Connecting for Health Steering Group
and the
Personal Health Technology Council

Response to Request for Information Issued by the
Centers for Medicare and Medicaid Services

Opportunities for CMS Actions in Support of Personal Health Records

August 31, 2005

Contact:
David Lansky, Ph.D.
Senior Director, Health Program
Markle Foundation
New York, NY
212-713-7624
dlansky@markle.org

About Connecting for Health:

Connecting for Health is committed to accelerating the development of a health information-sharing environment by bringing together an array of private, public, and not-for-profit groups to develop common standards and information sharing policies. Managed by the Markle Foundation and funded by both Markle and the Robert Wood Johnson Foundation, Connecting for Health works to overcome the technical, financial, and policy barriers to bringing health care into the information age.

About the Personal Health Technology Council:

The Personal Health Technology Council is a diverse group of 50 national organizations and thought leaders advocating for patient empowerment through personal health records and other health information technologies in the context of an emerging system of nationwide health information exchange. The Council explores the policy barriers and potential accelerators to adoption of effective health technologies by consumers and patients.

About the Markle Foundation

Emerging information and communication technologies possess enormous potential to improve people's lives. The Markle Foundation works to realize this potential by accelerating the use of these technologies to address critical public needs, particularly in the areas of health care and national security. The Markle Foundation Health Program is committed to accelerating the ability of patients and consumers to use information technology to improve their health and health care, while protecting patient privacy. The Markle Foundation envisions a time in the near future when individuals will be able to gain access to their own health information through nationwide electronic health information exchange, personal health records, and other emerging technologies, making it possible for patients to participate more fully in their own health care.

Opportunities for CMS Actions in Support of
Personal Health Records:
A Collaborative Response from Connecting for Health

Prologue

Connecting for Health is a public-private collaborative of more than 100 diverse organizations managed by the Markle Foundation and funded by both the Markle and the Robert Wood Johnson foundations. *Connecting for Health* is currently launching a prototype of a "health information-sharing environment," based on common, open standards and policies that protect privacy and security. This effort is the first step in enabling patients and authorized health care professionals across the United States to share important, even life-saving, personal health information on a completely voluntary basis in a secure and private manner.

Connecting for Health working groups have provided national thought leadership on policies to accelerate the beneficial use of personal health records (PHRs) and other personal health technologies. In 2003 and 2004, *Connecting for Health* published pioneering reports on PHRs based on the deliberations of expert panels made up of early PHR implementation sites and other concerned parties. In 2005, the Markle Foundation convened the Personal Health Technology Council, comprised of about 50 consumer and health care leaders working to ensure that new consumer health technologies help Americans better manage their health and health care. The PHTC is examining the policy barriers and accelerators to the adoption of effective consumer-based health technology.

This document thus represents a consensus of many of the nation's leading technology, health care, and consumer leaders (see appendices). We have sought to provide CMS with a strategic umbrella, under which many worthwhile programmatic and technical approaches will coexist. This paper outlines an emerging national PHR and EHR ecosystem, within which CMS actions should fit and to which CMS can contribute accelerating actions. We recommend actions in the near term, through 2008, in order to position CMS for innovative ways to help accommodate the wave of Baby Boomer beneficiaries.

Connecting for Health views the adoption of electronic PHRs not as an end in itself but as a foundation for Americans to improve the quality and safety of the care they receive, to communicate better with their clinicians, to manage their own health, and to take care of loved ones. PHR initiatives should be judged by whether they make it easier for ordinary people to engage more actively in their own health and health care. Do PHRs help people arrive better prepared at doctor visits? Do they inspire better self-care? Do they help people set, track and reach target goals for their conditions? Do they help people follow their treatment regimens and preventive service recommendations? Do they help people manage multiple medications and minimize adverse drug events? Do they help caregivers coordinate the care of loved ones across multiple providers? Do they help people make sure that health professionals have timely and convenient access to

clinically relevant information about them—whether in the primary care provider's office, the pharmacy, the emergency room or the intensive care unit?

These diverse aspirations are likely to be realized by a wide variety of personal health record products and applications — working from a common set of clinical and personal information. Data about symptoms, health behaviors, professional encounters, diagnoses, procedures, medications, and test results will be organized and interpreted by software applications designed to deliver specific value to specific groups of people. Some of these applications will be tightly linked to provider organizations and electronic medical records, and some will operate directly under patient control, independent of any provider. In any scenario, CMS is in a unique position to acquire and distribute some of the data — in a structured, beneficiary-controlled way — to enable innovative developers to provide valuable tools to American patients and families. This is a new and inadequately understood area, with implications for law, ethics, technology, finance and liability. CMS will need to address a number of challenges to identify its appropriate role in this new and unsettled environment. Beneficiaries — and the nation as a whole — will be best served if CMS works closely with both public agencies, private sector organizations, and the general public to develop models, policies, and standards that respond to these challenges.

Previous *Connecting for Health* reports have highlighted the variety of elements, features and services that personal health records, tied into a connected health information environment, can provide. A fully realized personal health record would reflect seven attributes:

1. Each person controls his or her own PHR.
2. PHRs contain information from one's entire lifetime.
3. PHRs contain information from all health care providers.
4. PHRs are accessible from any place at any time.
5. PHRs are private and secure.
6. PHRs are "transparent." Individuals can see who entered each piece of data, where it was transferred from, and who has viewed it.
7. PHRs permit easy exchange of information with other health information systems and health professionals.[1]

These principles provide a framework within which various products and services can be successful — and can interoperate. A truly empowering PHR "ecosystem" will provide for three levels of connected functionality: (1) clinician-driven functionality (under the clinician's exclusive control) — the standard of the traditional medical record, (2) collaborative functionality (jointly controlled by clinician and patient together), and (3) patient-driven functionality (under the exclusive control of the patient). National efforts to develop standards and policies should recognize the interdependency of these three layers of functions, and support the medical empowerment of growing numbers of laypeople, now and for future generations. To support and stimulate a marketplace of

[1] "Connecting Americans to Their Healthcare," Working Group on Policies for Electronic Information Sharing Between Doctors and Patients, Connecting for Health, July 2004, p24.

innovators, CMS must have a strategic vision and a tactical plan that takes into account likely trends in demographics and emerging technologies.

Over the next decade, we expect new Medicare enrollees to be increasingly capable and interested in online applications to help manage their health. We expect higher levels of health information consumption, and a greater demand for medications and treatments. The Medicare population will constitute a greater percentage of the entire U.S. population as Baby Boomers work their way into retirement.

In the coming decade, we expect the health information technology environment to change significantly, although it is not easy to predict exactly how. Among the possibilities:

- Slow, non-standardized EHR adoption and slow development of networks of regional health data exchanges.
- A gradual expansion of portable and home-based devices and gadgets, including a proliferation of home-monitoring devices and health-tracking features built into cell phones and PDAs.
- High connectivity among large national commercial networks (e.g., Aetna, RxHub, Quest Labs) but poor connectivity among individual physician practices.
- Demographic trends and the diffusion of information technology in other sectors that may promote a steadily rising expectation for similar services in health.

CMS strategies must allow for these trends and contingencies. The unpredictable environment, and the importance of CMS' role, makes it essential that CMS conform to stable, durable principles in whatever actions it undertakes. CMS should shape its activities within this body of acceptable principles, regardless of which roles or functions may appear to be appropriate at any given time. We propose the following as initial principles for guiding CMS program development:

No. 1: Public trust is paramount.
Recent qualitative and quantitative research highlights public concern about putting clinical information on the Internet. Markle's 2003 survey of online Americans found about 90 percent of respondents expressing concerns about maintaining the privacy of their health information, with about 25 percent of respondents unwilling to use online records due to privacy and security fears. Westin's 2005 survey reported that 70 percent of adults believed that "sensitive personal medical record information might be leaked because of weak data security," with roughly one-half of the population believing that the risks of online health information outweigh the benefits.[2] These concerns may diminish over time, but not without practical and visible governmental and private industry action.

No. 2: Privacy and patient control are the keys to public trust.
Although the majority of Americans believe that their health information should be available to them and that it can be valuable for them and their providers, privacy is an

[2] Westin, AF. Public attitudes toward electronic health records. Privacy & American Business. February 2005.

enduring value in health care. Patients must have the opportunity to control how their information is accessed and used. Privacy and security are not only personal values but also policy and technology design attributes. The overall technical architecture of our nationwide health information networks will affect our ability to assure the privacy and security of health information. Any CMS program must interoperate with many other health care information systems and cannot address either technical or policy challenges in a Medicare "silo" — particularly since the public will not recognize a CMS-only privacy or patient control issue separate from its view of provider, commercial, or other government health information systems. HIPAA provides a broad baseline framework for shaping privacy policy. However, in a world of personal health records, networked information systems, and new CMS roles not fully contemplated under HIPAA, CMS should play a leadership role in a fresh analysis of privacy, security, and authorization frameworks.

No. 3: Plurality is reality.
Over the course of a lifetime, people have relationships with many different doctors, payers, and other health care entities. And for the nearly two-thirds of Medicare beneficiaries with two or more chronic conditions, it's typically necessary to see multiple doctors and maintain relationships with several different organizations simultaneously. Health needs, attitudes, literacy, etc. vary from individual to individual. A diverse set of preferences and barriers must be addressed. The role of caregivers, proxies, and agents needs to be nurtured and emphasized. No single PHR application is likely to meet all beneficiary needs. Technology also demands a pluralistic approach: the CMS strategy must accommodate unpredictable advances in the use of technology in health care provision, including wireless devices, community-based disease management, personalized medicines, and consumer-directed health care financing models.

No. 4: Interoperability will support innovation, personalization, and widespread benefits.
In the long term, personal health records are most valuable when they permit the electronic exchange of information among patients, professionals and institutions. Personal health records will achieve greater impact if linked to an interoperable health information environment based on open standards and uniform privacy policies. There needs to be commonality of core PHR data fields and functions and universally accepted policies for data-sharing, with the consumer as the gatekeeper of how the information is shared. It is vital that the requirements of PHR efforts be integrated with other HHS, private sector and standards-development organizations' (SDO) work on EHR interoperability standards. The standards that create a foundation of interoperability must also permit sufficient flexibility for the marketplace to innovate to meet specific needs. CMS must avoid "dead-ends" that might create additional information silos and should favor evolutionary strategies that encourage national interoperability centered on the patient.

No. 5: Broad collaboration is necessary to build a national PHR environment. Because of the diversity and fragmentation of U.S. health care, CMS cannot work in a vacuum and create policies that lead to sustainable or optimal long-term outcomes. Several key issues facing PHR development have parallels in or are linked to other information technology settings, including the reliability of various data sources, administration of authorization and authentication, policies and enforcement mechanisms for privacy and security, and the liability for actions taken on the basis of available information. Collaborative, public-private processes can produce sound, comprehensive policy approaches (especially if guided by strategic thinking and reinforced by the nation's largest payer). CMS should act quickly to set policy directions for PHR adoption and use, summarized in the table below and described in more detail in our specific responses.

CMS should:

1. **Convene a national public-private collaboration to agree upon a set of operating principles for deployment of Medicare beneficiary data into personal health records;**
2. **Identify a sequence and mix of pilot projects, including expansion of the my.medicare.gov portal, that address the challenges described below and in the five topic areas posed by the RFI;**
3. **Design and support programs of beneficiary education, in conjunction with related private sector activities;**
4. **Provide technical and financial support to the pilot projects and require rapid implementation and publication of results by late 2008.**

Implications	
Principle	**Implication for CMS**
No. 1: Public trust is paramount.	• CMS must recognize public discomfort with creation or use of centralized government databases. • CMS can play a valuable role by stimulating market readiness, first by motivating beneficiaries and providers that personal health data should be routinely available when authorized by the patient. • Privacy and security protections must be real, prominent, and easily understood. • The process for program design must be public and transparent. • The protocol for fixing errors must be effective, visible, and proactive. • CMS should require education outreach programs by participating entities, and require the collection of a common set of program data to measure the effectiveness of various campaigns.

	• Outreach programs should emphasize tangible convenience and safety benefits to patients. • The pilot projects should be designed to learn about the privacy preferences of Medicare subpopulations. • CMS should consult with beneficiaries and their advocates in developing sound approaches.
No. 2: Privacy and patient control are the keys to public trust.	• Participation in any program must require discrete, well-understood consent, with a clear and easy method for beneficiaries to authorize access to their information. • There must be strong controls over any potential secondary uses. • Patients must have access to audit trails of all accesses to their personal information. • Beneficiaries must actively opt-in for downloads of CMS data to third parties. • Participating third parties must sign HIPAA covered entity business associate agreements with CMS. • CMS must be explicit about its role and the roles of other parties.
No. 3: Plurality is reality.	• CMS should support an innovative marketplace of PHR products. • CMS needs an analysis of how access to personal health information can provide recognizable value to beneficiaries and caregivers, including a breakdown by relevant population segments. • Communications research is vital to identify the range of preferences and barriers, and from that, determine which audiences may be most effectively reached through which means. • CMS should help develop and encourage adoption of security, authentication and data interoperability standards, but avoid setting standards for functions and features. • CMS should commission the development of common evaluation criteria and minimum survey sets to measure the effectiveness of its pilots.

No. 4: Interoperability will support innovation, personalization, and widespread benefits.	• CMS should advocate standards to ensure data interoperability. • CMS should add its voice to ensure that PHRs are part of the nationwide interoperability agenda. • CMS should continue to support EHR data standards and lead the effort to address PHR standards and the interfaces between PHRs and EHRs. • Based on research, CMS should target its initial pilots on groups of early adopters and opinion leaders, such as new enrollees, those with chronic conditions, and caregivers. • Participation in pilots should be open to multiple vendors and organizations based on CMS specifications for a data exchange interface to securely download beneficiary data. • Participating PHR suppliers should be certified by CMS or an independent commission. • Certified vendors and organizations should be capable of exchanging core data sets with other certified PHR suppliers in order to ensure PHR portability.
No. 5: Broad collaboration is necessary to build a national PHR environment.	• CMS should develop a process that includes public and private stakeholders in developing its programs. • CMS should recognize that key policy issues are not unique to PHRs but must be addressed as part of overall HIT planning and should provide leadership to the relevant policy discussions. • CMS should recognize the distinct credibility of beneficiaries' individual physicians in sharing clinical information.

1. CMS' Role with PHRs

CMS should not aim to be a direct provider of a comprehensive PHR product offering. However, CMS should play a central role in raising awareness, setting expectations, encouraging standards, and stimulating the private PHR marketplace.

In seeking concrete steps that CMS can take in the near term, we make the following assumptions about the health information technology ecosystem over the period 2006-2008.[3]

Circa 2008, we assume the following about clinical connectivity in the United States:

- No more than 30 percent of physicians will have an electronic health record (EHR) installed.
- No more than 20 percent of hospitals will have an EHR installed.
- No more than 10 percent of the public will live in communities with highly functioning regional information exchanges.

However, by 2008, we assume a greater level of standardized data availability and connectivity for transaction-based information:

- Nationwide, more than 90 percent of pharmacy claims transactions will be computerized and increasingly available through national clearinghouses, consistent with NCPDP coding.
- With the launch of Part D prescription benefit coverage, CMS will be capturing specific data fields on every Part D-covered transaction, including type of medication.
- As many as half of all laboratory results available electronically will be using LOINC standards (although it's not as clear how much of the lab information will be available through distributed networks).
- More than 95 percent of clinical claims will be in electronic format.

National surveys, including a 2004 national telephone poll by *Connecting for Health*, indicate that consumers would prefer to receive PHRs and related services (particularly secure e-mail) from their own doctor. However, the low expected penetration of ambulatory EHR over the next few years suggests that a PHR strategy that depends upon physician sponsorship or connectivity will be very limited. It may prove necessary, ultimately, that new, intermediate institutions and relationships be invented to achieve ubiquitous consumer engagement in electronic personal health management.

In this immature environment, however, CMS can play a valuable role by stimulating market readiness. It can do so first by motivating beneficiaries and providers to want and expect personal health data to be routinely available when authorized by the beneficiary.

[3] These broad estimates are derived from published literature (e.g., Kaushal et al., The Costs of a National Health Information Network; *Ann Intern Med*, Aug 2005; 143: 165 – 173), various work in progress (e.g., Calinx), and speculation by experts active in each field. They are not proposed as rigorous planning parameters but only to illustrate the likely overall landscape into which any CMS initiative will be inserted.

The most effective near-term action that CMS can take is to stimulate the environment by sharing claims and other available data with beneficiaries. The process should begin with CMS-sponsored pilot projects designed to create greater comfort with an infrastructure of transparency, beginning with the foundational layers of authorization (i.e., giving "consent") and authentication (i.e., having a Medicare password).

The preferred long-term role for CMS in support of PHRs will be as a data supplier in a distributed information environment. CMS should encourage the technology vendor and health care professional communities, in addition to its health plan and prescription drug plan contractors, to integrate beneficiary data in standard formats with applications that help beneficiaries and their providers manage health and improve safety.

A. What PHR functionalities are important for CMS beneficiaries to have available to them?

CMS serves a large and diverse population. Preliminary data indicate that interest in PHRs and the various functions supported by PHR products will vary significantly according to population subgroups. The needs of a healthy 66-year-old are different from those of a dying cancer patient. Both provider-based and commercial PHR products will emerge to respond to these diverse market segments.

Beyond broad qualitative research, however, there is little specific data on the size of each product segment or the relative value of various possible product features. We recommend in Section 4 that CMS undertake a segmentation analysis to identify the wants and needs of specific populations of Medicare beneficiaries for PHR-related services. We further recommend that CMS commission a series of demonstration projects, using common evaluation metrics across all projects, to develop more detailed data regarding desired features, utilization patterns, usability, and user attitudes or concerns (e.g., data security, portability, proxy access).

Although much more study is needed, we believe there is sufficient basis to move forward in two areas beyond the provision of benefit eligibility lookup and basic coverage information:

Area No. 1: Medication management — Medication management is an appropriate and optimal theme for initial CMS activity to encourage the use of PHRs. The American public is making a new and large investment in a publicly financed prescription benefit for seniors, and it looks to CMS to develop policies to improve safety and quality. CMS can help beneficiaries and their caregivers become more directly engaged in the care management process. CMS should test mechanisms to provide beneficiaries online access to their own prescription history in a manner that safeguards the security and privacy of the information.

Our rationale begins with three simple premises:

- **The consumer has the biggest stake.** It is the consumer who actually takes (or doesn't take) each prescription, who enjoys safe and effective treatment (or suffers from an adverse drug event), and who ultimately pays for every prescription.
- **The consumer is often in the best position to know.** In most ambulatory settings, no health care entity knows what only the consumer can know, i.e., what she is taking and how she is taking it.
- **A current medication list is critical data, often poorly managed.** Beneficiaries need help navigating the complexity of their medications, their costs, and their interactions. They should not need to rely on paper and memory in the Information Age. This is amplified when one considers the importance of OTC medications and dietary supplements. The new JCAHO definition of "medications" is relevant here and should be used as the model: "•Prescription •Sample •Parenteral nutrition •OTC's •Vitamins •Vaccines •Respiratory Therapy •Herbals •Nutraceuticals i.e. arginine •Diagnostic and contrast agents •Radioactive medications •Blood derivatives •IV solutions (plain, w/ electrolytes and / or drugs) •Any product designated by the FDA as a drug."

We suggest the following program goals:

- To increase the availability of a consolidated, reconciled medication list for America's seniors and the care providers who serve them.
- To reduce medication errors and adverse drug events.
- To increase beneficiary education regarding appropriate, cost-effective use of prescription medication therapies, particularly for beneficiaries with multiple chronic conditions and multiple medications.
- To increase beneficiary awareness of the benefits of accessing and managing their own health information.

There are practical reasons for starting with medications. Among the most important personal health summary data elements and transactions, the ambulatory prescription is perhaps the least complicated. The RxHub medication history standard is in its final stages of NCPDP ballot approval. CMS will use this as a foundation standard for its Part D e-prescribing efforts. Medications are of high interest to seniors; going to the pharmacy is a monthly routine for most Medicare-age Americans. In addition, our consultations with physicians lead us to believe that a standards-based medication list would be the most rapidly attainable way to show rank-and-file physicians a positive example of the transformative powers of health IT. A consolidated medication list, or at least a start of one based on Part D-covered prescriptions, could be a time-saver as well as a patient safety tool for doctors, and a key educational tool for beneficiaries.

Area No. 2: Clinical claims history — Doctors today in clinics, hospitals and emergency departments make decisions based upon what patients and family members can remember off the top of their heads and scribble on a clipboard. PHRs should be capable of receiving data feeds from a variety of reliable information aggregators. CMS, as the common payer for most Medicare-covered services, can offer PHR products a

starting point for assembling clinical history and consolidated condition lists. CMS should set up pilot projects to provide consolidated lists of visits, procedures and diagnoses.

In both areas, it is important to acknowledge limitations. CMS is just beginning its experience in outpatient prescription data. Raw and adjudicated claims data are notoriously difficult for consumers to understand, and their completeness and accuracy are often insufficient to ascertain a patient's true conditions. Pilot projects should develop empirical data regarding the reliability and usability of these and other existing data streams as well as practical methods to address any deficiencies and exceptions (e.g., when release of specific data is deemed harmful to the patient, as may be the case for some people diagnosed with schizophrenia).

B. Should CMS provide some PHR type services directly, and if so which ones?

We recommend that CMS adopt a phased approach leading, by 2008, to a sustained role as a supplier of data to a range of qualified and beneficiary-designated PHR services.

Although the addition of medication and medical claims data on the Medicare Beneficiary Portal may help educate beneficiaries about the value of accessing their personal health information, we believe that CMS should move without delay toward identification and documentation of necessary requirements (e.g., privacy, security, data management, standardization) for PHR vendor use of CMS-generated medication data.

The process should include:

- Industry consultations and pilot studies regarding data sharing options.
- Development of qualifications for PHR vendor participation in the data-sharing program.
- Availability of data sharing to qualified, beneficiary-designated PHR vendors.

C. Should CMS identify vendors who can provide appropriate PHRs to our beneficiaries and promote their use by beneficiaries through sharing of CMS data, links to them, communication to beneficiaries about their capabilities, etc?

CMS should establish authentication, authorization and secure data exchange rules by which private sector PHR applications (including stand-alone PHRs, PHRs integrated with EHRs, and those supplied by employers, health plans, PBMs, PDPs or regional health information exchanges) could be qualified to receive CMS data. To receive data from CMS, each participating PHR supplier would agree to a HIPAA business associate agreement with specifications for security and restrictions against unauthorized use of the data (see the response to Question 5F, below). Such requirements should be developed to ensure public confidence in the handling of CMS-based data while also accommodating innovative and flexible product ideas.

For example, the Medicare Web site could display a menu of qualified PHR applications, which could compete on the level of service they provide. By providing authorization and clicking a few buttons, the beneficiary would be able to set up regular data downloads from CMS into the application that the user selects.

CMS should conduct pilot projects to develop and test architectures that enable innovation and competition based on service performance and the ability to meet special needs of beneficiaries. The CMS request for proposals should also emphasize data standardization and data portability rules compatible with emerging standards on EHR interoperability of health summary data.

D. Should CMS make data available to many PHR vendors? If so, should CMS require vendors to be "certified" at some level to ensure that the vendor PHR provides the proper privacy and security safeguards for protecting beneficiary data? If so, how? If not, why not?

CMS should develop a standardized, transparent, and rigorous methodology for transferring personal health data to certified PHR vendors, based on beneficiary authorization. Key elements of this methodology include:

- Publication of data standards and related specifications
- Development of a vendor participation agreement that addresses security standards and practices, data ownership, portability, interoperability, privacy policies, user authentication practices, compliance with fair information practices and secondary use limitations and makes clear the legal and contractual penalties that may be faced.
- Establishment of a process that certifies PHR vendors on their adherence to the above policies and practices. Such certification could be handled directly by CMS or through a third-party process.

E. Should CMS regulate data content for PHRs targeted towards Medicare beneficiaries?

In its data-sharing agreements with participating entities, CMS can and should require conformance with its security specifications and prohibitions against unauthorized use of any CMS-sourced or beneficiary-sourced personal health data.

Other types of non-personally identified health content, such as patient education materials, are not appropriate for CMS to regulate. CMS should require basic transparency regarding source and date of health information presented in a participating PHR, and, when applicable, compliance with FDA rules on health information supplied by pharmaceutical companies. We view an approach of transparency, verified by an accepted, independent accreditation body, as more appropriate than a regulatory role for CMS for non-personally identifiable content.

2. Technology and Standards

A. What technologies are available to transmit information to PHRs from other record systems? Are there some technologies used more than others?

CMS' support of PHR access and use provides an unprecedented opportunity to help create and leverage the infrastructure for health information exchange. PHR is one application within a complex and diverse health information environment. However, unless there is purposeful attention paid to infrastructure requirements, it is unlikely that piecemeal technology adoption will result in the connected infrastructure necessary to realize the quality of care and economic efficiency gains promised by IT. The network requires a high degree of connectivity that arises from trust, safeguards for privacy and security, and a strategy that minimizes risks of patient data misuse. With that said, the approach must be voluntary and built on the premise of patient control and authorization.

Over the last two years, *Connecting for Health* has endorsed a model in which the health information infrastructure is developed in a way that safeguards privacy, leverages both bottom-up and top-down strategies, is incremental in nature, and is based on a decentralized and federated model — an interoperable, standards-based "network of networks" built on the Internet. We recommend the inclusion of architectural, technical, and policy safeguards within the "Common Framework," to safeguard the privacy and security of patient data while at the same time permitting the rapid and accurate exchange of information among authorized users.

The "Common Framework" is a set of common standards, policies and methodologies to enable the secure transport of data to support electronic connectivity. Only by conforming to a Common Framework can we ensure that data exchange pilots, personal health records and regional systems will be able to interoperate. The creation of a non-proprietary "network of networks" based on a "Common Framework" is essential to support the rapid acceleration of electronic connectivity that will enable the flow of information to support patient care.

Based on the current work of the *Connecting for Health* Prototype, the technical aspects of the Common Framework have been identified. With this in mind, electronic transfer of PHR data can be accomplished using SOAP accessible behind SSL, secure FTP, secure e-mail, and HL7 messaging. Portable media is another transfer mechanism, and includes USB drive technology and CD ROMs. Since many health care providers are still in the paper chart world, CMS should also encourage mechanisms for manual entry into a PHR by the patient (or the patient's authorized proxy or vendor) of scanned images, documents and printed reports.

B. What data and communications standards exist for the exchange and storage of PHR data among providers, individuals, and PHR vendors?

Such standards do not exist specifically for PHR data.

The most comprehensive public report defining and discussing a PHR is **Connecting Americans to Their Healthcare**, the product of a *Connecting for Health* working group. This report serves as the key reference for an HL7 Working Group now working on interoperability between EHRs and PHRs. The HL7 PHR panel is mapping PHR functions into the recently approved HL7 EHR functional model. A first, unofficial draft of this mapping was published in Appendix B of the *Connecting for Health* report. The working group will next develop conformance criteria for the secure, electronic exchange of basic patient health summary information between EHR and PHR systems.

There are several other efforts in the standards community that, although not directly focused on PHRs, could affect PHRs in the long run:

ASTM – Continuity of Care Record (CCR): ASTM has been working to create an XML-based structure for a basic set of data required for provider-to-provider transfers of patient information in the context of referrals from one care setting to another. Its product originated with a paper patient referral form developed by the Massachusetts Medical Society. The CCR has been proposed as a common template of data fields for EHR-to-EHR data exchanges as well as PHR-to-EHR and EHR-to-PHR data exchanges.

HL7 and ASTM - Harmonization on the CCR: The two standards bodies agreed in September 2004 to create an implementation of the ASTM's CCR standard within HL7's V3 Clinical Document Architecture (CDA). HL7 is the dominant information standards body in health care and its CDA is the basis for most electronic exchange of health information among sophisticated entities. However, the harmonization effort between the two bodies has stalled. The result is that vendors wanting to implement the CCR would have to choose either an HL7 implementation guide or an ASTM implementation guide. The industry needs to agree upon a single, common standard that supports secure electronic exchange of basic summary patient information.

Medication data: RxHub – a clearinghouse created by the large pharmacy benefit managers (PBMs) – has placed its proprietary standard for pharmacy coverage lookup, formulary lookup and patient medication list into NCPDP's standards process to become the industry standard. The RxHub standard could be helpful in efforts to import and export medication data in PHRs.

Standards harmonization: DHHS and ONCHIT intend to contract with a private sector entity to identify and integrate relevant health IT standards into implementation profiles and information policies. PHR suppliers and users should be actively engaged in the harmonization activity.

We note that many individuals have created homegrown personal health records on their own computers. Although there would be considerable authentication and usability challenges, the possibility of providing direct-to-beneficiary data downloads should be explored. Such an approach would require significant instructions and explanatory materials, standard formats, and legal protections.

C. What technologies and standards should be supported by CMS?

It is outside our scope to specify detailed technology and standards approaches. However, we believe CMS has an important voice, both within HHS and for the health care community as a whole, to advocate for PHRs' inclusion as an essential part of the ongoing health information interoperability discussion, which has thus far been EHR-focused. CMS should continue working jointly with the private sector and other federal agencies to shape the standards for PHR content and functions. Not just standards are needed but also implementation guides for each information exchange or use case to achieve consistent implementation and therefore interoperability. The pilot projects proposed in this response will raise interoperability and policy issues that will be instructive to this discussion. CMS should have a particular interest in the process by which the AHIC and government contractors are expected to identify priority use cases for interoperability prototypes and other projects. Given the government's commitment to personal health records, CMS should encourage the AHIC process to include a consumer application among the priority use cases, and use that opportunity to work with other agencies, vendors, SDOs, and the private sector to evaluate the adequacy of existing standards for PHRs.

Here are some approaches to standards for which we achieved consensus within Connecting for Health:

Foundational layers: CMS would move the market forward significantly if its demonstration projects and multi-stakeholder process lead to a commonly accepted standard for authentication of beneficiaries and their proxies and to a process for capture of beneficiary authorization for data sharing with professionals and caregiver proxies. CMS should define minimum performance standards in these areas but not prescribe technology solutions, as there will continue to be innovation in both technology and best practices that should be encouraged.

Secure envelope: CMS should use Web Services as its technology standard for integration of third party applications and data into PHR applications.

Data content: CMS should consider identifying a standards development organization to harmonize the medication and clinical claims data that it makes available with industry efforts to standardize a basic health summary template (e.g., condition lists, medication lists, labs, encounters, allergies, basic demographics) for electronic data exchange. We believe that the HL7 Clinical Document Architecture process is the appropriate starting point for this harmonization.

Data codification: Long-term CMS policies should encourage provider use of accepted controlled clinical vocabularies such as ICD9-CM, CPT4, SNOMED, LOINC, NDC codes, and others. CMS should support a program to develop new standards for patient-supplied data, such as symptom reports, medication use habits, and health status measures.

3. Data Content

A. What pieces of information housed by CMS could be used to populate a PHR?

We recommend that CMS initially share the Part D medication claims data passed to CMS from the PDPs. Pilot programs should be designed to evaluate this approach for effectiveness in reducing adverse drug events, as well as other medication management goals such as appropriate generic substitutions and improved adherence. An important area to study is whether offering the medication list by itself generates significant participation by beneficiaries, or whether the list needs to be coupled with other electronic services, such as online refills and e-messaging with doctors and/or pharmacists, in order to achieve significant adoption. It may be most feasible to limit initial pilots to beneficiaries for whom Part D is the only drug benefit, saving the complexities of coordination of benefits for later-stage pilots.

Secondly, we believe CMS should view its fee-for-service claims data (encounters, procedures and diagnoses) as a potentially useful subset of data to provide to PHRs. CMS should also look at sharing data captured during the "Welcome to Medicare" physical with qualified PHR products.

The pilot projects should help CMS and its public-private collaborators develop best-practices documentation on how the data can provide the most value to beneficiaries and their health professionals.

B. How often should the information be updated?

Optimally, data would be made accessible to beneficiaries and/or their designees as soon as they become available in a "real time" environment. The more frequently the content is updated and refreshed, the greater its potential to aid patient understanding and safety as well as supply health care professionals with clinically relevant information.

Batch processing of data that CMS receives from contracted payers and PDPs will result in lag times between the date of service and its eventual population into PHRs. CMS will need to work with its data suppliers and participating PHRs to determine economically and technically scalable means to reduce the lag time as much as feasible. Pilot studies should include designs to help evaluate and answer this question. Pilot studies can also help determine whether some length of lag time may be optimal for certain types of data

(e.g., to allow a time window for a claim to be amended before its initial population into a PHR.)

C. What information, beyond claims data and clinical and functional assessment data, should CMS provide to populate a PHR?

CMS is in a strong position to collaborate with other Federal and private information suppliers to support medication safety and beneficiary education. It can assist PHR suppliers with incorporating information resources from FDA, CDC and others. The tools might include a glossary of terms, a list of USPTF medical check-up/screening test recommendations (e.g., description, reason, and frequency), and links to diet/nutrition (e.g., ADA, AHA) recommendations relevant to a patient's chronic conditions. We encourage CMS to collaborate with FDA on developing the content related to medications so that it is consistent across agencies, and ask both agencies to refer to the 1996 Keystone report on effective and useful prescription medication information.

The display should include understandable explanations of Part D coverage status information such as deductible, TrOOP status, out-of-pocket maximum, etc., as well as the status of fee-for-service claims.

D. Should CMS provide "processed" beneficiary data, or should PHR services use claims information as it is received from the provider?

In general, we believe that some translation of clinical or medication claims, supplemented by trustworthy, up-to-date patient education materials, are important components of PHRs.

It is estimated that nearly one of every two U.S. adults has difficulty understanding basic information necessary to make appropriate health decisions. This alarming statistic is not based on the struggles of lay people to understand complex clinical terminologies. It is based on a "health literacy" survey assessing U.S. adults' understanding of basic, consumer-targeted healthcare communications, such as prescription instructions, test results and insurance forms.[4] There is an even wider gap between clinical terminology used by healthcare practitioners and lay language understood by most patients. The implication for PHRs — and any consumer-targeted health communications — is the importance of simplicity in language and user interface.

However, it is not clear that CMS should be the translator of clinical lexicons into consumer language or the provider of interpretations of raw data, which would represent a significant expansion of the CMS role. Many private sector organizations have

[4] Lynn Nielsen-Bohlman, Allison M. Panzer, David A. Kindig, *Editors*. **Health Literacy: A Prescription to End Confusion.** Committee on Health Literacy, Institute of Medicine, 2004. Viewed online 4 June 2004 at http://www.iom.edu/report.asp?id=19723

expertise in translating claims-based lexicons into more consumer-friendly language. We are concerned, nonetheless, that any translation process will have a potential for error due to misinterpretation or misrepresentation.

We recommend that pilot projects be designed specifically to address questions of the level of processing and translating of claims data necessary to provide value to beneficiaries. We suggest that CMS consider asking AHRQ and/or other HHS agencies to develop research guidelines that CMS could include in its contracts with participating PHR suppliers to improve understanding of beneficiary needs.

4. Marketing and Training

A. Is the market ready for increased use of PHRs? If not, how can CMS encourage growth of the market?

The early private sector PHR experience demonstrates formidable challenges in stimulating utilization among all ages. Today's seniors are unlikely to adopt personal health records in large numbers until they understand and have access to specific functions that provide them with value. Practical, visible demonstration projects will provide the best means of educating Medicare beneficiaries that a PHR can offer them benefits while also building evaluative data to guide future CMS actions.

Connecting for Health's research has found that although interest in the electronic PHR concept declines with age, still one-third of people over 65 with at least one chronic condition "strongly agreed" with the statement: "I'd like to have all my health information in one place - and get to it with the click of a mouse."[5]

The table below demonstrates a marked difference between current retirees and those retiring in the next two decades. The source is a 2004 *Connecting for Health* telephone survey of 1750 adults in which respondents were asked about their interest in PHRs featuring different service emphases.

[5] "Connecting Americans to Their Healthcare," p. 127.

	Now imagine this new service comes with two additional functions. Please select **TWO** of the following choices that most interest you:					
	An online tool to keep track of all your health-related expenses, such as deductibles and co-pays?	An online tool to keep track of all of your medications and order refills?	An online tool to send your health information into the doctor's office ahead of your appointments?	An online tool to ask questions and communicate with your doctor?	None of the above	Don't know
46-65 (n=672)	42%	46%	38%	44%	32%	19%
over 65 (n=580)	18%	28%	22%	28%	58%	71%

Note that the retirees of the future have almost double the interest in PHR-related services.

Other studies have found that interest in using online medical records is not confined to a white middle class population.[6] Rather, Internet familiarity (not age, ethnicity or socioeconomic level) was the primary predictor of interest. Internet familiarity is of course growing among the older adult population as the Baby Boom generation retires. Finally, even when older adults have difficulty accessing personal information online, it's common that younger family members assist in their care (and could do so more effectively if they had proxy access to their older loved one's PHR). Family caregivers, particularly the offspring and their spouses of Medicare beneficiaries, must be considered a critical audience segment of early adopters.

In sum, we know that the Medicare population is diverse, and we have sufficient evidence that PHRs can be helpful in fulfilling specific needs. This suggests that CMS perform or commission segmentation analyses of its population, with the initial objective of identifying important subpopulations of early adopters. The importance of early adopters is a well-documented stage of gaining broader acceptance of new technologies.

CMS should develop this program with special consideration for meeting the needs of selected subpopulations, including those in the Chronic Care Improvement Program and beneficiaries under 65 with disability coverage (who have enormous information management challenges). We recommend multiple geographic pilots and non-geographic pilots for specific subpopulations. CMS should look at its total array of roles — including working with states on Medicaid and SCHIP, its investment in the dual-eligible program, its beneficiary education activities and the QIOs — and look for opportunities to stimulate PHR adoption through collaboration with the states and other partners.

[6] Ross SE, Todd J, Moore LA Beaty BL, Wittevrongel L, Lin CT, Expectations of Patients and Physicians Regarding Patient- Accessible Medical Records, JMIR 7(2): e13.

B. What efforts should be undertaken to inform CMS beneficiaries about the benefits of PHRs?

CMS can raise awareness about the importance of keeping a medication list and sharing it with doctors. (For example, one of our collaborators suggested a campaign titled "Know it, SHOW it" to encourage seniors to keep their medication list and show it to providers before any new prescription is written.)

The educational campaigns should initially be tied to pilot projects. Entities that win pilot grants could be required to do systematic outreach campaigns to enlist beneficiaries and to provide CMS with regular monitoring data on adoption, utilization and satisfaction rates. See Section 4E below for a recommendation on developing common evaluation protocols across the pilots.

C. How can CMS encourage the appropriate use of PHRs by beneficiaries?

Through the pilots, CMS should educate by offering specific, visible, high-value services rather than by "preaching." Providing beneficiaries with access to their own medication or claims information, for example, will be more effective than media promotion alone.

The pilots must serve to educate and gain feedback from beneficiaries or their proxies about the process of information retrieval and exchange, including authorization, authentication, auditing of access, data interpretation, and error correction.

D. How can beneficiaries be trained on the use and maintenance of PHRs?

CMS should look first to lessons learned at the VA's MyHealtheVet program. There is also a growing body of experience in Europe and other countries regarding the consumer response to PHRs. CMS should also convene a creative session with successful private-sector consumer applications, such as Amazon, Google, eBay, Orbitz and Intuit. In general, however, we recommend that PHR products be offered by health care organizations and other third-parties and not by CMS itself. Necessarily, the training and optimal use of each PHR product should be documented and supported by the PHR suppliers. CMS should focus its training concerns on use of the beneficiary portal and its expanded functions, and sharing best practice information regarding beneficiary behavior with the larger PHR community.

E. Who can CMS best partner with to better publicize PHRs?

CMS should commission the development of common evaluation criteria and minimum survey sets to measure the effectiveness of its pilots. CMS could consider engaging its Advisory Panel on Medicare Education to develop a common evaluation framework for

privacy education, PHR adoption, utilization, and satisfaction as well as PHR impact on patient education and medication and clinical service utilization.

CMS should view as partners the many health care stakeholders who have already invested in PHRs, including employers, plans, hospitals, clinics, PBMs and commercial vendors. A key goal should be to get physicians and other health care professionals on board, since patients now and in the future will look to them primarily for data, confidence and advice.

CMS should not limit itself too much or too early in working with third-party organizations and collaborative bodies to find effective policies to promote beneficial use of PHRs. Achieving the broad national goal of PHR availability and adoption will necessitate close cooperation between the public and private sectors. CMS can play a key role as stimulant and convener, and by focusing attention on key issues that may be roadblocks. A coordinated national communications effort which increases public awareness of PHR benefits and issues could be led by CMS but involve extensive private sector partnerships.

5. Privacy and Security of Information

As explained in our Prologue, our responses in this section are based on principles, rather than specific techniques.

A. What methods are currently being used to obtain and track authorization from individuals to use their information to create or populate PHRs?

A key characteristic of the PHR is that the patient or consumer controls access to the data within it. Although PHR models may offer varying degrees of consumer control over data-sharing functions, we believe that all PHRs should begin with a fundamental principle of control: PHRs are voluntary. That is, the relationship between a PHR supplier and an individual consumer should be based on the consumer's discretion to enter into it, and to continue it.

It is therefore critical that this voluntary relationship be shaped by the value of transparency. Our core recommendation is that PHR suppliers adopt policies of transparency and full disclosure regarding privacy, security, data exchange, and the terms and conditions of service. Further, the business model and data-mining and data-portability policies must be clearly disclosed hand-in-hand with marketing materials describing services.

The default policy for a personal health record is that the consumer controls the access: No one may access the information — either personally identifiable information or de-identified aggregate information — without the consumer's authorization. These access controls must be flexible enough to allow the consumer to authorize persistent access to trusted entities such as their Primary Care Physician, while also allowing single-use

authorization for visits to specialists or for physicians consulted while travelling. Offering such persistent access to personal physicians may raise new questions regarding mutual responsibilities or professional liability, which will need to be addressed as part of a more comprehensive health IT policy analysis.

CMS should develop specific policies with regard to secondary use of personal health information, particularly when it provides the capability for beneficiaries to download or transfer data from the CMS system to third-party (provider or commercial) systems. (See our response to 5F below.)

B. What type of authentication is used to allow an individual to access a PHR? To modify a PHR?

Determining appropriate authentication methods is a difficult balance. The essential objective of any authorization system is letting each person into the data he or she is authorized to while keeping unauthorized people out. Generally speaking, the more stringent the authentication requirements, the greater the barriers consumers face in using the system. Conversely, the less stringent the requirements, the greater the risk of unauthorized access to protected health data. For example, a PHR system must decide whether the initial establishment of an individual's identity must be in person (in which case a driver's license or other form of material identification may be viewed), or whether it can occur remotely (without any physical identification). An in-person process is likely to require more personnel and training but provide better identification, whereas a remote process can be more automated and convenient but provide weaker identification assurance.

Three methods may be used to verify an individual's identity:

1. You provide something that you **know** (e.g., a username and password or personal identification number, or PIN).

2. You provide something that you **have** (e.g., a smart card, a credit card, or some other object presumed to be in your sole possession or control).

3. You provide something that you **are** (e.g., a fingerprint, retina scan, typing behavior).

There are strengths and weaknesses to all these methods. Passwords are inexpensive to implement but are a weak means of authentication. People often use a password that is easy to remember, and thus can be more easily guessed by an intruder. Requiring "strong" passwords (a long string of characters mixing letters, digits, and punctuation marks) makes it harder for an intruder to guess, but it also may be harder for the authorized person to remember. This may encourage the authorized person to write down the strong password, again opening an opportunity for unauthorized snooping. Physical tokens are, by definition, unguessable as they rely on physical presence. However, physical tokens in any form may be lost, temporarily or permanently. And biometrics, by

being tied most directly to the user in question, are also the most potentially invasive in terms of privacy, as well as requiring significant distribution of hardware for measuring the biometrics.

In practice, most systems allowing patients to access their records held in traditional EHR systems offer some guidance. Typically these systems raise a relatively high threshold of authentication for the first use of the system, and then issue a relatively strong username and password for subsequent uses.

Some systems physically deliver a unique "starter" password to an authorized person via registered U.S. Mail. The individual can go back to the Web site to log in with the temporary PIN, then must change the username and password. (The password expires after a given period of time to lower the risk of it being usable in the wrong hands.) Other systems require an in-person visit to one of the patient's health care providers, who provides independent verification of the patient's identity, which allows the issuing of a starter password similar to the registered mail system. There has also been discussion of using the Notary Public system to raise the threshold of initial authentication in a manner similar to the use of Registered Mail.

No one system is obviously superior for all cases, but the common objective is to raise a high threshold for the initial establishment of a user's identity (registered mail, health care professional as proxy.) This allows the user to access the system for the first time, after which they can be issued a username/password combination and allowed remote network access, subject to appropriate controls such as encryption of any information requested and periodic password changes.

C. How can we assure beneficiaries that their information is adequately protected?

Protecting medical privacy and confidentiality in the context of PHRs involves a wide range of issues. Providing adequate confidence in the system will require more than the somewhat piecemeal approach to privacy that currently exists. That is why we propose and emphasize the need for a systematic and architectural solution. An architecture for privacy is being discussed and developed in the CFH Policy Subcommittee. The foundations of this architecture are the following nine principles associated with fair information practices, as endorsed within the United States and internationally (OECD, EU and Canada):

1. **Openness and Transparency**: The practices and policies that affect the way personal data is handled must be visible to all users and the process for setting those policies must be open and broadly inclusive;
2. **Purpose Specification and Minimization**: The purposes for which personal data are collected (and accessed) should be specified timely and the subsequent use limited to the fulfillment of those purposes (as are specified on each occasion of change of purpose);
3. **Collection Limitation**: Personal data should only be obtained and collected by lawful and fair means and, when appropriate, with the knowledge or consent of

the data subject;

4. **Use Limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified;
5. **Individual Participation and Control**: The individual has the right to obtain confirmation of whether or not a data controller has data relating to him/her, and is able to challenge data relating to him/her and to have personal data erased, rectified, completed or amended;
6. **Data Integrity and Quality**: Personal data should be accurate, complete, relevant and kept-up-to-date;
7. **Security Safeguards and Controls**: Reasonable security safeguards must be built to protect against data loss, unauthorized access and modification, destruction, use, or other threats to data in a digital environment;
8. **Accountability and Oversight**: Violators and data controllers should be held accountable for complying with measures that give effect to the principles stated above;
9. **Remedies**: Legal and financial remedies must exist to address significant security breaches or privacy violations.

Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy that can help overcome the current policy fragmentation and high public concern. It is critical that we consider the nine principles as part of one package. Elevating certain principles over others will simply weaken the overall architectural solution we are proposing. Consequently we recommend that CMS develop a policy regime that integrates all nine of these areas and communicate them actively to beneficiaries and to data partners — both suppliers and potential third-party PHR vendors.

D. What privacy protections do vendors now put in place to protect the information?

The vendors themselves are in best position to answer this question.

E. What security technologies do vendors currently use to protect PHR information?

The vendors themselves are in best position to answer this question.

F. Do the HIPAA privacy and security regulations (45 CFR Part 164) provide a basis for designing the privacy and security aspects for PHRs?

Privacy is a core value in medicine and in U.S. society. Unauthorized disclosure of personal medical information is not wrong because it's illegal; *it's illegal because it's wrong*. Despite its imperfections and the backlash it has generated, HIPAA sets the national floor for implementing this fundamental value and therefore must be the minimum standard for privacy and security for PHR applications, even when those applications are not offered by "covered entities."

When a PHR is offered to consumers through a covered entity, such as a health plan or healthcare provider, it is required to abide by HIPAA standards. PHR models offered directly to consumers by commercial vendors not associated with any covered entity may not be subject to HIPAA's restrictions and practices. Yet the vast majority of people are unconcerned about such fine distinctions; they just want to know their information is protected. Indeed, strong consensus on this point has been articulated by ethicists and other healthcare leaders: every person or entity with access to personally identifiable health information is ethically obliged to act as a trustee of this sensitive information. Therefore, we recommend that all PHRs voluntarily adopt strict privacy policies and practices and provide clear advance notice of these policies and practices consistent with the HIPAA privacy rule, whether they are offered by covered entities or not.

CMS is a covered entity under HIPAA. In the specific case of CMS supplying beneficiaries' personal health information to a PHR supplier that is not already a covered entity under HIPAA, at least two actions must first occur:

1. The beneficiary must specifically authorize (i.e., active opt-in) CMS to provide the data to the recipient PHR entity.
2. The recipient PHR entity must have a "business associate" agreement with CMS as provided under HIPAA's business associate provision, clearly prohibiting any unauthorized secondary uses of the personal health data.

We acknowledge that a great deal still needs to be learned about wants and needs of specific populations in the area of privacy and security. It would be highly beneficial for the pilot projects to be designed to learn about the privacy preferences of Medicare audience subpopulations.

APPENDIX A

CONNECTING FOR HEALTH STEERING GROUP

***Note**: Federal officials (indicated with a *) are members of the Steering Group but did not participate in the development of this response.*

Lead

Carol Diamond, MD, MPH
Managing Director, Health Program
Markle Foundation
Chair, Connecting for Health

Members

Peter A. Andersen, MD
Senior Program Manager
Lockheed Martin Information Technology

William Braithwaite MD
Senior Vice President and Chief Medical Officer
eHealth Initiative
Co-Chair, Policy Sub-Committee

Claire Broome, MD *
Senior Advisor, Integrated Health Information Systems
Centers for Disease Control and Prevention

Gary Christopherson *
Senior Advisor to the Under Secretary
Veterans Health Administration,
Department of Veterans Affairs

Carolyn Clancy, MD *
Director
Agency for Healthcare Research and Quality

Janet Corrigan, PhD
President & Chief Executive Office
National Committee for Quality Health Care

Michael Cummins
Chief Information Officer
VHA Inc.

Francois de Brantes
Program Leader, Health Care Initiatives
GE Corporate Headquarters

Mary Jo Deering, PhD *
Director for Informatics Dissemination
NCI Center for Bioinformatics
National Cancer Institute

Don E. Detmer, MD
President and CEO
American Medical Informatics Association (AMIA)

David Epstein
Director, Solution Development - Public Sector
IBM

Colin Evans
Director Policy & Standards, Digital Health Group,
Intel Corporation

Mark Frisse, MD, MBA, MSc
Accenture Professor and Director, Tennessee Volunteer eHealth Initiative
Vanderbilt Center for Better Health
Co-Chair, Policy Sub-Committee

Daniel Garrett
Vice President, Managing Partner, Global Healthcare Leader
Computer Sciences Corporation
Vice Chair, Connecting for Health

J. Peter Geerlofs, MD
Chief Medical Officer
Allscripts Healthcare Solutions

John Glaser, PhD
Vice President and Chief Information Officer
Partners HealthCare System

John Halamka, MD
Chief Information Officer
CareGroup Healthcare System

William Edward Hammond, PhD
Professor, Community and Family Medicine
Duke University

Linda Harris, Ph.D. *
Senior Health Communication Scientist
National Cancer Institute

Douglas Henley, MD
Executive Vice President
American Academy of Family Physicians

Joseph Heyman, MD
Secretary
American Medical Association

Yin Ho, MD
Director eBusiness
Pfizer, Inc

Kevin Hutchinson
Chief Executive Officer
SureScripts

Michael Jackman
Chief Technology Officer, Health Imaging Group
Eastman Kodak Company

Charles Jaffe MD, PhD
Vice President, Life Sciences
SAIC

William F. Jessee, MD
President and Chief Executive Officer
MGMA

Michael Kappel
Senior Vice President, Government Strategy and Relations
McKesson Corporation

Brian F Keaton, MD
Vice President
American College of Emergency Physicians

Linda Kloss, RHIA, CAE
Executive Vice President and Chief Executive Officer
AHIMA

Allan M. Korn, MD
Senior Vice President - Clinical Affairs
Blue Cross Blue Shield Association

David Lansky, PhD
Director, Health Program
Markle Foundation
Chair, Personal Health Technology Council

Gail Latimer, MSN, RN
Vice President, Chief Nursing Officer
Siemens Health Services

Mark Leavitt, MD, PhD, FHIMSS
Medical Director/ Director of Ambulatory Care
HIMSS
Co-Chair, Strategy Sub-Committee

Josh Lemieux
Omnimedix Institute

Randy Levin, MD *
Associate Director for Electronic Submissions
Food and Drug Administration

Gary Levine
Senior Director, Business Planning & Development
Medco Health Solutions

Jack Lewin, MD
President
California Medical Association

Stephen Lieber, CAE
President
HIMSS

John Lumpkin, MD MPH
Senior Vice President, Director, Health Care Group
Robert Wood Johnson Foundation and
Vice Chair, Connecting for Health

Patricia MacTaggart
Vice President, Executive State and Local Government
EDS

Janet Marchibroda
Executive Director, Foundation for eHealth Initiative
Chief Executive Officer, eHealth Initiative
Co-Chair, Strategy Sub-Committee

Howard Messing
President
Meditech

Arnold Milstein, MD, MPH
Medical Director
Pacific Business Group on Health, The Leapfrog Group

Margaret O'Kane
President
National Committee for Quality Assurance

Dennis S. O'Leary, MD
President
Joint Commission on Accreditation of Healthcare Organizations

J. Marc Overhage, MD
President and Chief Executive Officer, Indiana Health Information Exchange
Associate Professor of Medicine, Indiana University School of Medicine
Senior Investigator, Regenstrief Institute

Herbert Pardes, MD
Chief Executive Officer
New York-Presbyterian Hospitals, University Hospitals of Columbia and Cornell
Vice Chair, Connecting for Health

Alison Rein
Assistant Director of Food and Health Policy
National Consumers League

Russell J. Ricci, MD
Chief Medical and Strategy Officer
HealthSTAR Communications

Craig Richardson
Vice President, Health Care Connectivity and Alliances
Johnson & Johnson Pharmaceutical Services

Wes Rishel
Vice President, Research
Gartner
Board Chair, Health Level Seven

William Rollow, MD *
Deputy Director, Quality Improvement Group
Office of Clinical Standards and Quality Centers for Medicare and Medicaid Services

Steve Shihadeh
General Manager Healthcare Industry Solutions Group
Microsoft

Clay Shirky
Adjunct Professor, New York University
Graduate Interactive Telecommunications Program
Chair, Prototype Technical Sub Committee

Steve Sleigh, PhD
Director, Strategic Resources
International Association of Machine and Aerospace Workers

Michael R. Solomon
Vice President Strategic Planning & Initiatives
IDX Systems Corporation

Ellen Stovall
President
National Coalition for Cancer Survivorship

Thomas Sullivan, MD
Women's Health Center Cardiology

Paul Tang, MD
Chief Medical Information Officer
Palo Alto Medical Foundation

Robin Thomashauer
Executive Director
Council for Affordable Quality Healthcare

John Tooker, MD, MBA, FACP
Executive Vice President
American College of Physicians

Micky Tripathi
Chief Executive Officer
Massachusetts eHealth Collaborative

Charlene Underwood
Director/Government & Industry Affairs
Siemens Corporation

Robert Wah, MD, Captain MC USN *
Associate CIO for Clinical Informatics, Military Health System
Director, Information Management
Tricare Management Activity, Office of Secretary of Defense/Health Affairs

Scott Wallace
President and Chief Executive Officer
The National Alliance for Health Information Technology

Andrew Wiesenthal, MD
Associate Executive Director
The Permanente Federation

Chelle Woolley
Communications Officer
RxHub

William Yasnoff, MD, PhD
Managing Partner
NHII Advisors

Scott S. Young MD *
Director for Health Information Technology
Agency for Healthcare Research and Quality

APPENDIX B

PERSONAL HEALTH TECHNOLOGY COUNCIL

Lead

David Lansky, PhD
Senior Director, Health Program
Markle Foundation

Members

Tim Andrews
Principal
Transform Partners

Wendy Angst
General Manager
CapMed, A Division of Bio-Imaging Technologies, Inc.

Rodney Armstead, MD, FACP
Chief Executive Officer
Care 1st Health Plan Arizona

Cynthia Baur, PhD*
Senior Health Communication and e-Health Advisor
ODPHP, U.S. Department of Health and Human Services

Marc Boutin, JD
Vice President, Policy Development and Advocacy
National Health Council

Patti Brennan, PhD
Moehlman Bascom Professor- School of Nursing/College of Engineering
University of Wisconsin Madison

Helen Burstin, MD, MPH*
Director, Center for Primary Care, Prevention, and Clinical Partnerships
Agency for Healthcare Research and Quality

Carolyn Clancy, MD, PhD*
Director
Agency for Healthcare Research and Quality

Rex Cowdry, MD
Executive Director, Maryland Health Care Commission

Mary Jo Deering, PhD*
Director for Informatics Dissemination
NCI Center for Bioinformatics
National Cancer Institute

Richard Dick
Chief Executive Officer
You Take Control

Eric Dishman
General Manager, Consumer Health Platform
Intel Corporation
Digital Health Group

Stephen Downs
Senior Program Officer
Robert Wood Johnson Foundation

Joyce Dubow
Associate Director
AARP Public Policy Institute

Esther Dyson
Editor, Release 1.0
CNET Networks

Rob Epstein
Chief Medical Officer
Medco Health

Tom Ferguson, MD
Senior Associate Center for Clinical Computing
doctom.com

Craig Forman
Vice President and General Manager, Media and Information
Yahoo!

Ed Fotsch, MD
Chief Executive Officer
Medem

Peter Frishauf
Board of Directors
Healthcare Marketing & Communications Council, Inc.

Gilles Frydman
President
ACOR

Janlori Goldman
Director
Health Privacy Project

Linda Golodner
President
National Consumers League

Ken Goodman, PhD
Director, Bioethics Program
University of Miami

Linda Kloss, RHIA CAE
Executive Vice President and Chief Executive Officer
AHIMA

Missy Krasner, MA *
Senior Advisor, Programs & External Affairs
ONCHIT

Gary Levine
Senior Director, Business Planning & Development
Medco Health Solutions

Jack Mahoney, MD
Corporate Medical Director
Pitney Bowes

Bob Marotta
Senior Vice President, Legal and Regulatory
WebMD

Phil Marshall MD, MPH
Vice President, Product Strategy
WebMD

Omid Moghadam
Director of Personal Health Records Technology
Intel, Digital Health Group

Ginger Price *
My HealtheVet Program Director
Department of Veteran's Affairs

Sumit Rana
Division Manager, Clinical Products
Epic Systems Corp

Alain Rappaport, MD, PhD
Chief Executive Officer/Founder
Medstory, Inc.

Alison Rein
Assistant Director, Food & Health Policy
National Consumers League

William Rollow, MD*
Director, Quality Improvement Group
CMS

Marie Savard, MD
Health Educator and Founder
Savard Systems

Albert Shar
Vice President of Information Technology
Robert Wood Johnson Foundation

Joel Slackman
Managing Director, Office of Policy and Representation
BlueCross BlueShield Association

Justin Starren, MD
Assistant Professor of Biomedical Informatics
Columbia University

Paul Tang. MD
Chief Medical Information Officer
Palo Alto Medical Foundation / AMIA representative

Robin Thomashauer
Executive Director
Council for Affordable Quality Healthcare

Fran Visco
President
National Breast Cancer Coalition

Anne Woodbury
Managing Director
Fleishman-Hillard

Matthew Wynia, MD
Director, The Institute for Ethics
American Medical Association

**Note: Federal officials are members of the PHTC but did not participate in this collaborative response.*