PREPARED STATEMENT OF
CAROL C. DIAMOND, MD, MPH
MANAGING DIRECTOR, MARKLE FOUNDATION;
CHAIR, CONNECTING FOR HEALTH

Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs of the Senate of the United States

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

February 1, 2007

PREPARED STATEMENT OF
CAROL C. DIAMOND, MD, MPH
MANAGING DIRECTOR, MARKLE FOUNDATION;
CHAIR, CONNECTING FOR HEALTH

Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia
Committee on Homeland Security and Governmental Affairs of the Senate of the United States

PRIVATE HEALTH RECORDS: PRIVACY IMPLICATIONS OF THE FEDERAL GOVERNMENT'S HEALTH INFORMATION TECHNOLOGY INITIATIVE

February 1, 2007

Chairman Akaka, Senator Voinovich and distinguished members of the Subcommittee on Oversight of Government Management, thank you for inviting me to testify today. I am delighted to be called upon to share the Markle Foundation's insights on how information technology initiatives can enable the use of information to improve health care while protecting privacy. The report released by GAO summarizes well a number of issues regarding the current state of policy development for health information technology. Today I will address the implications of the current policy approach and propose a comprehensive privacy and security framework developed by the Markle Foundation's Connecting for Health collaboration. Our broad collaborative believes that such a Common Framework must be defined and maintained if we are to realize the goal of health information sharing environment that makes vital information available for patients and their

providers when and where it's needed, while protecting privacy and earning the trust of the American people.

THE MARKLE FOUNDATION: ADDRESSING CRITICAL PUBLIC NEEDS IN THE INFORMATION AGE

The Markle Foundation currently focuses on two areas where we believe expanded use of information technology (IT) and the improved use of information hold particular promise: the strengthening of our nation's security, and the modernization of our complex and over-burdened healthcare system. These are two of the most critical issues of our time, where the benefit to be gained from putting the right information in the right hands at the right time is enormous. In each of these areas, we know that the effective and appropriate use of IT can literally save lives. We also know that our nation's goals in both areas cannot be met without better use of IT[1].

At the same time, national security and healthcare also highlight a critical challenge we face in seeking new ways of using information: the need to protect our established values of privacy and civil liberties. Our commitment to designing new approaches to using and exchanging information must always be coupled with the development of policy and technology solutions that protect civil liberties and privacy from the outset, not as an afterthought.

If the policies and rules are not in place at the moment sensitive information, such as patient data, are collected and shared, public trust will be undermined, and in the process the very viability of electronic information collection and sharing will be threatened. In addition, we believe that these policies and business rules must be developed in a transparent, inclusive and

[1] The discussion of the objectives guiding the Markle Foundation work are based upon the 2004 letter by Zoë Baird, President of the Markle Foundation on **Addressing Critical Public Needs in the Information Age**. Available at http://www.markle.org/resources/president_letter/index.php

accountable manner; only this will ensure that the public accepts—and, indeed, embraces—new uses of technology as legitimate and desirable.

Markle has previously supported this Committee when it addressed the use of IT to improve information collection and sharing for national security purposes, while protecting critical privacy interests. Markle's Task Force on National Security in the Information Age[2], a distinguished panel of security experts spanning five administrations as well as experts on technology and civil liberties, developed a framework for improving our ability to share information while protecting privacy and civil liberties. To a significant extent, the President and Congress have now adopted a large set of recommendations suggested by the Task Force. Specifically, the Intelligence Reform and Terrorism Prevention Act of 2004, developed by this Committee and its leadership, Senators Joseph Lieberman and Susan Collins, grappled with these issues when it called for the creation of a trusted information sharing environment with Attributes and privacy policies encouraged by the Markle Task Force.

Many of the lessons learned and approaches taken by this Committee and its leadership in the national security area can also be applied to the focus of today's hearings: privacy and health information.

In the health area, we operate an initiative called Connecting for Health. Convened and operated by the Markle Foundation since 2002, Connecting for Health[3] works to accelerate the development of a health information-sharing environment to improve the quality and cost effectiveness of health care by bringing together private, public, and not-for-profit groups to develop common standards and policies. Together this group of leading government, industry, and health care experts have shaped and led the

[2] The Reports of the Markle Task Force on National Security in the Information Age are available at: http://www.markletaskforce.org/
[3] See http://www.connectingforhealth.org/

national debate on creating a health information-sharing environment that can make vital information available in a private and secure manner to improve the health and health care of all consumers.

In our 2004 Connecting for Health Roadmap[4], we recommended a decentralized and standards-based information network that is based on a framework of privacy and built on a model of trust, and identified a set of consensus actions to be taken by all healthcare stakeholders. In April 2006, this framework was fully documented and published, based on actual prototype implementation in Boston, Indianapolis and Mendocino County, California. The Connecting for Health Common Framework is based on a set of explicit privacy and technology principles and comprised of specific technology standards, health information policies, and model participation agreements. The model policies of the Common Framework were developed in and with the three prototype communities over the course of a year in parallel with the technical standards and architecture specifications. We convened both local stakeholders and the nation's leading experts in privacy, law, health information technology and health care delivery. The Common Framework is in the public domain and has been widely distributed and referenced[5].

The biggest lesson learned from participating in Connecting for Health for the last five years is now its guiding principle: that a sustainable environment for exchanging health information requires **technological design decisions to be developed in sync with policies and business rules that foster trust and transparency**[6].

---

[4] See **Achieving Electronic Connectivity In Healthcare**. A Preliminary Roadmap from the Nation's Public And Private-Sector Healthcare Leaders. Connecting for Health, July 2004. Available at http://www.connectingforhealth.org/resources/cfh_aech_roadmap_072004.pdf

[5] The **Common Framework** is available at http://www.connectingforhealth.org/commonframework/

[6] See **Keynote**, delivered by Zoe Baird at the Connecting Americans to Their Health Care Conference, December 8, 2006. Available at http://www.phrconference.org

We fully agree that technology and technical standards are crucial to realizing the benefits of health information sharing. But the government's greatest challenge is not finding the right technology or creating the most sophisticated technical infrastructure – it is finding agreement on the complex array of policies necessary for trustworthy information exchange. Computer systems that use the same technical standards will not move information by themselves for the care of a patient. Pushing the "send" button requires that the people who need to share information trust each other, understand and implement the necessary protections for the information they hold, and know that the information policies in place will be upheld and enforced in the event of a breach.

An explicit policy framework is as important as any effort to create technical standards. In health IT, technology standards by themselves are like an interstate highway system with no rules of the road. In order to serve the communities through which it passes, a highway must have a coherent set of rules, made obvious through signage and visibly enforced.

The converse is equally true: technology decisions made without clear information policies create information policy *de facto* - without public debate or agreement. Nowhere will this be more true than in the decisions regarding health information standards and prototype architectures for the Nationwide Health Information Network (NHIN). A design process that focuses purely on technology and standards will in fact also create health information policy. For example, decisions about where data should be stored or aggregated are also decisions about the kinds of risks to which data will be exposed. Choices among technical standards and architectures also determine whether personal health information is commingled with demographic data on the network as well as whether services and data are centralized. Make no mistake, these technical choices are all in fact health information policy decisions and they will all have implications for protecting privacy and

security. As with all significant policy decisions, the question of who has the authority to make the decision is as important as the initial policies themselves. In this case, policies that touch the most private concerns of every American can not simply be delegated to industry standard setting bodies. They must be made by a publicly accountable process. If technology is developed in advance of or in the absence of the relevant policy framework, our nation runs the risk of inappropriate uses of personal information followed by a public clamor for hasty remedies. In those circumstances, we may find ourselves retrofitting complex technologies at great costs. Experience tells us that these fixes will be inadequate, costly and operationally so difficult to implement that the policies may later be dismissed, delayed or modified because they cannot be realized. This unnecessary cycle will undermine the sustainability of a health information sharing network.

A better approach is to develop information policy alongside the technical system requirements. The challenge then is not a purely technical one. It's about finding the right technologies, standards and architectures that can implement the necessary policies to protect health information while allowing it to be shared with authorized parties.

AMERICANS SEE ELECTRONIC ACCESS TO THEIR MEDICAL INFORMATION AS A WAY TO IMPROVE QUALITY AND REDUCE HEALTH CARE COSTS IF THEIR SIGNIFICANT PRIVACY CONCERNS CAN BE ADDRESSED

If Government is unsure about the importance of these policies to the American public, it need only look at the years of public polling data that have been accumulated.

In December 2006, we released the results of a new survey on public views toward personal health records[7]. As in past years, our survey reveals a few key attitudinal themes regarding electronic personal health information. First, Americans want access to their personal health information electronically over the Internet for them and those who provide their care because they believe that the online services enabled by such access are likely to increase their quality of care. Additionally, the public sees online records as a way to increase health care efficiency by reducing unnecessary and repeated tests and procedures. A desire for more control over their health care also seems to be behind the public's interest in electronic personal health information. For instance: 97 percent think it's important for their doctors to be able to access all of their medical records in order to provide the best care; while 96 percent think it's important for individuals to be able to access all of their own medical records to manage their own health[8].

At the same time, Americans have significant **privacy concerns**, and will be reluctant to support health information exchange until these concerns are addressed in a comprehensive manner. Indeed, most respondents express concern that their medical information could be misused:

- 80 percent say they are very concerned about identify theft or fraud;
- 77 percent report being very concerned about their medical information being used for marketing purposes;
- 75 percent say the government has a role in establishing rules to protect the privacy and confidentiality of online health information;
- 66 percent say the government has a role in establishing rules by which businesses and other third parties can have access to personal health information; and

[7] Findings are available at http://www.markle.org/downloadable_assets/research_doc_120706.pdf
[8] Ibid.

- 69 percent say the government has a role in encouraging doctors and hospitals to make their personal health information available over the Internet in a secure way.

Our own surveys in the past and surveys done by others have repeatedly documented similar levels of concern:

- A Harris Interactive Survey on Medical Privacy[9] (February 2005) indicated that between 62% and 70% of adults are worried that sensitive health information might leak because of weak data security; that there could be more sharing of patients' medical information without their knowledge; that computerization could increase rather than decrease medical errors; that some people won't disclose necessary information to healthcare providers because of worries that it will be stored in computerized records; and that existing federal health privacy rules will be reduced in the name of efficiency.
- A California Health Care Foundation survey[10] (November 2005) indicated that 67% of Americans remain concerned about the privacy of their personal health information and are largely unaware of their rights.

These new risks require a comprehensive policy framework that builds privacy and security protections in from the start, rather than as post-hoc remedies. It is essential to realize that creating policies for information privacy is not a one-time effort. Information policies are no more static than technology developments; they must evolve with each new opportunity and innovation. Public trust cannot be fully accomplished by relying only on existing legal provisions such as the 1996 Health Insurance Portability and Accountability Act (HIPAA), which was created well before the advent of networked, portable health information systems and before any real

[9] Available at http://www.pandab.org/Healthtopline.pdf
[10] See http://www.chcf.org/topics/view.cfm?itemID=115694

contemplation of direct, or third party mediated electronic access to personal health information by consumers.

Some of the questions raised by GAO and with which this Committee will have to grapple include: how should these policies be developed? What is the appropriate level of oversight and public involvement? Who should have the authority to make these critical policy decisions? How will we ensure that a comprehensive policy framework applies to HIT efforts across government and within HHS, and to those in the private sector with which they interface? What are the key attributes that good information systems must uphold?

THE NEED FOR A COMMON POLICY AND TECHNOLOGY FRAMEWORK, BASED UPON PUBLIC INPUT

For the last three years, the Markle Foundation and 100 health stakeholders, from both the public and private health care sectors, the IT community and consumer advocates through the Connecting for Health Collaborative, have been developing consensus approaches toward information sharing. Our approach is based upon the shared belief that we must create **a Common Framework for secure, authorized, and private health information sharing**, so that patients and their authorized providers can have access to vital clinical data when and where they are needed.

The Connecting for Health *Common Framework* is specified in a set of 16 technical and policy guides developed by experts in information technology, health privacy law, health care delivery and policy. These guides were developed and tested in a working prototype in three different community settings in Indianapolis, Boston, and Mendocino County, California. The Common Framework specifies the necessary polices and technical standards for disparate health information networks to securely share information while protecting privacy and allowing for local autonomy and innovation.

THE ATTRIBUTES OF A COMMON FRAMEWORK

The Common Framework includes a set of Attributes that were identified to achieve the policy objectives of protecting privacy and building public trust.

I. Decentralized and Distributed Architecture

The health information sharing environment should not require the development of large centralized repositories of personal health information. Instead, it should be achieved by a decentralized "network of networks" based on common open standards with strong policy management and enforcement. The technical design was premised on leaving clinical data in the hands of those who have a direct relationship with the patient and leaving decisions about who should and should not see patient data in the hands of the patient and the physicians that are directly involved with his or her care.

II. Index that Separates Demographic from Clinical Information

Sharing information for the care of a patient from disparate information records should be accomplished with indices that show where relevant information resides but not what the information is. This approach does not require a unique patient identifier. Only those with proper authorization will then be allowed to access that information.

III. A Flexible Platform for Innovation

Creating a viable platform for innovation and new participants is critical to rapid evolution. The long-term value in an open set of standards and policies will be considerable in that it will create low barriers to entry, encourage innovation, maximize competition for privacy and security protections and reduce costs.

IV. Implement Privacy through Technology

Information technology tools should be developed and deployed to allow fast, easy, and effective implementation of our attributes for protecting privacy. These tools should create **audit trails** of who accesses the information, and prevent both the intentional and unintentional disclosure of information to unauthorized persons or entities by **building rules and permissions into the process** of accessing and distributing information. The approach to technology should create flexibility, implement strong security and promote data accuracy.

V. Nine Foundational Privacy Principles

The nine foundational privacy principles of the Connecting for Health Common Framework have been developed from the fair information practices as articulated within the United States Privacy Act and also from international privacy frameworks such as those developed internationally[11]. For each privacy principle, we suggested a corresponding question that points toward assessment criteria for e-health services:

1. **Openness and Transparency** *(Is it easy to understand what policies are in place, how they were determined, and how to make inquiries or comment? Is it clear who has access to what information for what purpose?)*

[11] The Committee should note that the questions it is considering today have also been considered by every other developed nation as it modernizes its health information systems. Our international colleagues, each working within their own political system and context, have come to very similar conclusions. They have conducted broad and transparent public discussions, prepared draft policies and subjected them to vigorous debate, and often altered their technical approach to address public concerns. The resulting policies – such as those summarized in the British "Care Record Guarantee" and the Australian 10 National Privacy Principles - lay out a national commitment to privacy in language that the public can understand. See http://www.connectingforhealth.nhs.uk/crdb/docs/crs_guarantee.pdf and http://www.privacy.gov.au/publications/chib.html

2. **Purpose Specification and Minimization** (*What is the purpose of gathering these data? Are the purposes narrowly and clearly defined?)*
3. **Collection Limitation** (*Are only those data needed for the specified purposes being collected, and are subjects fully informed of what is being collected?)*
4. **Use Limitation (***Will data only be used for the purposes stated and agreed to by the subjects?)*
5. **Individual Participation and Control** (*Can an individual find out what data has been collected and exercise control over whether and with whom it is shared?)*
6. **Data Integrity and Quality** (*How are data kept current and accurate?*
7. **Security Safeguards and Controls:** (*How are the data secured against breaches, loss or unauthorized access?)*
8. **Accountability and Oversight** (*Who monitors compliance with these policies and how is the public informed about violations?)*
9. **Remedies** (*How will complaints be handled, and will consumers be able to respond to or compensated for mistakes in decisions that are based upon the data?)*

Guided by these Attributes those who implement information networks can translate them into appropriate business rules, processes and practices that are embedded in a decentralized technical architecture and fine-tuned through public input and consultation. Considered and applied together, these attributes add up to an integrated and comprehensive framework to protect privacy. Together, they can help overcome the current fragmentation of policies and the evident consumer concern over privacy.

CONCLUSION

Today's hearing takes place at a unique moment. The President, the Secretary of Health and Human Services, AHIC, the National Health Information Technology Coordinator, and literally thousands of other actors are currently considering nationally, regionally and locally how to share health information using information technology.

Notwithstanding the current momentum and unified call for investment in health care information technology infrastructure, today we are missing a strong policy framework that would protect peoples' health information. Without the implementation of such a policy framework, accelerating the flow of health information could jeopardize the public's trust in a nationwide information exchange network. Current public concerns about identity theft and the broader dangers of breaches could lead to inadequate participation in health information sharing and a setback to our current window of opportunity to transform health care.

Congress, the administration and all parts of government have a critical role to play to ensure that personal health information can move where and when it's needed while also building public confidence in the privacy and security of our system. **Our key recommendations are**:

First, any government health information technology (health IT) initiative should be based on a privacy framework with the Attributes set forth in this testimony. Federally funded initiatives should be measured against metrics derived from each one of the Attributes of the framework.

Second, Congress is now considering the statutory authority of the Office of the National Coordinator for Health Information Technology (ONC) in the Department of Health and Human Services, the American Health Information

Community (AHIC) and other coordinating and oversight bodies. As it does so, it should appreciate that while these entities have been useful to initiate action in this field, we now need to determine the appropriate longer-term processes for making policy decisions and the technology determinations that implement them. Our national strategy for health IT must be executed by decision makers informed by, and accountable to, a broad range of interests—in particular decision makers that have direct public accountability. We must assure that all stakeholders and the American public are fully included in the policy and oversight processes. This should include an independent mechanism with high public visibility to receive public complaints and handle disputes such as the chief privacy officers, ombudsmen or inspectors general that have been established for other purposes.

If we cannot accelerate the use of information technology for health information sharing, we will fail to address our health care challenges. We need the right policies to provide privacy and security, we need transparent oversight, and we need accountability.

I thank you for the invitation to appear. It has been a privilege to chair Connecting for Health, where so many dedicated individuals have worked together to recommend a Common Framework that accelerates the use of information to improve health and health care while protecting consumer privacy. I look forward to working with you to create a sustainable information-sharing environment for health care.

Thank you.

Carol C. Diamond

Appendix: Implementing the Nine Privacy Principles

Privacy Architectural Principles[12]	Policies and Procedures in a Networked Health Information Environment	Use of Technology for Privacy Protection[13]
Openness and Transparency *There should be a general policy of openness about developments, practices, and policies with respect to personal data. Individuals should be able to know what information exists about them, the purpose of its use, who can access and use it, and where it resides.*	– Transparency and tracking policies; – Collection and uses of personal data; – Adequate proper notice of privacy practices; – Disclosure procedures to individuals of security breaches; – Outreach and public education efforts to enhance awareness of privacy issues and privacy rights,	– Standards and technologies for expressing policies; – Standards and technologies for discovering policies once an institution's HIPAA provider number is known; – Defenses against people using transparency as an opportunity for phishing.[14]

[12] Considered and applied together, these principles add up to an integrated and comprehensive approach to privacy necessary for a connected health information exchange environment. **It is critical that the nine principles are considered as part of one package—elevating certain principles over others will simply weaken the overall architectural solution to privacy protection in a networked health information environment**.

[13] The use of technology for privacy protection depends to a large extent on the level of automatization of the envisaged process.

[14] Phishing is a tool used to gain personal information for purposes of identity theft. It involves using (fraudulent) e-mail messages that appear to come from legitimate businesses.

	as well as the risks and benefits of a networked environment.	
Purpose Specification and Minimization The purposes for which personal data are collected should be specified at the time of collection, and the subsequent use should be limited to those purposes or others that are specified on each occasion of change of purpose.	– Define acceptable uses of the system; – Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement); – Develop policies requiring that data collected for one purpose should not be used for another; – Implement a minimization requirement.	– Audit and logging technologies (including versioning); – Standards for expressing uses.

Collection Limitation Personal health information should only be collected for specified purposes, should be obtained by lawful and fair means and, where possible, with the knowledge or consent of the data subject.	– Define purposes of collection and of access for separate users such as: health care provider; health plan; public health authority; other government agency (law enforcement); researchers; individuals accessing their own health information; contractors and vendors (these might have a separate agreement).	– Separation of clinical and demographic information.
Use Limitation Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified.	– Define acceptable uses of the system; – Decisions about linking and sharing are to be made by the participating institutions and providers at the edges of the network; – "User" limitation: different categories of users to be governed by different rules based upon separate use agreements; – Some data may not be shared because of special sensitivity (e.g., alcohol/drug abuse history, psychiatric treatment); – Patient authorization procedures need to be clarified and	– Technologies for de-identification; – Technologies for data aggregation; – Security to prevent unintended disclosures; – Limiting queries.

	streamlined; – Permitted disclosures need to be clarified (e.g., disclosure to health care providers for purposes of treatment, disclosure to health plans for payment); – Define reuse exceptions in cases of national security or law enforcement; – Use and disclosure for management and administration of Sub-Network Organizations (SNOs).	
Individual Participation and Control Individuals should control access to their personal information; *Individuals should be able to obtain from each entity that controls personal health data, information about whether or not the entity has data relating to them.* Individuals should have the right to:	– Patient authorization procedures; – Patient access to information procedures when information is: • Maintained by provider • Maintained by third party vendor; – User's responsibility w/r/t consent prior to sharing data; – Need for meaningful and clear patient control clauses that do not present "all or nothing" choices; – Consider ways to enhance patient control; – Clarify new liability issues arising from greater individual control;	– Differing degrees of control should be built into technology; – Users should be able to choose the level of control and necessary tradeoffs that are acceptable to them; – Defenses against phishing and data theft (through user authentication).

– *Have personal data relating to them communicated within a reasonable time (at an affordable charge, if any), and in a form that is readily understandable;* – *Be given reasons if a request (as described above) is denied, and be able to challenge such denial; and* – *Challenge data relating to them and have it rectified, completed, or amended.*	– Policies by which data may be withheld at direction of patient; – Requirement to draft consent and authorization forms in clear language, easily understandable to users.	
Data Integrity and Quality All personal data collected should be relevant to the purposes for which they are to be used and should be accurate, complete, and current.	– Policies to ensure accuracy, consistency, and completeness of data; – Check their information and correct any errors (possibly model on Fair Credit Reporting Act); – Patient should be able to correct context of data use as well as content of data (i.e., they should	– Practices to ensure quality, accuracy, and availability, including backups, integrity checks, and periodic sampling; – Technical methods for allowing an individual to access and review his/her health record.

	be able to correct any misuse of data); – Clarify the SNO's liability in the case of: • Failure of the system to operate as expected or at all; • Loss or corruption of data within the system; • Incomplete or inaccurate data; • Misuse of the system by others, including other users; • Breach of security of the system.	
Security Safeguards and Controls Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure.	– Authorizing, managing, and policing access to information in the system by all categories of users; – Clear security policies (User's responsibility to implement reasonable and appropriate measures to maintain the security of the system and to notify the SNO of breaches in security, including any specific measures required by the SNO's policies and procedures); – Policies to handle intra- and extra-community matching	– Matching algorithm and thresholds; – Authentication of users; – Encryption technologies; – Auditing, service management, and logging.

	issues.	
Accountability and Oversight Entities in control of personal health data must be held accountable for implementing these information practices.	– Contract administration; – Policies by which the user has clear and sole responsibility for use of the system and actions taken in reliance on data in the system; – Consider mandating a position of Chief Privacy Officer (CPO) in organizations; – Clear user enrollment and termination procedures; – Designate someone responsible for ensuring patients' rights, such as access and amendment.	– Logging tools; – Auditing tools (including versioning); – Tracking systems; – Standards and technologies for allowing remote institutions to identify those accessing data at the individual level.
Remedies Legal and financial remedies must exist to address any security breaches or privacy violations.	– Policy and remedies for unauthorized disclosures.	– Web site with information about how patients can identify and pursue possible remedies.

Appendix: Connecting for Health, Steering Group Participants

Markle Foundation
Connecting for Health…A Public Private Collaborative
www.connectingforhealth.org
STEERING GROUP MEMBERSHIP (as of 12/06)

Antoine A. Agassi
Director and Chair
State of Tennessee eHealth Council

Peter A. Andersen, MD
Public Health and Clinical Informatics Officer, Relationship Manager
Lockheed Martin Corporation

Zoë Baird
President
Markle Foundation (ex-officio)

Robert B. Bogin, MD
Managing Director
Strategy and Collaborations Health Promotions Department
American Cancer Society

William Braithwaite MD
Former Senior Vice President and Chief Medical Officer
eHealth Initiative

Carolyn Clancy, MD
Director
Agency for Healthcare Research and Quality

Janet Corrigan, PhD
President and Chief Executive Officer
National Quality Forum

Mike Cummins
Chief Information Officer
VHA, Inc.

Mary Jo Deering, PhD
Director for Informatics Dissemination
Center for Bioinformatics
National Cancer Institute
National Institutes of Health, USDHHS

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

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

Mark Frisse, MD, MBA, MSc
Director, Regional Informatics
Vanderbilt Center for Better Health

Daniel Garrett
Former Vice President, Managing Partner, Global Health Solutions
Computer Sciences Corporation

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

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

Janlori Goldman JD
Director, Health Privacy Project

John Halamka, MD
Chief Information Officer
CareGroup Healthcare System

Linda Harris, PhD
Senior Health Communication Advisor
Office of Disease Prevention and Health Promotion
Office of the Secretary, HHS

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

Joseph Heyman, MD
Trustee
American Medical Association

Gerald Hinkley, JD
Partner
Davis Wright Tremaine LLP

Yin Ho, MD
Director, eBusiness
Pfizer, Inc.

Kevin Hutchinson
Chief Executive Officer
SureScripts

Michael Jackman
Chief Technology Officer, Health Imaging
Eastman Kodak Company

William F. Jessee, MD
President and Chief Executive Officer
Medical Group Management Association

Y. Michele Kang
Vice President and General Manager, Health Solutions
Northrop Grumman Corporation

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

Brian F. Keaton, MD, FACEP
Attending Physician/EM Informatics Director
Summa Health System
President, American College of Emergency Physicians

Linda Kloss, RHIA, CAE
Executive Vice President and Chief Executive Officer
American Health Information Management Association

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

David Lansky, PhD
Senior Director, Health Program
Executive Director, Personal Health Technology Initiative
Markle Foundation

Stephen Lieber, CAE
President
Healthcare Information and Management Systems Society (HIMSS)

J. P. Little
Chief Operating Officer
RxHub, LLC

John R. Lumpkin, MD MPH
Senior Vice President, Director, Health Care Group
Robert Wood Johnson Foundation

Janet M. Marchibroda
Executive Director, Foundation for eHealth Initiative
Chief Executive Officer, eHealth Initiative

Howard Messing
President
Meditech, Inc.

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

Carol Raphael
President and Chief Executive Officer
Visiting Nurse Service of New York

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

Craig Richardson
Vice President, Health Care Strategy & Development
Johnson & Johnson Health Care Systems, Inc.

Wes Rishel
Vice President and Research Area Director
Gartner, Inc.

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

David Schulke
Executive Vice President
The American Health Quality Association

Steve Shihadeh
General Manager
Health Solutions Group
Microsoft, Inc.

Clay Shirky
Adjunct Professor
New York University
Graduate Interactive Telecommunications Program

Ellen Stovall
President
National Coalition for Cancer Survivorship

Thomas Sullivan, MD
Past President, Massachusetts Medical Society
Women's Health Center Cardiology
American Medical Association, Council on Medical Service
DrFirst.com Officer

Paul Tang, MD
Chief Medical Information Officer
Palo Alto Medical Foundation (PAMF), Sutter Health

Randy L. Thomas, FHIMSS
Associate Partner
Healthlink, a Division of IBM Corporation

Robin Thomashauer
Executive Director
Council for Affordable Quality Healthcare

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

Micky Tripathi
Chief Executive Officer
Massachusetts eHealth Collaborative

Charlene Underwood, MBA
Director, Government and Industry Affairs
Siemens Medical Solutions

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

Andrew Wiesenthal, MD
Associate Executive Director
The Permanente Federation

Marcy Wilder, JD
Partner
Hogan & Hartson LLP

Robert B. Williams, MD, MIS
Director, Healthcare Practice
Deloitte Consulting

Hugh Zettel
Director, Government and Industry Relations
GE Healthcare Integrated IT Solutions