Personal Health Records:

An Industry Primer from the Privacy and Security Perspective

SNIP
Personal Health Records: An Industry Primer from the Privacy and Security Perspective
Working Draft Version 7.0 – July 2007

SNIP Security and Privacy Workgroup

Workgroup for Electronic Data Interchange
12020 Sunrise Valley Drive., Suite 100, Reston, VA 20191
(t) 703-391-2716 / (f) 703-391-2759

Contents

Disclaimer

While all information in this document is believed to be correct at the time of writing, this document is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by the Workgroup for Electronic Data Interchange. The listing of an organization does not imply any sort of endorsement and the Workgroup for Electronic Data Interchange takes no responsibility for the products, tools, and Internet sites listed.

The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by the Workgroup for Electronic Data Interchange (WEDI), or any of the individual workgroups or sub-workgroups of the Strategic National Implementation Process (SNIP).

Document is for Education and Awareness Use Only

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security and Privacy requirements are designed to be ubiquitous, technology neutral and scalable from the very largest of health plans, to the very smallest of provider practices. As the Privacy Rule and Security Rule relate to policies and procedures, many covered entities will find compliance not an application of exact template processes or documentation, but rather a remediation based on a host of complex factors unique to each organization.

White Paper Background and Overview

Many consumers are now offered a Personal Health Record (PHR) through their employer, health plan, or provider. Additionally, there are a number of vendors currently offering PHRs on the internet that consumers can independently create and maintain. This increased activity relating to PHRs is part of the increasing focus on of one of the latest healthcare industry initiatives: consumer driven healthcare. WEDI SNIP Security and Privacy co-chairs and others recognized a need to gather current information regarding personal health records and organize it in a practical way in order to assist the industry in understanding the general PHR evolution.

During the past few years, President George W. Bush has called for greater interoperability of electronic medical records and personal health records. This greater interoperability is possible only when base security and privacy controls first lay a foundation for securing and protecting health information. As a result of President Bush's initiatives, ASTM International began to set a standard to change the way in which healthcare professionals preserve and transfer healthcare information about their patients. The standard, E 2369, Specification for Continuity of Care Record (CCR), was developed by Subcommittee E31.28 on Electronic Health Records, which is under the jurisdiction of Committee E31 on Healthcare Informatics.

E 2369 represents a major step forward in assisting vendors and healthcare organizations in their search for simple, yet powerful tools that will help meet the president's objectives.

- The extensible markup language (XML) is the format for structuring CCR information. By the virtue of XML, the information would be both human readable and computer interpretable at the same time.
- In simplistic terms, the information contained within a CCR is XML data conforming to a specific schema.
- And as such, that information is not only be importable into a clinical system but also exchangeable between otherwise incompatible clinical systems.

The Continuity of Care Record (CCR) is a core dataset to be sent to the next healthcare provider whenever a patient is referred, transferred, or otherwise uses different clinics, hospitals, or other providers. To put this into perspective, the American Academy of Family Physicians (AAFP) lists on their web site (http://www.aafp.org/online/en/home.htmlover thirty vendors that have developed the CCR into their products to facilitate interoperability and transportability, including various PHR software development businesses.

PHRs will likely serve as a valuable resource for consumers and their providers. However, the security, privacy, and clinical use aspects of PHRs have yet to be fully addressed. For example, many vendors offering PHRs do not appear to be covered by HIPAA or similar regulations. Also, it is yet to be seen whether or not PHRs will gain widespread acceptance of consumers or providers.

As mentioned previously, there are multiple types of organizations that offer PHRs. The following table summarizes the different types and provides a brief description of each. This table is expanded in the "Personal Health Record Overview" section of this white paper to include information on the use, access, and maintenance of PHRs from each perspective.

	PHR Sponsor	Where the Data Resides
Untethered		
	Paper File	Traditional paper file
	Portable Electronic Media	Medical identifier containing expanded information or carried computer memory
	Personal Computer Based	PHR organizing software on a home PC, not externally linked and not generally portable
Tethered		
	PHR Vendor	Data held by a company whose sole functions are records or data storage and retrieval
	Employer	Data held by a company who may also hold other personal data not covered by HIPAA
	Healthcare Provider	Data held by a provider who does hold other HIPAA protected personal data. This "PHR" may be only limited patient access to an existing record.
	Health Plan	Data held by a company which does hold other HIPAA protected personal data. May be a collection of data from various providers. This "PHR" may offer limited patient access to an existing record.

Consumer Perspective on Personal Health Records

-After all, it is MY information isn't it? – Consumer Perspective

Patients of today's technology-driven generation, who use the computer to research their own symptoms on the Internet, and who pay close attention to the news reports of increasing data errors, and what these errors mean in terms of morbidity and mortality, are increasingly interested in maintaining their health information independently of healthcare providers.

The first PHR may have begun simply as an attempt to make a paper copy of lab results or a provider's diagnosis. But after a while, a quickly progressing technical environment enables one to bring a USB storage device to the provider and ask for a download. In addition to wanting independent access to their health information, today's patients are annoyed by the frequent redundant questionnaires the providers have them fill out and are concerned that they might omit some important historical detail on one form or another.

This generation's youngest school children are often taught via computers. Many people prefer to send an email and allow someone to respond in their own time rather than having to wait on the phone or leave a voicemail message during office hours. Hence there is a heightened need and consumer expectation for automation. This is further enhanced by the job force and deletion of middle management and administrative support. Why ask someone else to schedule something when I can do it myself? It is therefore only natural that many of today's healthcare patients have chosen to keep track of their own healthcare progress via a personal health record. It saves time (not having to verbally tell your story multiple times) in this fast paced society while allowing the consumer more control.

Provider Perspective on Personal Health Records

-After all, it is MY job to be sure patients get the very best healthcare available. I need to know the data is accurate and current, and I need to be able to make accurate clinical decisions. It is my legal and ethical responsibility. – Provider Perspective

Providers have long been conscientious of their role as trusted custodians of patients' personal health information. Until the recent development of non-provider-based health records, such as PHRs, payer-based health records, employer-sponsored health records, and provider-based health records, providers were the sole source for a longitudinal record of a patient's clinical care and treatment. Five years ago, a provider would have likely defined a "PHR" as the patient.

The increasing focus on consumer driven healthcare has facilitated the growing interest in PHRs. Providers may wish to encourage patients to create a PHR for the patient's personal use to track their medical care and treatment and share with their family for emergency situations. Although there may be many benefits for the patient to maintain PHRs, the PHR has also raised many questions and concerns from the provider's perspective, such as what is the appropriate use of a PHR in the provider setting related to coordination of care.

Health Plan Perspective on Personal Health Records

-As a health plan, we have a responsibility and a business pressure to deliver and promote the use of personal health records for consumer use. – Plan Perspective

Today's health plan is feeling the pressure not only to participate in the consumer driven healthcare initiative, but also to leverage this new product/technology to improve on basic plan functions and activities such as the following:

- Helping to raise member awareness of their own health status
- Monitoring and assuring that the most appropriate and cost effective care is provided (not duplicative or unnecessary)
- Participating in consumer driven healthcare

Other Perspectives on Personal Health Records

-As a vendor of a computer system which contains healthcare information, what better way to offer additional value to my customers than to develop a PHR? - Vendor Perspective

A great many PHR products are available in today's environment. However, PHRs are a fast moving target. Standards are in development – but not yet crystallized. There are many organizations in the industry that recognize the value of PHRs and have developed workgroups to research and define standards relating to the security and privacy of PHRs. This white paper provides an overview of the various types of PHRs and offers information about how PHR data is used and maintained from differing perspectives. The various privacy and security aspects of PHR and what regulations, if any, currently govern their use are then discussed. Finally, information from some of the major efforts currently to standardize the use, content, and functionality of PHRs is summarized and referenced. This is not an attempt to define or even make recommendations for standards of privacy and security relating to PHRs. It is intended to summarize efforts currently underway.

NOTE: It is also important to note that most of these efforts are currently in progress and the information presented in this document is only providing what has been done to date. The reader should utilize the references to the various workgroups to find the latest information on the status of each effort.

Definitions

The definitions provided here are for use within this white paper and should not be considered final standardized definitions. These are simply a compilation of definitions from various industry groups currently working on PHR initiatives that have been reviewed by the workgroup participating in the development of this document. They are described here to help clarify the understanding of the current usage. Many of these terms have evolving meanings. For now, from here, this is what it looks like.

At the end of many descriptions is a note as to at least one place where the term used as described.

Computerized Provider Order Entry (CPOE):

Refers to a computer-based system of ordering medications and often other tests. Physicians (or other providers) directly enter orders into a computer system that can have varying levels of sophistication. Basic CPOE ensures standardized, legible, complete orders, and thus primarily reduces errors due to poor handwriting and ambiguous abbreviations. Almost all CPOE systems offer some additional capabilities, which fall under the general rubric of Clinical Decision Support System (CDSS). Typical CDSS features involve suggested default values for drug doses, routes of administration, or frequency. More sophisticated CDSSs can perform drug allergy checks (eg, the user orders ceftriaxone and a warning flashes that the patient has a documented penicillin allergy), drug-laboratory value checks (eg initiating an order for gentamicin prompts the system to alert you to the patient's last creatinine), drug-drug interaction checks, and so on. At the highest level of sophistication, CDSS prevents not only errors of commission (eg, ordering a drug in excessive doses or in the setting of a serious allergy), but also of omission. (For example, an alert may appear such as, "You have ordered heparin; would you like to order a PTT in 6 hours?" Or, even more sophisticated: "The admitting diagnosis is hip fracture; would you like to order heparin DVT prophylaxis?") (Agency for Healthcare Research and Quality, http://psnet.ahrq.gov/glossary.aspx#cpoe)

Electronic Health Record (EHR): Provider centric and controlled by providers or hospitals, these records keep track of the care given to the patients in a clinical setting. EHR may be oriented toward multiple venues of clinical care. They are usually comprised of pulling data from various other data sources (EMRs, CPOEs, etc.). (University of Texas, LBJ School of Public Affairs) (DHHS, Summary of Nationwide Health Information Network: Request for Information Responses, June 2005)

Electronic Medical Record (EMR): Provider centric and controlled by providers or hospitals, these clinical records keep track of the care given to the patients in a clinical setting. Generally synonymous with EHR, EMR may be oriented toward billing. (University of Texas, LBJ School of Public Affairs)

Health Information Exchange (HIE): The technology infrastructure that a RHIO would use.

Health Insurance Portability and Accountability Act (HIPAA): A law passed in 1996 which is also sometimes called the "Kassebaum-Kennedy" law. The Administrative Simplification provisions of the HIPAA (Title II) required the Department of Health and Human Services (HHS) to establish national standards for electronic healthcare transactions and national identifiers for providers, health plans, and employers. It also addressed the security and privacy of health data. As the industry adopts these standards, the efficiency and effectiveness of the nation's healthcare system will improve through the use of electronic data interchange.

Nationwide Health Information Network (NHIN): As its name implies, the NHIN is an overarching network that will connect many Health Information Networks within the nation. Thus, it is envisioned as a network-of-networks.

Personal Health Record (PHR): Patient centric and largely controlled by individuals, these records are generally more life-based than incident based, transcend venues of care, and are intended to be longitudinal records of an individual's health history. While a provider may hold all the records about a specific medical incident in a patient's life and some relevant medical history gathered at the time of treatment. A PHR is generally more focused on collecting at least some information on all of a patient's medical events and may include diet, relevant family medical history, daily logs of responses to medication, and almost anything else a person may wish to include.

They may be paper files, electronic copies carried on memory chips, or computer based, and may be accessible on the internet.

Protected Health Information – means information, including demographic information, whether oral or recorded in any form or medium, that relates the individual's health, health care services, or payment for services and which identifies the individual. (This includes information that 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 includes information that could reasonably be used to identify the individual, such as social security number or driver's license number, even if the name is not included). Protected health information does not include the following:

1. Records covered by the Family Educational Right and Privacy Act
2. Employment records held by the covered entity in its role as employer. (HIPAA Regulation)

Regional Health Information Organization (RHIO): Typically nonprofits, these organizations orchestrate the electronic exchange of information among area hospitals and other providers, with the consent of the patients. They choose standards and protocols for the electronic exchange of information.

Tethered PHR (see also Untethered): Tethered and Untethered are terms used to describe the continuum from the data that is used to populate a PHR data sets that are completely stand alone (untethered) to those that are to some degree linked (tethered) to provider, health plan, pharmacy or payer controlled data sets. Tethered PHRs create some particularly complex

access and validation questions. (National Health Information Infrastructure Workgroup, Nov. 12, 2004) Tethered PHRs are a form of the integrated model that connect with a single provider-based EHR system or other institutional database, offering patients access to parts of their electronic health records or claims data and pharmacy via web portals. Tethered PHRs are pre-populated from existing electronic sources of personal health data on an individual

Untethered PHR (see also Tethered) : Tethered and Untethered are terms used to describe the continuum from PHR data sets that are completely stand alone (untethered) to those that are to some degree linked (tethered) to provider or payer \
controlled data sets. Untethered PHRs create some particularly serious security questions. These PHRs typically require individuals to directly enter their health data into the PHR. (National Health Information Infrastructure Workgroup, Nov. 12, 2004).

Personal Health Record Overview

What Is a Personal Health Record?

In the definitions section of this document, we defined a "Personal Health Record" as follows:

"Patient centric and largely controlled by individuals, these records are generally more life-based than incident based, transcend venues of care, and are intended to be longitudinal records of an individual's health history. A provider may hold all the records about a specific medical incident in a patient's life and some relevant medical history gathered at the time of treatment. A PHR is generally more focused on collecting at least some information on all of a patient's medical events and may include diet, relevant family medical history, daily logs of responses to medication, and almost anything else a person may wish to include."

They may be paper files, electronic copies carried on memory chips, or computer based, and may be accessible on the internet."

A PHR differs from other types of medical data in who creates it, who maintains it and who has access to it. A medical record is typically created, used, and maintained by the health care provider. Access is limited based upon applicable state and federal regulations. An electronic health record, or EHR, is built upon the medical record and may include decision support. The EHR and electronic medical record (EMR) are both legal records.

A PHR is typically created and maintained by the individual, and access to the PHR is controlled by the individual. Depending on the type of PHR, access may strictly be in control of the individual, who can allow or restrict access as they see necessary. Additionally, much of the information updated on the PHR can be entered and updated directly by the individual without going through a provider. The PHR can be a consolidation of multiple medical records, or claims information, or just based on input from the individual.

Types of PHR

There are many types of PHRs. Because networked services are primary drivers of innovation in consumer health Information Technology (IT), PHR products are typically categorized by the degree of integration with other health information systems. Today, there are two dominant PHR models:

Standalone or free-standing PHRs are often computer-based and require manual data entry to populate and update the record.

Integrated, interconnected, or networked PHRs can be populated with patient information from a variety of sources, including EHRs, insurance claims, pharmacy data, and home diagnostics and can provide consumers with a more complete view of relevant health information. **Tethered** PHRs are a form of the integrated model that connect with a single provider-based EHR system or other institutional database, offering patients access to parts of their electronic health records or claims data via web portals.

PHR Types		
	Standalone (Does not connect with other systems)	**Integrated (Connects with potentially unlimited sources of health data)**
Media	▪ Paper-based ▪ Computer-based ▪ Data storage device ▪ Web-based	▪ Web-based
Value to Consumer	▪ Helps organize and store medical data ▪ Provides anytime/anywhere access ▪ Enables information sharing with providers	▪ Includes all "Standalone" values, plus: ▪ Provides access to provider-based records ▪ May eliminate manual re-entry of data ▪ Enables an additional patient-provider communication channel ▪ May reduce medical errors, eliminate duplication, and improve quality ▪ Enhances efficiency and convenience with online transaction tools ▪ Promotes a more comprehensive view of health status and healthcare activity

Source: Kaiser Permanente Institute for Health Policy, Realizing the Transformative Potential of Personal Health Records, *In Focus*, Spring 2007

PHR Functions

Consumers recognize PHRs for their design features, including basic electronic tools that help people collect, organize, and store their health information. More advanced PHRs (particularly those with digitally networked services) offer additional functions such as the following:

- Access to medical records
- Ability to make or change appointments
- Patient-provider secure email
- Retrieval of laboratory and other tests
- Ability to refill prescriptions
- Drug interaction checking
- Interactive health risk profiling and patient education resources
- Prevention and wellness reminders
- Claims viewing and payment processing
- Ability to review insurance eligibility and benefits
- Decision support for health benefit selection
- Out-of-pocket costs modeling
- Deductible or health savings account status

Types of Organizations that Offer PHRs

The following table summarizes the product or service offering of the various stakeholders that are promoting PHR adoption and use.

Stakeholders	Product or Service Offering
Health Systems & Provider Groups (Including Hospitals)	Offering patients a " portal" to their medical information along with additional online functionality
Healthcare Payers (same as Health Plans)	Promoting PHR tools that encourage consumers to be more active in self care and to coordinate their care among providers
PHR Vendors & Service Providers	Offering PHR products and services in networked and non-networked environments
State and regional initiatives (i.e., RHIOs)	Including consumers in regional health information exchange
Health Plans (same as Healthcare Payers)	Offering consumers claims-populated health record systems and online transaction functionality
Employers	Offering electronic tools to help employees manage their health.

History of the PHR

The concept of a PHR came about as the need for a central mechanism by which all pertinent information about an individual's health can be stored. PHR development originated primarily as an employer (purchaser) driven tool – not for consumer driven health care per se, but for improving self care and assessment thereby reducing health care costs. In today's society, an individual may see many different providers in their lifetime. There are multiple areas of specialties an individual may need to see – pediatrician, ophthalmologist, dermatologist, or orthopedist, just to name a few. Even if a person does not see multiple specialists, they may need to see different providers for other reasons such as change in jobs, change in insurance, a move to a new city, or need for urgent/emergent care.

Prior to the development of the PHR, an individual might have tried to keep hard copies of their own medical records in a file or tried to request transfers of their medical record between each provider. However, the more providers a person sees, the more tedious it gets to maintain this information, and in many cases, the individual may choose not to bother to keep up with it. As a result, various pieces of their medical records are scattered throughout multiple provider's offices and there is no central consolidated point by which a complete medical record for the individual can be viewed. As more advances are being made in medical research, we are finding that it is indeed very important to have a complete medical record in order to make a proper diagnosis for almost any condition. PHR systems strongly feature decision support tools and are often aimed at patients with chronic diseases as a way to improve their adherence to diet, lifestyle, exercise, medication management and related issues.

Ideally, the single goal of the PHR is to facilitate the sharing of an individual's health information to and between providers to supply a complete and accurate view of his/her medical background. Various organizations such as medical providers, health plans, employers, and even

independent vendors have recognized the value of this type of sharing of information, and as a result, have begun to create their own mechanisms for a consumer to set up his/her own PHR. The availability is rapidly growing and today, a quick Internet search will quickly find many different options for the creation of a PHR. Even online bookstores offer a USB jump drive specifically designed to store an individual's medical data so that it is portable and can be carried around with the person.

How is PHR Data Used and Maintained?

Any classification of PHRs is going to be inevitably imprecise. They are still quite new and there are already endless variations available. Perhaps the most critical distinction is the degree to which the PHR holds or is linked to external medical data. Existing regulations do not appear to exercise any control over what an individual may do with his/her own data. However, once that data is handed over to a provider "for the purposes of treatment," the data is HIPAA protected data if the provider meets the definition of "covered entity". PHR structures that make data viewable from a computer when the data may be held in a combination of provider based networks and local personally controlled computer files make the issue really complex.

In general, information covered under HIPAA regulations does not lose its protection when appropriately shared. However, information released to the patient loses all protections. Patients may do anything they wish with their copy of their own data. If a patient takes possession of the data, that copy is unregulated.

	PHR Type	Control	Regulated (See Codes)
Untethered			
	Paper File	Strictly Individual	0
	Portable Electronic Media	Strictly Individual	0
	Personal Computer Based	Individual[C1]	0
Tethered			
	Specialty Provider	Vendor? Wide variety possible [C2]	0
	Employer	Shared individual and employer [C3]	2
	Medical Provider	Clinician/Provider, may or may not have patient control [C2]	1
	Health Plan	Health Plan, may or may not have patient control [C2]	2

Control Codes;

C1 - May have some provisions for remote access and may allow importing some medical data.

C2 - A wide variety of data import/export options may exist. These are significant because what is shared and by whom may alter what regulations apply.

C3 – Varies depending on how it is set up by the employer. In some cases, employer may have access and control. In other cases, the employer may give complete control to the individual and not have access to the data themselves.

Regulated Codes;

0 - No known national standards for Privacy or Security apply. Various states have some provisions in place or pending. Applicable state regulations were not researched for this project.

1 - National HIPAA Privacy and Security regulations would generally apply.

2 - Hybrids, National HIPAA Privacy and Security regulations may not generally apply. An employer may create a place for employees to store and access their own data and no regulations might apply or the employer might merge data in a manner that put the data under various regulations.

How Is a PHR Used?

A PHR is a tool designed for consumers. If our understanding is guided by one of the current definitions of PHR, a personally held and maintained collection of health information, use of the PHR is unchanged. However, once widely adopted by consumers, PHRs have other benefits. The PHR may be used by providers to expand on the information a patient may be able to provide from memory. Use of modern technology simply means the PHR has the potential to be much more comprehensive, easier to search, and potentially both more reliable and more detailed.

Instead of a collection of notes and old medical bills, the newer concept of a PHR can mean a usefully cataloged collection of everything a patient has chosen to record and a shortcut between provider held data sets. The patient could bring with him/her either a copy of records from other providers or a real-time links to other provider's data about the patient. While it may be useful to find that a patient knows he had an ECG "about two years ago," it would be far more useful for a provider to have immediate access to the reasons for the test, the results, and detail on any treatment provided at that time.

A very significant problem in the rapid growth of EHR/PHR options is the current lack of controls. If a patient loses an envelope with some of his medical history in it, the damage may be minimal. For one thing, the records can only be in one place at a time. If a much larger set of electronically held information is inadvertently distributed on the Internet, it is virtually impossible to ever recover. If a central database with tethers (links) to hundreds of thousands of EHR/PHR's is breached, the damage to privacy is unprecedented. Modern marvels make it possible to do more damage faster than at any time in history.

How Information is Maintained in a PHR

Maintenance of PHRs is entirely dependant upon who controls access and what form of PHR is being maintained. Several factors will significantly control growth of PHRs;

- How complete is the record?
- How accurate is the record?
- How easy is it to find the right pieces of information?
- How easy is it to share the information?
- How is it populated? Pre-populated? Manual entry only? Combination of both?

Finding a note about a prescription is not tremendously useful if no information is available on what other drugs were taken at the time and what outcomes were achieved. Maintenance in its simplest form is simply the addition of new information. The problems come when deciding which information is significant, how it can be found later, and, possibly more important, who decided it was accurate? All PHR information should be regarded with some skepticism. How much trust should be placed in data provided by the patient?

Hand-written notes in pencil on a yellow legal pad are "notes." Type those notes into a computer and print them out in crisp black characters and perception tends to shift the same data from "notes" to "facts." If a provider asks a question about family medical history, the provider has some opportunity to evaluate the reliability of the information based on body language, voice, and

wording. If the same information is shared across a computer network, assessing the reliability of the data is almost impossible. If the on-screen presentation does not make it clear which information has been authenticated, using the information may shift from benefit to risk. If a provider does not use the information and harms the patient, it may be said that they "should have known." If the provider does use the information and it is wrong and harms the patient, possibly it will be viewed that they "should have known better." As with all health information, all of the benefits of a PHR are directly tied to the degree to which the data may be relied upon.

Who Owns the Information Stored in the PHR?

Depending on which type of PHR is being used, ownership, access, privacy and security and maintenance issues will vary. For example, the provider clearly owns the data in his/her office and on his/her system. Once the provider gives the patient data/access to the data, the law is unclear. However, unlike tangible property, information may have some impressively complex overlapping control issues. The provider who created the information has some legal rights to use it, even though he/she may have little or no right to dispose of or share that information. The issues were a bit simpler when the medical record was a single paper file. Today, information storage and retrieval have become so complex that it is often difficult to determine who actually has the information, much less who owns it. The issue is probably best discussed in terms of who controls access to the information rather than who owns it. Most effective use of the data requires ease of access. Ease of access is diametrically opposed to control and privacy.

One of the more complex aspects of control is what happens when information is shared. If a hospital downloads data to a patient's personally held PHR, it would seem the patient both owns and controls the information, or at least that copy of it. This is simple enough with, perhaps, the caveat that the hospital is still responsible for the accuracy of the data supplied (up to the time of supplying the data, not thereafter). If a computer screen displays information that is clearly covered under HIPAA privacy and security regulations, and data free of all regulation because it is part of the patient's personal input into the PHR, how is the user to know which regulations apply? If access to the patient's copy is improperly handled, what responsibility do the agencies who contributed data have? Certainly, it could be argued that the information technology department at a major medical center understood the risks better than an elderly patient who wasn't quite clear on what, exactly, the "send" button does.

Who Has Access to the PHR?

Access is a challenge and again depends upon the type of PHR being used. HIPAA has fueled some lively discussions and spurred progress toward some excellent systems for controlling who gets access to what. HIPAA has also done wonders for information technology employment. Having data is easy. Letting people use it requires more staff.

Tiered access (i.e., only giving individuals access to the parts of the record that they "need to know" for their job duties) is a well established practice in business. However, with a PHR, it may be that the door is either open or closed. This may be a minor issue if the PHR is made up entirely of the patient's contribution. What happens when the PHR is a blend of data from clinical databases? It is easy to see how this could develop into a serious leak in the hull.

At a recent conference, a provider loudly displayed his confusion over the distinction between his wish to know everything about a patient and his legal right to know. His sincere desire to provide the best possible care completely obliterated his respect for the patient's right to keep certain information private. It may be he should not be placed in charge of access. At the same conference a consumer vehemently maintained his right to not tell anyone any information that might be used to deny him care he felt appropriate. It may be we don't want him writing all the standards either.

The reality is that a lot of providers don't really want to know everything about a patient. Too much information is a big fear for some providers, too. They are used to operating in the absence of detailed information about the patient.

Data mining has the potential to revolutionize our understanding of medicine. The information collected by your grocer, your healthcare providers, your credit card companies, your employer, and your PHR could entirely change how we treat patients. If your provider knew your purchases of antacid are up, you recently ran up impressive balances on your credit cards, and you have teenagers, treatment of your indigestion may be altered. Computers can reveal patterns that may aid in diagnosis. Since lifestyle is, to a large degree, health, there is a lot of information that could be used to improve healthcare. However, the question remains: which information is relevant and what is the strength of the relevance? The cost in privacy may or may not be one we are prepared to accept. The more data we have pooled, the better we can do. The more data we have pooled, the higher the potential magnitude of a breach.

Incentives for Keeping Data Complete, Current, and Accurate

Consumer Incentive

The consumer's incentive in maintenance of PHRs is probably rooted in a desire to have the most effective healthcare possible. More information on previous drug and treatment responses could lead to better selection of treatment options in the future. The ability to provide a clear and accurate medical history could both avoid undesired complications and improve outcomes. There is also an incentive to make sure each health professional you see knows what the others have done. Absent updated information, the patient can keep cycling through expensive and inconvenient health care visits without effectively getting to root causes of ailments.

Additionally, the PHR is a method to better organize and store medical information from multiple sources, thus making it is easier to share patient information and clinical history with providers.

Health Plan Incentive

From a business perspective, health plans have two strong motivations. The first is clearly a desire to provide for the best care possible for patients. The second is to provide the best care at a reasonable price. Cost containment is not a cold business issue; it is an integral part of patient care from the health plan perspective. If the cost of high quality care exceeds the ability of the patient to pay, no one wins. In the end, patient care costs must be passed on to patients. This cost may be pooled and shared, but it must be paid for by patients. Health plans do not create the money, they only manage it

and part of that management is doing everything possible to control costs. Effective use of PHRs could reduce cost-of-care. But even though the effective use of PHRs could help keep cost-of-care from skyrocketing, the perceived consumer risk is that the data may be used to control the cost-of-care for a particular health plan by dumping potentially expensive patients.

Also, the PHR shifts the emphasis and responsibility for information gathering and care from the institution to the consumer with the anticipation of aiding to promote best practices and improve outcomes reporting results.

Healthcare Provider Incentive

Provider incentives are to provide the highest quality and most accurate care possible to their patients. Certainly providers will place more emphasis on delivering care, but many providers are acutely aware of the degree to which cost influences access to care. Providers in general, look forward to more complete information upon which to base decisions about treatment options.

There are a number of legislative initiatives that have been introduced in Congress to provide incentives to health care providers to use health information technology, including electronic and personal health records.

Another PHR benefit is that the provider is also benefited by having convenient access to a patient's clinically accurate information based on clinical standards rather than having to rely on a patient recalling and remembering what a prior provider has requested in terms of orders and prescriptions.

Employer Incentive

The employer can shift a portion of the medical care, best practices, and aid with the controlling of medical costs to the employee. The PHR engages the employee in their own wellness program and helps control corporate costs.

Vendor Incentive

Various provider billing software vendors and hospital system vendors can focus on interoperability and transportability of data information with lends their products to being more competitive in the market place and provides another return on investment (ROI) opportunity. This also enables the enterprise vendors to bring in the consumer into the provider and health plan healthcare community, again lending their products to potentially more sales opportunities.

Privacy and Security Implications of PHR

Current Privacy and Security Issues

Because a PHR contains personal medical information about an individual, it is important that certain privacy and security measures be implemented to prevent unauthorized access. ***However, depending on which type of organization creates and maintains the PHR, current state and federal privacy and security regulations may or may not apply.*** If appropriate privacy and security measures are not in place, there is no guarantee that the individual's information will be safeguarded. And, if the organization is not covered by any type of regulation, there would be no regulatory consequence for unauthorized release of the individual's personal information, although there may be other common law or statutory protections. As a result, it is very important that the individual know and is comfortable with the privacy and security practices of the organization prior to developing a PHR.

Depending on the type of organization offering a PHR, certain state or federal regulations regarding the privacy and security of the information may apply. For example, HIPAA regulations may apply if a healthcare provider or health plan is the entity responsible for creating and maintaining the PHR and they meet the definition of a "covered entity" according to the regulations. In that case, the covered entity would be responsible for instituting policies and procedures for the privacy and security of the PHR as it may be considered to retain "Protected Health Information" (PHI) under the HIPAA regulations.

We suspect that there are some organizations offering PHRs that are covered by regulations, but may not be aware of it. One such case would be an employer operating as a group health plan. As a result, they would be responsible for compliance with the HIPAA regulations. However, there are likely many employers who have not yet realized this responsibility.

In certain situations, a PHR may not be covered by any type of privacy and security requirements to protect the consumer's data. This would likely be the case if the organization offering the PHR is an independent vendor that is not covered by any state or federal regulations regarding privacy and security of health information. In this case, the consumer could be considered to be in control of what information is stored and who has access to it. There are certainly no regulations which would prevent an individual from sharing his or her own health information with whomever they choose (except in cases such as a minor or those with designated personal health representatives). The only security mechanisms in place to protect the data from unauthorized access would likely be whatever security the vendor has chosen to implement. And, unfortunately, the consumer would have no guarantee over its reliability.

Multiple industry organizations have recognized these issues and are currently working to create standards regarding the use of PHRs in order to provide for the privacy and security of the

records. The next section outlines some of the major efforts that are currently underway to address these issues.

It is also important to point out that HIPAA has not be vigorously enforced by any measure. Just throwing the HIPAA blanket over PHRs without a more nuanced articulation of policies and protections will not necessarily eliminate risks.

PHR Standards Activity

This section outlines many of the efforts currently underway in the industry to set some standards relating to privacy and security of the PHR. The information included here is current as of the time of the writing of this paper. For the most recent information, please contact the organizations directly and many of these efforts are ongoing.

Current National Private Sector Projects

There is growing activity on the national and standards development organization (SDO) level regarding the development of PHR standards, and most of the focus has been on development of standards related to EHR's and electronic health information exchange. There is recognition that PHRs could well prove valuable in improving care, reducing costs and addressing consumer concerns regarding direct access to their medical information. Some promising federal initiatives include a PHR pilot sponsored by the Centers for Medicare & Medicaid Services (CMS) for Medicare, various state initiatives, and MyHEALTHeVet from the Veterans Administration. Additionally, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) have been active in the area of privacy protections for consumers.

Privacy and security, especially for employer sponsored and third party unaffiliated vendor sponsored PHRs, is inconsistent. If the PHR is sponsored by a covered entity, the covered entity has a regulatory framework for maintaining adequate security and privacy as defined under HIPAA and other state and federal law. This, again, is not the case with the employer or non-affiliated vendor PHR offerings. There have been discussions regarding promulgating regulations requiring entities offering PHRs to adhere to the same or similar privacy and security standards included in the HIPAA rules. At this point, no such regulations exist.

Coordination of Efforts between Parties

Recent collaboratives have been formed in order to support coordination of several efforts that are currently underway. Vendors assisting health plans, providers and employers to make a PHR available to consumers or employees have been successful in developing and marketing standardized PHRs that are in use or soon will be in use by providers, health plans and employers. This provides some consistency but, there might be an inherent conflict of interest as such vendors are competing to market their version of a PHR to employers and healthcare organizations. In some cases, this means that issues relating to interoperability and standardization are left up to the vendor, and vendors will and do differ in their approach.

Additional coordination efforts need to be initiated to address the standards issues raised in the previous section and to develop a clear PHR definition and to agree on basic security and privacy practices.

Today, many PHR development efforts are conducted in a vacuum. It will become more and more important to see and encourage an expansion of collaborative efforts to avoid conflicting standards, compatibility issues, the inability to securely transmit data from the PHR too a provider or other caregiver, etc.

Efforts to Involve the Government

PHRs have been topics of discussion as part of federally funded projects such as the Health Information Security and Privacy Collaboration (HISPC) and Health Information Technology Standards Panel (HITSP) (further described below) projects. Most discussions are occurring as part of efforts to sell PHRs and by non-governmental organizations such as WEDI, eHealth Initiative, etc. interested in seeing appropriate marketing and use of PHRs.

AHIC

The American Health Information Community (AHIC) is a federal advisory body, chartered in 2005, to make recommendations to the Secretary of the U.S. Department of Health and Human Services on how to accelerate the development and adoption of health information technology. AHIC was formed by the Secretary to help advance efforts to achieve President Bush's goal for most Americans to have access to secure electronic health records by 2014.

Since its formation, the AHIC identified multiple workgroups with potential for early breakthroughs in the advancement of standards that will lead to interoperability. One of these workgroups, the "Confidentiality, Privacy and Security Workgroup" was formed with a specific charge to "Make actionable confidentiality, privacy, and security recommendations to the Community on specific policies that best balance the needs between appropriate information protection and access to support, and accelerate the implementation of the consumer empowerment, chronic care, and electronic health record related breakthroughs."

This workgroup began meetings in August 2006 and is continuing on a monthly basis to date. They are comprised of multiple industry experts in the areas of privacy and security to help address privacy and security issues relating to the implementation and use of PHRs. As part of this effort, several other industry groups, including the Health Information Security and Privacy Collaborative (HISPC), the Healthcare Information Technology Standards Panel (HITSP), the Certification Commission for Healthcare Information Technology (CCHIT) and the Nationwide Health Information Network Architecture Project (NHIN) are working on various areas of the problem and will make recommendations back to AHIC. Discussion of both the HITSP and HISPC projects are included in the following sections of the white paper.

Archives from AHIC's monthly meetings are available at http://www.hhs.gov/healthit/ahic/confidentiality/cps_archive.html.HISPC

Purpose of the HISPC Project

The HISPC project was initiated by Agency for Healthcare Research and Quality (AHRQ) and the Office of the National Coordinator (ONC) with the goal of identifying barriers to electronic

HIE, developing solutions that address identified barriers (business and legal) and developing implementation plans to address problems identified. Ultimately, the goal is to remove barriers to HIE while continuing to protect the privacy and security of consumer health information.

At the time the HISPC project was kicked off in 2005, the talk of PHRs nationally was rather limited. As it has become more and more of an issue, states and the national project team are concerned about how the project has progressed. It is important to note, though, that the project officially ends for states at the end of April 2007 and nationally at the end of June 2007. Few states have developed implementation plans that address the recent explosion in the PHR market.

Actions to Date and Future Plans

States are in the process of drafting state level final solution and implementation plan reports. Solutions currently being addressed in implementation plans relate to authorization, authentication, consent, development of security standards, RHIO development, etc, although these plans do not directly address PHR adoption or standards, at least in the short run. Plans in the short run are focused on removing the barriers to the exchange of health information within the industry and between the industry and consumers.

It is likely that security and privacy for PHRs will become more and more of an issue. It needs to be understood though, that states cover a wide continuum. Some are at the beginning phase of adopting electronic HIE and others have a fairly sound infrastructure and are fairly well advanced regarding the adoption of electronic HIE. While PHRs will likely play a role in improving healthcare, especially from the consumer perspective, they are not necessarily high on the agenda of most states as relayed through their reports to the national HISPC contractor.

For more information about the HISPC project, please refer to your state's HISPC web site (if you are from a participating state) and the RTI International web site (the national coordinator/contractor leading the HISPC project) at http://www.rti.org/page.cfm?nav=6&objectid=09E8D494-C491-42FC-BA13EAD1217245C0. Additional information will be published in the near future following review and approval by AHRQ and ONC.

HITSP & Health Level 7

In 'The Review of the Personal Health Record (PHR) Service and Provider Market' report of March 13, 2007, published 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), the findings are presented as follows:

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.

This document is found on the US Department of Health and Human Services web site in the AHIC section under the Consumer Empowerment tab. See http://www.hhs.gov/healthit/ahic/consumer/ce_archive.html and select "Updated Altarum Institute PHR Privacy Policy Report."

The Patient Safety and Quality Healthcare: News reported on February 20, 2007, the following: "Health Level Seven (HL7), with the collaboration of the ASTM International E31 Healthcare Informatics Committee, today announced that the Continuity of Care Document (CCD) has passed HL7 balloting and is endorsed by the Healthcare Information Technology Standards Panel (HITSP) as the harmonized format for the exchange of clinical information including patient demographics, medications and allergies."

http://www.psqh.com/enews/0207d.html

The Healthcare Information Technology Standards Panel (HITSP) endorsed the Continuity of Care Document (CCD) as the harmonized format for the exchange of clinical information, including patient demographics, medications, and allergies. In 2006, HITSP was asked to produce a harmonized IT standard recommendation to HHS.

"The CCD is a joint effort of HL7 and ASTM to foster interoperability of clinical data to allow providers to send electronic medical information to other providers without loss of meaning, which will ultimately improve patient care."

What Has Been Done to Date and What Are Plans for the Future?

Currently, HITSP has been charged by ONC to harmonize standards based on use cases derived from AHIC priorities and requirements.

AHIC has already handed down to HITSP its main priorities for 2007, which will be hammered out from now to October when the standards and interoperability specifications will be again delivered to the national coordinator through a similar process.

The 2007 priorities include the following:

- Harmonization of privacy and security standards;
- Emergency Responder Electronic Health Record – a transportable record to enable emergency providers to care for you with the aid of essential medical details. This could be applied to mass casualty events or for individuals,
- Expansion of the Consumer Empowerment Use case to incdlue additional PHR features. Personal Health Records – an enormous amount of activity has taken place in this realm, with numerous companies signing on to PHR initiatives for employees. The companies include large employers such as Intel and Wal-Mart. There are also a number of private companies putting PHR products out on the market, or planning to. These must all be resolved so they can work together. HITSP' task is to get a handle on all of this activity and to develop standards;
- Expansion of the Electronic Health Record Use Case to include Medication Management – "We have to now harmonize standards for medication management for the country. This one is difficult because there are so many stakeholders," said John Halamka, Chair of HITSP and CIO of Harvard Medical School; and
- Quality – HITSP will aim to harmonize the reporting of hospital and physician quality measures

The HL7 EHR Technical Committee has worked towards a project proposal to develop a core data set for the PHR. As a result, starting in April, 2007, HL7 will have established a committee working to prepare a HL7 PHR Functional Model and to ensure that the import and export process for EHR to PHR connectivity and conformance.

Plus, there is research being done to address a question in the HL7 communities mind as to whether the PHR is a United States phenomenon or if PHRs are used internationally.

Financial Industry

A primary concern in the development and distribution of all banking and financial services is Public Trust. Without Public Trust a bank ceases to operate, so this area is very sensitive in banking. In addition, the operations of banks, credit unions and financial services firms are overseen by a number of agencies and closely related organizations that provide best practices and protocols to support Public Trust. The configuration of overseers has some overlapping areas, and this is done intentionally in order to rigorously guard Public Trust in the banking arena. Some of these agencies and/or regulatory bodies include the Board of Governors of the Federal Reserve Board, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, National Credit Union Administration and Office of Thrift Supervision and others. This particular set of overseers form the Federal Financial Institutions Examination Council (FFIEC) that provides banking, financial services organizations, and others who offer similar services, with a series of best practices related to online banking and many other areas. The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630.

The FFIEC issued guidance in 2001 specifically related to banking in the online environment. This guidance was updated in 2006 to include, among other things, a strong recommendation that all national banks implement online banking protocols that support multi-factor authentication when

there is access to monetary transactions in the online environment, among other scenarios in banking. The underlying agencies have implemented this recommendation in their ongoing audit programs as of January 1, 2007. A key principle driving heavy investment in this area by banks is a risk to their reputation within the electronic banking area. This type of risk, legal risk, economic risk and other risk categories form the basis for approving national bank activities by the OCC. A list of "permissible" national bank activities is located at: http://www.occ.treas.gov/corpapps/BankAct.pdf. The FFIEC guidance related to privacy and security controls, such as identity proofing, authentication of persons and systems and other identity management techniques may be found at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

In 2005 the Medical Banking Project launched a PHR standards effort within the banking and financial services sector. The effort creates a common platform for banks, healthcare plans and providers, IT firms, pharmaceutical firms, government agencies and others via bi-lateral trade and operating agreements, technical standards development for inner/intra-bank transfers of administrative and clinical information and other areas. The effort implements the HIPAA privacy, security, transaction and unique identifier requirements, as well as related banking regulations (i.e., Title V of Gramm Leach Bliley, others). The architectural design enables the transport of clinical transactions among banks in order to "fulfill" a PHR request by an online banking customer, and uses existing healthcare standards group work (i.e., Integrating the Healthcare Enterprise (IHE), HL7, HITSP, others) coupled with banking standards. These hybrid or "medical banking transaction sets" seek to enable partnering of banks with healthcare stakeholders (plans, providers, RHIOs, others) in order to use the banking system to distribute PHRs. In this manner, national PHR adoption strategies could reach a wide ranging demographic of healthcare consumers who are signing online to pay their bills (some 55 million online banking consumers). In a growing number of cases, these consumers are also reviewing their healthcare expenses in new "account-based health plans" (i.e., Health Savings Accounts (HSAs), Health Reimbursement Arrangements (HRAs), Flexible Spending Accounts (FSAs), etc) and seek on-demand access to their healthcare records in a secure online environment. The Advisory Board for MBProject's effort includes the American Hospital Association/Solutions, Healthcare Information and Management Systems Society (HIMSS) and IHE, National Clearing House Association, National Health Council, the Center for Charitable Statistics at the Urban Institute, Electronic Healthcare Network Accreditation Commission, Family Voices and Consumers for Healthcare Choices.

Markle Foundation

Connecting for Health, a collaborative group of more than 100 organizations operated by the Markle Foundation, has published work group reports and new research on PHRs every year since 2003.

Currently, Connecting for Health has convened two new national panels to recommend policies for networking PHRs with institutional health data sources: The Work Group on Consumer Authentication and the Work Group on Consumer Access. The former will be recommending policies for authenticating individual consumers and the latter is working on other critical policies for privacy, consent, secondary uses, breach, etc.

December 2006
Connecting for Health released a white paper that describes a networked health information environment in which consumers could establish secure connections with multiple entities that hold personal health information about them. The paper begins with a brief discussion of how consumer participation in networked environments has transformed other sectors, such as travel and finance. It contends that the health care sector would benefit greatly from a properly designed secure network that enables consumer participation.

http://www.connectingforhealth.org/commonframework/docs/P9_NetworkedPHRs.pdf

December 2006
Connecting for Health released research showing that Americans overwhelmingly want to have electronic copies of their medical records and believe that having greater access to their information will reduce medical mistakes and costly repeat procedures,

October 2005
The Personal Health Technology Council released its consumer principles related to health information exchange and personal health records.

http://www.markle.org/downloadable_assets/consumer_principles_101105.pdf

October 2005
The Markle Foundation released a survey showing strong nationwide support for secure electronic health information exchange and personal health records.

http://www.phrconference.org/assets/research_release_101105.pdf

August 2005
The Personal Health Technology Council responded to a Request for Information (PDF, 636k) on Personal Health Records from the U.S. Centers for Medicare & Medicaid Services (CMS), the government agency that manages Medicare and Medicaid.

http://www.connectingforhealth.org/resources/CMS_Response_Final_083105.pdf

July 2004
The Working Group on Policies for Coordination Across the EHR and the PHR released the groundbreaking Connecting Americans to Their Health Care report.

http://www.connectingforhealth.org/resources/wg_eis_final_report_0704.pdf

July 2003
The Personal Health Working Group became the first collaborative body to define the key characteristics and benefits of electronic personal health records when it released its Final Report (486k).

http://www.connectingforhealth.org/resources/final_phwg_report1.pdf

Consumer Findings

Personal Health Record Survey

As part of the development of this white paper, we asked members of the team developing the white paper to create their own PHR and answer a questionnaire relating to their experience with the PHR. We did not provide guidance as to which PHR to use. Rather, the individual was to locate a PHR provider on their own and create their own record. They were told that they could use either their own real data or fabricated data.

The feedback on the use of PHRs was good overall. Everyone thought that it was beneficial to their health to maintain a PHR, although some felt that it was too much trouble to keep updated. Some respondents had health conditions that required them to keep track of health information, such as glucose levels, diet, or blood pressure readings on a daily basis and felt it was a very useful too for tracking this information and being able to share the information with their providers. However, at the time of the survey, very few respondents had actually shared the information they entered in their PHRs with their providers. It was divided as to whether they used medical records/claims data to pre-populate their PHR or they manually entered the data themselves.

Most everyone was comfortable with the privacy and security of their data while using the PHR. Some received a Notice of Privacy Practices. Many were not aware of whether or not the organization providing the PHR was considered a covered entity under HIPAA, and therefore were required to comply with HIPAA privacy and security requirements. There was only one respondent who said she was not comfortable with the privacy and security of her data in the system she chose. A couple of respondents indicated that they chose not the complete a PHR survey because they were concerned with privacy and security of PHRs in general.

We asked what the respondents felt the potential issues were. Here are a few of their responses:

> "Getting consumers to keep their information current. Making it available to your primary as well as other medical personnel that may need to access in case of emergency. How do you keep this in sync with EMR or do you? How do people that do not have computers and/or not capable of creating and maintaining a PHR handle this? How is the information provided to someone to do for them? Where is the PHR stored?"
>
> "Not valuable if not complete and up to date."
>
> "General privacy and security issues if the covered entity does not actively manage their security and privacy program."
>
> "Time in getting started. Change. Access. Viewed as complex by the population that needs this health management tool the most."

"I'm afraid the providers won't look at it or use it, but just continue business as usual."

"I may not keep it current and I'm not sure how much access I want to give to others or if I want it to auto populate."

"I really think the online options need to have some kind of proven security. Would even be nice if there were some kind of certifications like I believe there are for EHR."

We also asked the respondents for any recommendations they have for the use of PHRs. Here are several of their responses:

"Updates and maintenance are critical for the PHR to ever be of value for medical personnel authorized to access it for information."

"The navigation is slow due to lots of advertising links and notices, and the screens are very busy for a typical consumer. Once in the PHR, the flow is okay but could be made a lot simpler and easier to use."

"Continuing to develop security measures to ensure appropriate firewalls are in place to limit hacker activity."

"Engage our young people in PHRs early to help with reinforcing healthy choices and giving them tools that demonstrate their successes."

Summary

In this paper, we have described many different types of PHRs that have evolved over the last several years. Since there are multiple variations, it is important to understand which type of PHR you are dealing with prior to defining the appropriate privacy and security standards for it. For example, HIPAA privacy and security regulations only apply if the organization creating the PHR is considered to be a covered entity as defined by HIPAA. And, even that can become unclear in certain situations. For example, an organization not considered to be a covered entity under HIPAA creates the PHR template, but the data is actually populated by a covered entity, such as a provider or health plan.

Any privacy and security standards that are created to regulate the use of PHRs need to define exactly what is considered to be a PHR based on who creates it, who has access to it, and who maintains the data. They will likely need to define different standards for different types of PHR. But, whatever the variation, the consumer should take the initiative to familiarize themselves with what regulations apply and what the specific privacy and security practices are.

Another area that needs to be considered is technology. As the industry has observed in the past few years, technology has become a critical component to planning. Wireless has become more prominent, USB devices storage capacity now exceeds that of most home computers and there is no end in sight. Privacy and Security standards should be general enough to encompass technology available today and to what extent possible, technology that might be used in the future.

As we have seen, there are many industry efforts – both government and private – that currently have efforts underway to define standards for privacy and security of PHRs. There is some coordination between these efforts, but there needs to be an overall coordination between these organizations and their specific objectives to take advantage of the expertise within each of the groups and to prevent duplication of effort.

In conclusion, “medical consumerism” is on the rise and will continue to increase. Today’s society urges consumers to take responsibility for their own health, and a PHR is just one of the many ways that this can be facilitated. Consumer demand will continue to increase the need for PHRs that are both easy to create and maintain, but also secure. The industry needs to respond with clear, concise standards that provide measures such that the consumer’s data is protected from unauthorized access.

Other Sources of Information

Name	Description	Website
AHIC	American Health Information Community	http://www.hhs.gov/healthit/community/background/
AHIMA	American Health Information Management Association	http://www.ahima.org/
AHIP	American Health Insurance Plan	http://www.ahip.org/
AHRQ	Agency for Healthcare Research and Quality	http://www.ahrq.gov/
ASTM	American Society for Testing and Materials Standards	http://www.astm.org/
CCHIT	Certification Commission for Healthcare Information Technology	http://www.cchit.org/
HIMSS	Healthcare Information and Management Systems Society	http://www.himss.org/ASP/index.asp
HISPC	Health Information Security and Privacy Collaborative	http://www.rti.org/page.cfm?objectid=09E8D494-C491-42FC-BA13EAD1217245C0
HITSP	Health Information Technology Standards Panel	http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3
HL7	Health Level 7	http://www.hl7.org/
IHE	Integrating the Healthcare Enterprise	http://www.himss.org/ASP/topics_ihe.asp
Markle Foundation		http://www.markle.org/
NHIN	National Health Information Network	http://www.nhin.com/
ONC	Office of the National Coordinator	http://www.hhs.gov/healthit/onc/mission/
WEDI	Workgroup for Electronic Data Interchange	http://www.wedi.org

Acknowledgments

Chris Apgar
President
Apgar and Associates, LLC

Lesley Berkeyheiser
Principal
The Clayton Group, LLC

John Casillas
Executive Director
The Medical Banking Project

Lorraine Doo
Senior Policy Advisor
Centers for Medicare and Medicaid Services

Connie Hein
Principal
Hein Consulting Group

Elizabeth Holland
Health Insurance Specialist
Centers for Medicare and Medicaid Services

Dale K Howe, PhD

Dave McCord
Director of Application Development
TM Floyd and Company

Brian Raymond
Senior Policy Consultant
Kaiser Permanente Institute for Health Policy

Marge Simos
Director Industry Standards and Government Programs
Express Scripts

Barbara Sesny
Transaction Specialist
BCBS of Michigan

Nancy Spector
Director, Electronic Medical Systems
American Medical Association

Mary Julia Street
HDX Project Manager
Siemens Medical Solutions USA, Inc

SNIP Security and Privacy Co-Chair Reviewers:

Mark Cone, N-Tegrity Solutions Group

David A. Ginsberg, PrivaPlan Associates

Susan A. Miller, Health Transactions