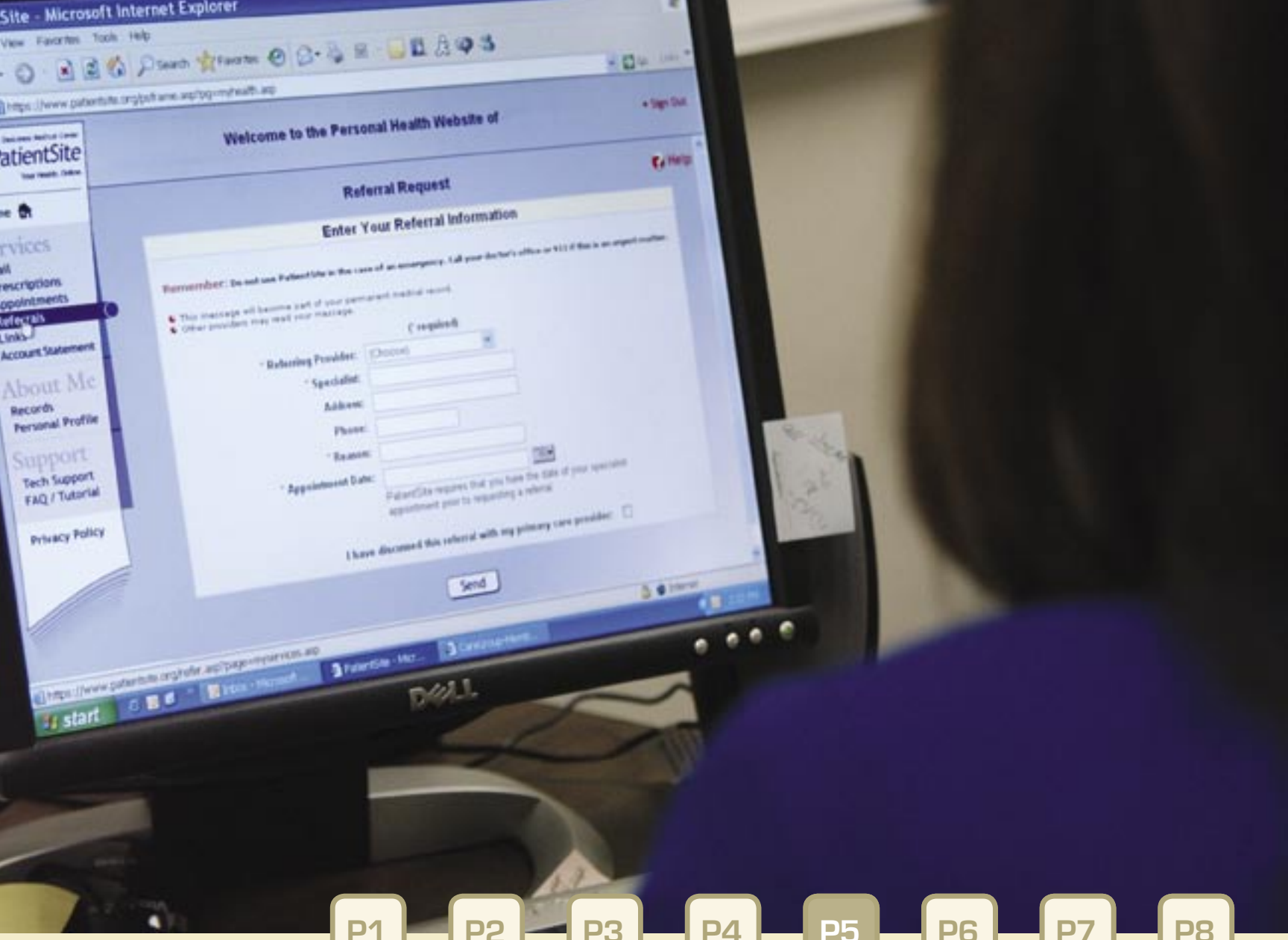


P1 P2 P3 P4 **P5** P6 P7 P8

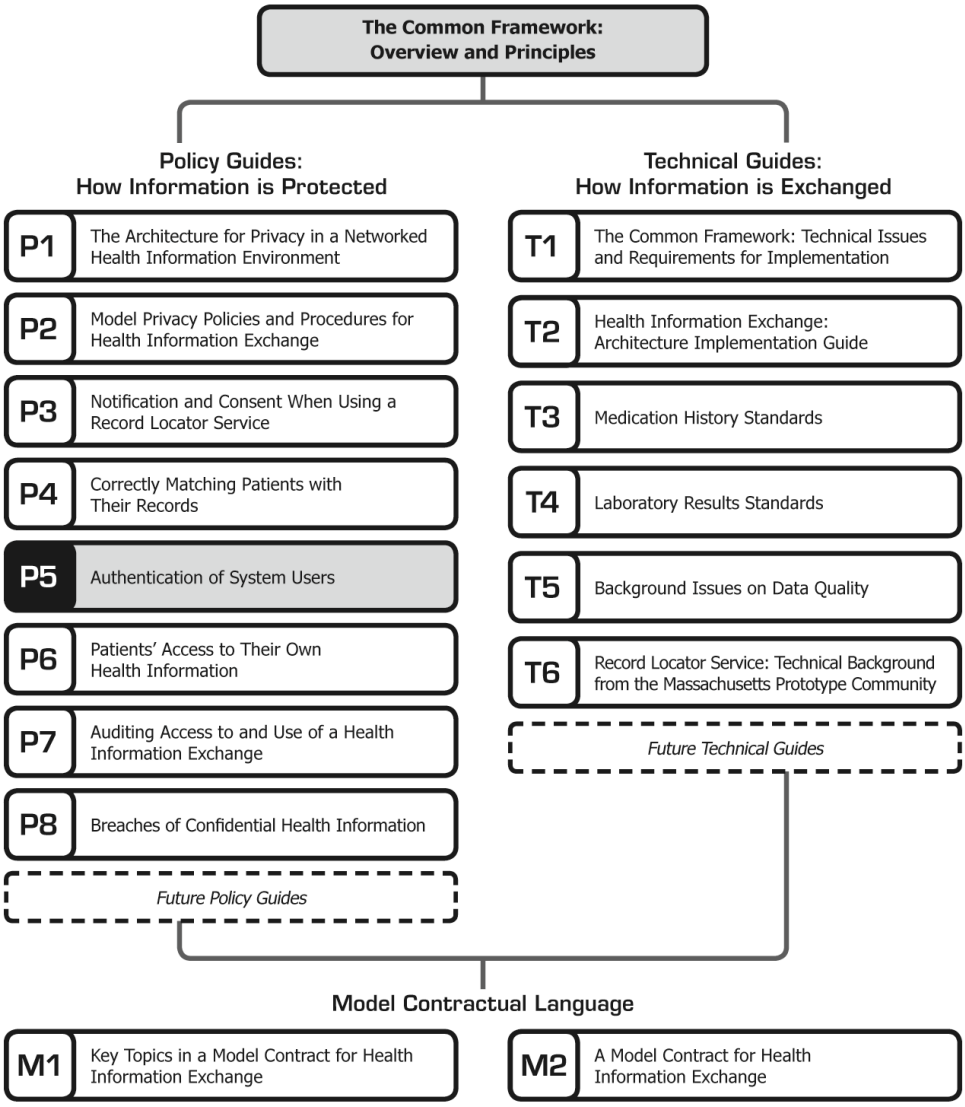
T1 T2 T3 T4 T5 T6 M1 M2

Authentication of System Users

Authentication of System Users

CONNECTING FOR HEALTH COMMON FRAMEWORK

The document you are reading is part of *The **Connecting for Health** Common Framework,* which is available in full and in its most current version at: http://www.connectingforhealth.org/. The Common Framework will be revised and expanded over time. As of April 2006, the Common Framework included the following published components:



Authentication of System Users*

This document describes the policy considerations for handling identity, authentication, and authorization issues in the **Connecting for Health** Common Framework. Every sub-network organization (SNO)[1] will need to define particular policies related to these issues which must take into account both the basic requirements laid out here, and the local conditions among the SNO's members.

Identity, authentication, and authorization can be thought of as the answers to a quartet of questions:

- Who am I? (Identity)
- How is that identity represented? (Identifiers)
- How can I prove who I am? (Authentication)
- What can I do when I've proved who I am? (Authorization)

Though the differences among these questions are relatively simple, they are often confused in the literature. It is critical that any SNO implementing the **Connecting for Health** Common Framework make plans to address all four questions, and to handle them separately, with regard to their unique characteristics, described below under "Definitions."

This document describes the requirements of governance, not implementation. It does not cover HIPAA requirements of either the participating members, or of the SNO itself. The federal HIPAA Privacy and Security Rules provide the baseline for the **Connecting for Health** Common Framework, although in some cases greater privacy protections and individual rights are recommended by the **Connecting for Health** Policy Subcommittee. Importantly, the **Connecting for Health** Common Framework permits SNO participants to establish and follow their own more protective data management, privacy, and security policies and procedures. In addition, some customization may be necessary at the SNO and participant level to ensure consistency and compliance with applicable state and local laws.

Similarly, this document does not cover technical issues of security of either the participating members, or of the SNO itself. The variability of systems in place for securing data, and the differences in regulatory regimes for the kind of data to be secured (for example, use or non-use of Social Security Numbers (SSNs)) makes modeling the threats and possible security responses a local requirement.[2] Other than the policy minimums specified here, security issues are subject to local control. Each SNO will need to decide how much or little to require uniformly of its members, always assuming HIPAA compliance. Procedures such as password recovery, log-in protections, or two-factor authentication can be set by each entity, or standardized across the SNO.

Because of the sensitivity of patient data, unauthorized users of any electronic system for discovering, transmitting, or viewing patient data must be prevented from unauthorized access, and the users of such a system who do have authorization must be accountable for how that information is used or misused. The issuance of identifiers that point uniquely and unambiguously to persons allowed to access patient data, and the handling of both authentication and authorization for those users, are challenging problems. For the purposes of this document, identity, identifiers, authorization, and authentication are defined in

* **Connecting for Health** thanks Clay Shirky, Adjunct Professor, New York University Graduate Interactive Telecommunications Program, for drafting this paper.

[1] A sub-network organization (SNO) shall operate as a health information data exchange organization (whether regionally or affinity-based) that operates as a part of the National Health Information Network (NHIN), a nationwide environment for the electronic exchange of health information made up of a "network of networks."

[2] ISO 15408, Common Criteria for IT Security Evaluations, represents industry best practices for such modeling.

the next section.

There is no obvious parallel in the world today for an electronic health care information system in the US. Highly secure systems such as those used by defense agencies have control of both the users and the technology; systems with multiple participants and a high degree of end-user access such as the credit card clear system are tolerant of a degree of fraud that would be unacceptable in a medical context; and all such systems exclude large numbers of individuals.

The current health care system is large, heterogeneous, and fragmented. There is no one entity or small coordinated group responsible for it, yet it covers all consumers of health care services. Furthermore, it is governed by HIPAA, which sets strong national minimums for privacy and security protections of health care information, but allows local deviations to stronger protections, and in all cases has very high requirements for deterring misuse. As a result, any local solution is likely to be both contextual and temporary. The solutions adopted by any given SNO will be largely guided by the degree of technical investment already made in the region and by any local requirements that are more stringent than HIPAA, and are more likely to be adopted in response to available technologies that may change in the near future.

Given these characteristics, the policies around identity, authentication, and authorization are going to be aimed in the direction of assuring compliance with the spirit of the **Connecting for Health** Common Framework, and avoiding a small number of known errors. A more comprehensive and definitional framework will have to wait for more robust technology and more extensive real-world experience.

Definitions

Identity

Identity is, in this context, an individual person or institution that needs access to health care data, for any purpose. Crucially, an identity is not merely a role; if you want to know the identity of someone who authorized a particular prescription, you want to know that it was Dr. Smith, not just that it was a doctor.

Identifier

An identifier is an attribute that points unambiguously and uniquely to an identity. In practice, the person identifier will often be an employee ID number, or, possibly, a log-in name guaranteed unique within the scope of the institution. It is critical that such identifiers not be re-issued to other, later users. If "jsmith" is used as an identifier, all future John or Jane Smiths must be issued a different identifier. (Note that this policy will require a tightening of existing policy for those institutions that currently allow for re-use of identifiers.)

An identifier is an abstract attribute and generated attribute of a particular person or entity, in the case of institutional identifiers. Tokens that refer to roles such as "Primary Care Physician," or those referring to institutional relations such as "Admitting Privileges at General Hospital" are not considered identifiers in this context.

The problem is often expressed in terms of issuing identities, which means, in practice, issuing unique identifiers that correspond uniquely and unambiguously to an existing identity, in the manner of providing an employee ID or unique login.

Authentication

Authentication requires an identifier, and is required for authorization. Authentication is a way of allowing a user to prove that he is who he claims to be. The simplest form of authentication is in the providing of an identifying token, plus a secret of some sort, such as a bank card + PIN, or a username + password or phrase.

An example of how *not* to handle authentication is the SSN. One of the reasons the SSN has turned out to be a bad identifier is that one number is meant to provide the function of both the public and secret parts of authentication: you have an SSN that points uniquely to you, but you must reveal it as proof that you have it. Without being accompanied by a second, secret token such as a PIN, the SSN is damaged in regard to authentication by the very use that makes it otherwise worthwhile.

Authorization

After a user claiming a given identity has been authenticated, an authorization mechanism

needs to determine what data the user is allowed to access and what functions may be performed by the user on that data, e.g., to view, copy, or update data. Authorization is typically role-based; that is, the different operations available are tied to the role of the user, such as physician, administrative support, etc. One individual can have many roles within the system (for example, Primary Care Physician, Admitting Physician, Specialist, etc.).

In the event of a health care emergency, some method may be provided to allow access in the event of an authentication failure as a kind of "Break the Glass" function on an existing account. However, role-based authorization is not sufficient for use of the system; no access to the system should be allowed for any such role without a human identifier attached. It is not enough to ask that someone prove that they have admitting privileges at General Hospital; they must also provide their actual identity, so that should a later audit be required, a person can be associated with the audited actions, not just a role.

A Note on Auditing

Though the handling of identity, identifiers, authentication, and authorization is often lumped together with issues of auditing, these issues are best approached separately. Auditing is required simply to have the ability to determine who accessed the system after the fact. Auditing as a technology is largely orthogonal to the technologies required for identity, identifiers, authentication, and authorization, and auditing is also used for unrelated requirements, such as statistical sampling of use patterns, and needs and trends analysis. The **Connecting for Health** Policy Subcommittee is publishing a separate piece on auditing requirements.[3]

Requirements

Every transaction involving patient data between institutions in a SNO will operate by transitive trust, often based in the legal requirements of a contract. The institutional members of a SNO trust one another, and therefore they trust requests from the authenticated and authorized employees of those institutions. The backbone of the transitive trust model is the ability to identify anyone violating that trust, and to link them unambiguously to the entity that gave them access.

Transitive trust is a practical rather than ideal system. Though there has been work on more elaborate federated identity systems, none are yet at a level of practicality necessary for this work, nor are they simple enough to be implemented broadly. The advantages of transitive trust are thus largely practical: it allows systems to scale upwards in the number of employees covered without forcing each institution to know about every other employee in every remote institution. The design and implementation of even a simple system of transitive trust is complex, and will be highly dependent on existing technological tools and frameworks, but all such systems should have the following basic policy restrictions:

- A SNO must have identifiers for all its participating institutions. These identifiers can be issued by the SNO, or they can be adopted from an external source (e.g. HIPAA-mandated identifiers[4]), as long as that source guarantees the uniqueness and persistence of any given identifier.

- All users must be authenticated before they are given access to any SNO-wide resource containing patient data. This may take a number of different forms: the local institutions can ask users to log in, and communicate the authenticated identifiers to other participants in the SNO, or the SNO can run authentication services itself, getting lists of users and roles from the participating institutions. This latter strategy may suffer from scaling problems, but may be useful for getting a SNO off the ground.

- Any request for data from a remote institution, an institution other than the one the user is logged in to, must be accompanied by at least two pieces of identifying information: which

[3] See **Connecting for Health**, "Auditing Access to and Use of a Health Information Exchange."

[4] 45 CFR § 162.404(a). HIPAA requires that covered health care providers comply with the specifications in § 162.410 regarding implementation of the standard unique health identifiers no later than May 23, 2007.

institution authenticated the requesting user and an identifier for that user. There are a number of ways such a system could be implemented technically, but the basic policy prescription is that, for any given request from a remote institution, the local institution should know where the request came from, and who authorized it.

- A method may be provided to allow access to patient data in the event of an authorization failure—a so-called "Break the Glass" function. Access failure for someone who should be authorized can happen for a number of reasons: he or she does not remember or have the required information or tokens for authentication; or he or she does not have permission from the system to look at or interact with the data they are requesting. Any request that allows a known user to request data they believe they need, e.g., a physician attempting to access the medication history of a patient, when the system would not otherwise give that person access, should be accompanied by a brief description of the rationale for the request.

- No matter what the cause of the authorization failure in the Break the Glass scenario, any system access must be accompanied by an identifier for that user. In no case is an otherwise unidentified "Emergency" account to be used, on the grounds that it amounts to the provisioning of a role without an accompanying person identifier.

- Any request that allows a known user to request data they believe they need, when the system would not otherwise give them access, must be accompanied by enhanced auditing and timely human review.

- The Record Locator Service itself may not offer a Break the Glass function; all such requests must go to the institutions hosting the clinical data.

- In the case of a SNO providing a method for a patient or patient representative to access his or her own records, some "bootstrapping" will be required. The initial issuing of the patient access capability must be done by a participating institution, or by a third-party recognized by the SNO. The patient can then be given a SNO-specific identifier, accompanied by an authentication method, with authorization limited to looking at his or her own material. Depending on implementation within the SNO, the patient could then access his or her records directly after having been issued such credentials, subject to local terms and conditions, and to periodic review. SNO-wide patient access requests, however handled otherwise, must carry the name of the institution that initially created the patient's identifier.

Authentication methods can be as simple or complex as the SNO requires; however, the SNO should publish minimum standards for authentication adhered to by all participating institutions, or be ready to add an additional layer of SNO-hosted authentication. The issue here, to be handled SNO by SNO, is that the less secure an authentication system is, the likelier it is to suffer from misuse, but the more secure it is, the likelier it is to suffer from non-use.

Authorization presents similar issues to authentication. The more granular such a role-based authorization system is, the better a fit can be imagined between a set of roles and any given situation, e.g., a patient's primary care physician accessing data from a hospital where they refer patients, but where they do not have admitting privileges. However, with each added element come both management complexity and the possibility of subtle and unpredictable errors.

Authorization can also be as simple as the SNO desires, with two caveats: there must be restrictions on who, if anyone, can add to or alter a record (as opposed to simply viewing it), and there must be restrictions on who can trigger any available Break the Glass functions.

When implementing identity, authentication, and authorization policies, SNOs will need to balance defensiveness, flexibility, and practicality. Defensiveness is the quality that leads a SNO to actively model and protect against threats of accidental or malicious access to or misuse of data. Flexibility is necessary because medicine is not banking—when there is a judgment call, it should be in favor of getting patient data to a clinician who needs it to provide care, even when such provisioning

requires Break the Glass functionality. Such uses of the system must be accompanied by enhanced auditing and timely human review. Finally, practicality is that set of choices which balances heightened security with adoptability. It is possible to design a system so well defended against misuse that it is defended against legitimate uses as well. As this cannot be allowed to happen, each SNO will have considerable discretion in designing its identification, authentication, and authorization policies, as long as those policies conform to the minimum standards listed here, and are subjected to annual review to ensure that they are continually improved where such improvement is practical. Such annual review is probably best done in conjunction with the mandated HIPAA security audit.

Acknowledgements

The members of the **Connecting for Health** Policy Subcommittee have accomplished an extraordinary task in less than a year's time—the development of an evolving piece of work that can serve as the core of nationwide health information exchange—the policy components of **The Common Framework**. During this time, we have been fortunate to work with respected experts in the fields of health, information technology, and privacy law, all of whom have contributed their time, energy, and expertise to a daunting enterprise. Our consultants and volunteers have worked long hours in meetings and conference calls to negotiate the intricacies of such issues as privacy, security, authentication, notification, and consent in health information exchange.We offer them our heartfelt thanks for taking on this journey with us, and look forward to the remaining work ahead.

In addition, we would like to offer special thanks to the volunteers and consultants who authored the initial drafts of this body of work—their hard work created a strong foundation upon which to focus the Subcommittee's deliberations:Stefaan Verhulst, Clay Shirky, Peter Swire, Gerry Hinkley, Allen Briskin, Marcy Wilder, William Braithwaite, and Janlori Goldman.

Finally, we must note that none of this work would have been possible without the leadership and inspiration of our co-chairs, William Braithwaite and Mark Frisse.They have led us with steady hands and determination of spirit.

Connecting for Health Policy Subcommittee

William Braithwaite, MD, eHealth Initiative, (Co-Chair)

Mark Frisse, MD, MBA, MSc, Vanderbilt Center for Better Health, (Co-Chair)

Laura Adams, Rhode Island Quality Institute

Phyllis Borzi, JD, George Washington University Medical Center

Susan Christensen*, JD, Agency for Healthcare Research and Quality, United States Department of Health and Human Services

Art Davidson, MD, MSHP, Denver Public Health

Mary Jo Deering*, PhD, National Cancer Institute/National Institutes of Health, United States Department of Health and Human Services

Jim Dempsey, JD, Center for Democracy and Technology

Hank Fanberg, Christus Health

Linda Fischetti*, RN, MS, Veterans Health Administration

Seth Foldy, MD, City of Milwaukee Health Department

Janlori Goldman, JD, Columbia College of Physicians and Surgeons

Ken Goodman, PhD, University of Miami

John Halamka, MD, CareGroup Healthcare System

Joseph Heyman, MD, American Medical Association

Gerry Hinkley, JD, Davis, Wright, Tremaine LLP

Charles Jaffe, MD, PhD, Intel Corporation

Jim Keese, Eastman Kodak Company

Linda Kloss, RHIA, CAE, American Health Information Management Association

Gil Kuperman, MD, PhD, New York-Presbyterian Hospital

Ned McCulloch, JD, IBM Corporation

Patrick McMahon, Microsoft Corporation

Omid Moghadam, Intel Corporation

Joyce Niland, PhD, City of Hope National Medical Center

Louise Novotny, Communication Workers of America

Michele O'Connor, MPA, RHIA, MPI Services Initiate

Victoria Prescott, JD, Regenstrief Institute for Healthcare

Marc A. Rodwin, JD, PhD, Suffolk University Law School

Kristen B. Rosati, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

Sara Rosenbaum, JD, George Washington University Medical Center

David A. Ross, ScD, Public Health Informatics Institute

Clay Shirky, New York University (Chair, Technical Subcommittee)

Don Simborg, MD, American Medical Informatics Association

Michael Skinner, Santa Barbara Care Data Exchange

Joel Slackman, BlueCross/BlueShield Association

Peter P. Swire, JD, Moritz College of Law, Ohio State University

Paul Tang, MD, Palo Alto Medical Foundation

Micky Tripathi, Massachusetts eHealth Collaborative

Cynthia Wark*, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

John C. Wiesendanger, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

Marcy Wilder, JD, Hogan & Hartson LLP

Scott Williams, MD, MPH, HealthInsight

Robert B. Williams, MD, MIS, Deloitte

Joy Wilson, National Conference of State Legislatures

Rochelle Woolley, RxHub

Amy Zimmerman-Levitan, MPH, Rhode Island State Department of Health

**Note: Federal employees participate in the Subcommittee but make no endorsement*