or de-identified data are sold or transferred to a third party.
- No privacy policy reveals to the customer what data have been so transferred.
- No privacy policy was available in multiple languages or indeed in any language other than English.

3.4 Requirements for a Model Privacy Policy

Relevant source documents for a model policy include the FTC Fair Information Practice definitions (provided in Appendix C), the OMB model Internet privacy policies for Federal Web sites, and other private efforts to define and describe appropriate levels of privacy protection for individually-identifiable and de-identified data not currently in the public domain. Examples of the latter include Daniel Solove and Chris Jay Hoofnagle's "A Model Regime of Privacy Protection" and Charles Safran, et al's "Toward a National Framework for the Secondary Use of Health

[2] United States Federal Trade Commission (1998) *Privacy Online: A Report to Congress*. June 1998, Section III "Fair Information Practice Principles"; Office of Management and Budget (1999) *Privacy Policies on Federal Web Sites* M99-18, June 2, 1999.

Data."[3] Due to the limited nature of this report, we do not provide a thorough review of relevant policy, pending legislation, or the legal history of privacy protections, although such a review is warranted by the nature of the question.

We note two important concepts. First, there is no current consensus on the appropriate role of government in the development, enforcement, and maintenance of privacy policies in general or in the PHR market. A notable example occurred in the FTC 2000 report to Congress, where a split committee recommended statutory requirements for privacy enforcement but the chairman vehemently dissented.

Second, there is no consensus among consumers or vendors regarding the core set of principles that should underlie PHR privacy policies. With or without statutory requirement or Federal guidance, the leadership of PHR vendors deriving from a fundamental impetus from consumers is likely essential to successful implementation and protection of privacy in the PHR market. Absent such consumer demand, it is difficult even to say whether the observed poor coverage of privacy criteria by the policies we reviewed truly constitutes a problem or not. What we do note is that PHRs contain much of the same information covered by HIPAA, even if the PHR vendor is not itself a HIPAA-covered entity. It would appear to be an inconsistency in the legal framework to have rigid restrictions on, for example, the secondary use of data by some kinds of PHR vendors but not others.

That being said, our review of existing privacy policies, Fair Information Practices, and other proposed privacy models suggests that the following areas should at a minimum be covered by any PHR privacy policy. We recognize that this is an area of discussion for the vendor, provider, and consumer communities, but put forth this straw man to further this conversation.

PHR privacy policies should:

- Be required for all PHR vendors;
- Be available at all times for review without any requirement that the reader first provide personal information (including name, email address), so that the consumer can make an informed choice prior to releasing any data to the vendor;
- Provide current contact information and date when policy went into effect, and inform the consumer of any changes in the policy, so that consumers can resolve any questions they may have with respect to the policy and know what rules are in effect at any given point;
- Provide transparency on any secondary data use: make available to consumers all business partners to whom Personal Health Information or de-identified data is sold or transferred, in aggregate or on an individual basis;

[3] Solove, Daniel and Chris Jay Hoofnagle (2006) "A Model Regime of Privacy Protection" *Illinois Law Review*, Vol. 2006, p. 357, 2006 and http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881294; Safran, Charles, Meryl Bloomrosen, W. Edward Hammond, Steven Labkoff, Suzanne Markel-Fox, Paul Tang, and Don Detmer (2006) "Toward a National Framework for the Secondary Use of Health Data" A Report of a working conference of the American Medical Informatics Association (http://www.amia.org/inside/initiatives/healthdata/finalpapertowardanationalframeworkforthesecondaryuseofhealthdata_09_08_06_.pdf).

and, describe the potential release of individually identifiable data to law enforcement or others in the course of e-discovery of medical records. Because of the enormous potential for harm to individuals from the disclosure of Personal Health Information to litigants, employers, insurers, or the community, special protections must be established for these data, and particular care must be taken to prevent "back door access" to HIPAA-protected data via the PHR. At a minimum, PHR vendors should give consumers complete transparency on the release of PHR data to any third-party;

- Disclose or make available to consumers all business relationships relating to the handling, processing, data mining, or other management of PHR data, whether identifiable or not;
- Disclose any financial or other business relationships with any promoted or offered services, so that individuals can make informed choices regarding their use of these services;
- Describe special protections offered for minors, although these may by necessity vary by State and locality;
- Describe the relationship of the vendor's policies to HIPAA requirements, Privacy Act, e-discovery, and other relevant Federal rules and regulations;
- Provide readable (e.g., 6th-grade reading level) descriptions and a glossary of all technical terms used in the privacy policy; and
- Be separate and distinguishable from the Internet privacy policy associated with the vendor's Web site, and be separate and distinct from descriptions of the security provided by the vendor to protect the PHR data and enforce this privacy policy.

While not exhaustive, we believe this list provides a starting point for a minimum essential privacy policy with necessary consumer transparency. Whether or not an opt-in or opt-out policy is required for secondary use of data, at a minimum consumers should know whether or not the vendor intends to sell or otherwise transfer de-identified or individually identifiable data to any third parties. Finally, we note the importance of private-sector efforts in branding or use of "seal of approval" third parties to provide enforcement mechanisms for these privacy policies. Where the law is silent or established case law does not exist, other mechanisms including open descriptions of authorized secondary uses of data are required to maintain informed consumer consent and the essential trust relationship between consumers and PHR vendors.

3.5 Areas for Further Discussion

At the same time, our analysis shows a number of topic areas for which there does not appear to be a current consensus or usage. We describe these in this section as areas that might be taken up by the AHIC Consumer Empowerment Workgroup for discussion and resolution.

- Should the consumer be informed every time there is any secondary use of the data, for example sale of aggregated data to a pharmacy benefits manager for utilization review?
- Should all current third-party users of de-identified or individually identifiable data be explicitly named by the PHR vendor?
- Should the consumer be required to explicitly opt-in prior to any transfer or sale of individually identifiable PHR data?
- Should the vendor be required to notify all consumers of any change in privacy policy? Should a written copy of the privacy policy be mailed to every PHR customer on a periodic basis, as is required for consumer credit?
- Should vendors be required to notify all affected consumers in the event of an accidental privacy breach? What if that breach takes place in a business partner, an Application Service Provider (ASP) vendor, or other third party? Must the data involved in the breach be provided to consumers affected?
- Should a history of the vendor's privacy breaches, accidental disclosures, or other unauthorized access or viewing of PHR data be provided to all PHR consumers, perhaps on demand?
- Should a seal of approval or other privacy certification or audit of privacy policies be developed, and provided by a non-profit consortium, government agency, or for-profit firm?
- Should vendors be required to provide privacy policies in multiple languages?
- Should rules regarding asset ownership, destruction and disposal of Protected Health Information (PHI) data be developed, for cases where the vendor goes out of business, is taken over, or otherwise loses control of its assets to debtors, lenders or a court?
- Should rules be developed to require that consumers be able to close their PHR accounts and be assured that any data they contain has been destroyed and will not be subject to any further re-use?
- Should all vendors be required to be able to document their chain-of-custody process for all PHR data they may hold, perhaps for audit or other investigatory purposes?
- Should all PHR vendors be covered under HIPAA?

Again, this list is not exhaustive, but is intended to act as an initial set of problem areas that will require some resolution in the policy arena, by the private sector, government, or some collaborative arrangement among all parties.

4.0 Conclusion and Recommendations

Our review of 30 publicly available privacy policies revealed wide variation in understanding and implementation. We also note that not every PHR vendor Web site has a publicly available privacy policy, and we found more than one instance of privacy policies that could only be reached after enrolling and providing private information such as an email address.

We draw the following conclusions from our analysis:

- Based on our analysis of 30 PHR vendors, existing privacy policies are incomplete;
- Consensus requirements for the contents of a PHR privacy policy do not yet exist, and many vendors appear to have focused instead on security procedures and Internet privacy descriptions;
- Transparency of secondary use of data could be greatly improved;
- The majority of vendors reviewed did not reference HIPAA;
- Data disposal rules and regulations are ill-defined, especially for closed accounts and vendors that go out of business; and
- Many specific terms including "personal health information" are not defined in the privacy policy or related documentation.

We therefore make the following recommendations:

- Privacy, in the context of the PHR, should have a commonly-understood meaning among all vendors, healthcare providers and consumers;
- Consumers and vendors will need to establish a forum to develop a common understanding of the most important components of a PHR privacy policy, especially on the level of transparency in secondary use of data; and
- There is a clear role for the AHIC work groups to help define a "model privacy policy" for the PHR industry, an ideal form against which other policies can be compared, as for example OMB provided for the Federal Web site privacy policy.

Appendix A: Description of Categories and Criteria Used for Evaluation

Exhibit A-1: Attributes of Vendor Privacy Policies

Attribute	Scope
Communication between vendor and user	Is there a specific contact or contact address to whom users can address questions concerning the privacy policy? Does the policy show the date the policy went into force? Does the published policy address whether or not users are notified when the policy is changed? Are users given the option of opting-in to new privacy policies affecting their personal health information or staying with the current policy?
Readability	Is the privacy policy written in plain language wording understandable to users of average literacy? Does the published policy contain a frequently asked questions (FAQ) section? Is the privacy policy available in another common language (Spanish, French, etc.)?
Coverage of inactive accounts	Does the policy address the treatment of accounts whose contract with the vendor has lapsed? Does the policy address the treatment of personal information if the company goes out of business or is bought?
Collecting user data	Does the policy address the use of cookies (small pieces of code placed on the user's computer by the vendor)? Does the policy discuss situations where the user may be asked to voluntarily provide information in the form of surveys or similar vehicles? Does the policy address the use of Web service logs to track user activity? Does the policy address whether users are given an option to opt-out of responding to solicitations of information?
Sharing of user data with non-health care entities	Does the policy address whether or not user data is shared with the following entities and what types of data are shared? • Vendor's business partners or associates including potential advertisers or for vendors' marketing purposes • Users' family members • Health care research including public health and pharmaceutical • Legal entities including law enforcement or the courts • Another third party not specified? • Is consent required prior to sharing information to third parties?
Definition of terminology	Does the policy define "personal health information?" Does the policy define "de-identified personal health information?"
Adherence to published guidelines or codes	Does the policy address adherence to published security or privacy guidelines, codes or recommendations? Are any of the following specifically mentioned? • HIPAA • URAC • EU Safe Harbor Guidelines • AMA • HON • VeriSign
Bundled with security policies	Is the published privacy policy bundled with a published security policy?
Approximate length in Web pages	How long – in published Web pages – is the privacy policy?
Comments	Does the vendor provide any additional comments regarding features or functionality of their privacy policy?

Appendix B: Evaluation of 30 Privacy Policies

		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD
Communication with Vendor	Contact Info																														
	Effective date																														
	Notification of change in policy																														
	Opt-in to changes																														
Readability	Alternative Languages																														
	Readability (1-3)	1	2	3	2	2	1	3	2	2	2	2	2	3	2	3	2	2	2	3	3	2	3	2	2	2	3	1	2	3	3
	FAQ																														
Coverage	De-activated accounts?																														
	Buy/Sell of Company																														
Gathering non personal data	Cookies																														
	Solicit voluntary participation (surveys, etc)																														
	Web service logs																														
	Opt-out option																														
Detail how/that information is shared?	Different policy for identifiable vs. de-identified																														
	Business Associates																														
	Family Members																														
	Clinical Trials																														
	Research																														
	Marketing																														
	Law Enforcement																														
	Other																														
	Consent Prior to sharing?																														
Definition of Critical Terms	Personal Health Information																														
	De-identified																														
Data guidelines or compliant to any privacy codes?	HIPAA																														
	URAC																														
	EU Safe Harbor Guidelines																														
	AMA																														
	HON																														
	VeriSign																														
Bundled with security policies?																															
Approx. Length (pages)																									15						
Total Coverage		1	3	18	8	11	4	8	12	10	11	6	13	3	8	10	12	5	10	6	4	2	7	13	14	12	6	4	12	15	13

Red indicates the category was not addressed in the published privacy policy	Green indicates the category was addressed in the published privacy policy	Yellow (2) indicates a published privacy policy of moderate readability; Red (1) indicates poor readability; Green (3) indicates good readability

Appendix C: Fair Information Practice Principles

Source: Federal Trade Commission (1998) *Privacy Online: A Report to Congress* and http://www.ftc.gov/reports/privacy3/fairinfo.htm . Note that (unlinked) footnotes in this document have been retained; the reader is referred to the above Web site for those references.

III. Fair Information Practice Principles

A. Fair Information Practice Principles Generally

Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection.(27) The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.(28) Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

1. Notice/Awareness

The most fundamental principle is notice. Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.(29) Moreover, three of the other principles discussed below -- choice/consent, access/participation, and enforcement/redress -- are only meaningful when a consumer has notice of an entity's policies, and his or her rights with respect thereto.(30)

While the scope and content of notice will depend on the entity's substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

* identification of the entity collecting the data;(31)

* identification of the uses to which the data will be put;(32)

* identification of any potential recipients of the data;(33)

* the nature of the data collected and the means by which it is collected if not obvious (passively, by means of electronic monitoring, or actively, by asking the consumer to provide the information);(34)

* whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information;(35) and

* the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data.(36)

Some information practice codes state that the notice should also identify any available consumer rights, including: any choice respecting the use of the data;(37) whether the consumer has been given a right of access to the data;(38) the ability of the consumer to contest inaccuracies;(39) the availability of redress for violations of the practice code;(40) and how such rights can be exercised.(41)

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web. To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. Choice/Consent

The second widely-accepted core principle of fair information practice is consumer choice or consent.(42) At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information -- i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.(43) Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.(44) Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.(45)

3. Access/Participation

Access is the third core principle. It refers to an individual's ability both to access data about him or herself -- i.e., to view the data in an entity's files -- and to contest that data's accuracy and completeness.(46) Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.(47)

4. Integrity/Security

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.(48)

Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.(49) Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data; limits on access through use of passwords; and the storage of data on secure servers or computers that are inaccessible by modem.(50)

5. Enforcement/Redress

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.(51) Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.(52)

a. Self-Regulation(53)

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).(54) Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;(55) external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.(56) A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.(57)

Appropriate means of individual redress include, at a minimum, institutional mechanisms to ensure that consumers have a simple and effective way to have their concerns addressed.(58) Thus, a self-regulatory system should provide a means to investigate complaints from individual consumers and ensure that consumers are aware of how to access such a system.(59)

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.(60) Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.(61) The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;(62) and the elements of any such cause of action.

c. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.(63) Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.(64)

Appendix D: Abbreviation and Acronym List

AHIC	American Health Information Community
AMA	American Medical Association
ASP	Application Service Provider
CE	Consumer Empowerment
EU	European Union
EHR	Electronic Health Record
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act of 1996
HON	Health on the Net Foundation
NCVHS	National Committee for Vital and Health Statistics
OMB	Office of Management and Budget
ONC HIT	Office of the National Coordinator for Health Information Technology
PHI	Protected Health Information
PHR	Personal Health Record
URAC	Independent, nonprofit organization promoting health care quality through its accreditation and certification programs (formerly incorporated as the "Utilization Review Accreditation Commission")