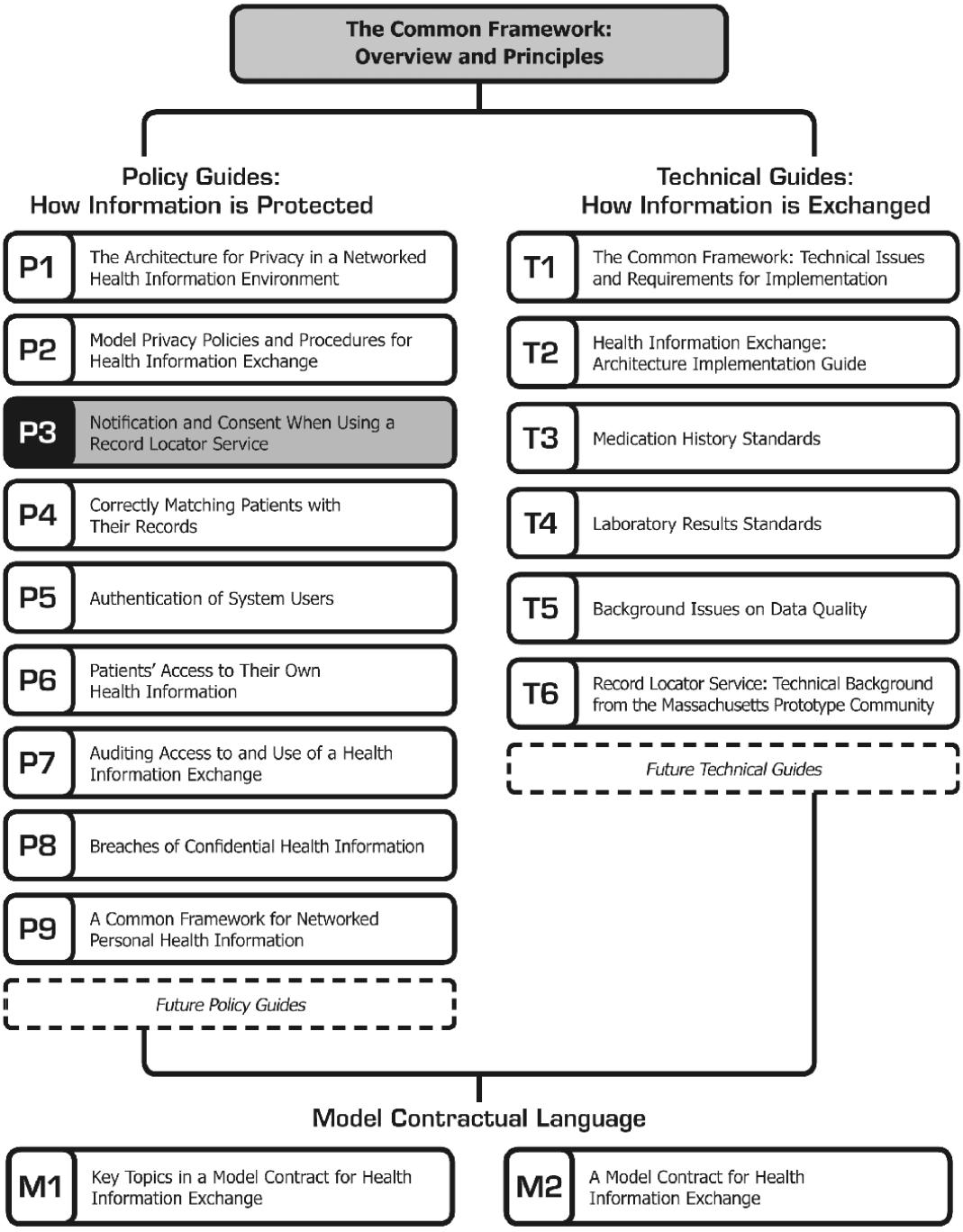
P1 P2 **P3** P4 P5 P6 P7 P8

T1 T2 T3 T4 T5 T6 M1 M2

# Notification and Consent When Using a Record Locator Service

# Notification and Consent When Using a Record Locator Service

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 October 2006, the Common Framework included the following published components:



# Notification and Consent When Using a Record Locator Service*

## Statement of Issue

Protecting medical privacy and confidentiality in the context of the Record Locator Service (RLS) involves a wide range of issues. Providing adequate confidence in the RLS will require more than a piecemeal approach to privacy. The **Connecting for Health** Policy Subcommittee therefore proposes and emphasizes the need for a systematic and architectural approach to these issues. The foundations of this approach depend on the balanced implementation of the following nine principles associated with fair information practices:

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Considered and applied together, these principles enable the development of an integrated and comprehensive approach to privacy that can be built into any information-sharing system or network at the outset in order to ensure confidentiality and privacy of patient data. It is critical that the nine principles be balanced together and considered as part of one package, as elevating certain principles over others will weaken the overall architectural solution, and no one principle can assure confidentiality and privacy of patient data on its own. It is not true, for instance, that just because patient consent (control) over the use or dissemination of information is obtained that it can alone take the place of an integrated approach to protecting the privacy of information addressed by the other eight principles. We therefore recommend that an institution or provider participating in the RLS develop an actionable policy regime that integrates all nine of the principles and communicates them actively to patients and others involved in sub-network organizations (SNOs).[1]

The particular policy question at issue in this document is: What should an institution or provider participating in the RLS be required to do to inform patients and give them the ability to decide not to be listed in the index? In addressing this question, the **Connecting for Health** Policy Subcommittee has considered in particular the principles of openness and transparency, individual participation and control, purpose specification and minimization, collection limitation, and use limitation.

While this particular document does not address the remaining principles of data integrity and quality, security safeguards and controls, accountability and oversight, or remedies, the **Connecting for Health** Policy Subcommittee has developed additional materials that do so. Please refer to the **Connecting for Health** Common Framework resources, and in particular, "A Model Contract for Health Information Exchange," "Background Issues on Data Quality," "Auditing Access to and Use of a Health Information Exchange," "Breaches of Confidential Health Information," "Authentication of System Users," and "Correctly Matching Patients with Their Records." These papers are individual elements of an integrated

* **Connecting for Health** thanks Marcy Wilder of Hogan & Hartson LLP 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."

and comprehensive policy framework that is intended to be considered in its entirety.

## Background: Structure of the Record Locator Service

Requests for protected health information will go through a two-stage process in the context of a Record Locator Service. In the first stage, a participating institution or provider ("Participant") will query the Record Locator Service ("RLS") to see if information about a particular patient exists at other participating institutions.[2] The RLS index would include only the patient name, non-clinical details used to identify the patient (name, date of birth, etc.), and participating institutions where that patient has had care. If the RLS reports that patient information exists at a participating institution, the requester may then contact the listed institution or institutions to request the clinical records, and will need to satisfy the disclosure requirements of those institutions. The RLS itself, however, would only return a pointer to the institution(s) or provider(s) holding the records, and an indication that one or more records for the patient exists at those institutions.

A hallmark of the RLS system is that the RLS index, which will contain patient names and demographic information only, will be maintained separately from any clinical records. This separation of records is a technical specification that was developed specifically to protect patient privacy. Providing transparency and individual control with regard to the RLS helps ensure that the system is adequately and securely populated with patient information so as to be a useful and viable tool, while enabling only a minimal amount of information, given its stated purpose, to be available from the RLS itself—the location of records for a given patient. Its design relies on the participating institution or provider to decide in the first instance whether to load patient information into the RLS. Moreover, it leaves the decision as to whether or not to release *clinical* records with the individual institution or provider holding the records, acting in compliance with its own disclosure policies and the stated desires of patients, when relevant. The RLS two-step approach: (1) is a key piece of the **Connecting for Health** architecture that enables the sharing of clinical information to occur without requiring it to be stored in a central repository—it enables clinical information about patients to remain in the hands of the clinicians and institutions that have a direct relationship with the patient; (2) leaves judgments about who should have access to patient information to patients and their providers; and (3) assures that the system is robust and sufficiently useful from an early stage to be considered viable. The RLS two-step process was developed in part to assure that the system would not lead to any increased exposure of personal health information while at the same time providing some early value by establishing a way to readily and efficiently locate records in order to improve health care quality and patient safety. Though clinical records and other personal information will be kept private, and not in the RLS, knowing where a patient might have other health information is a first and important step to improving the health care he or she receives.

## Background: What HIPAA Requires

The Policy Subcommittee agrees that the HIPAA Privacy Rule would permit participation in the RLS system without a provision requiring for notice to the patient or patient authorization. The Privacy Rule permits covered entities to "use or disclose protected health information for treatment, payment, or health care operations" without first obtaining an individual's authorization for such use or disclosure.[3] Treatment is defined as "the provision, coordination, or management of health care and related services by one or more health care providers."[4] Health care operations is broadly defined and includes, for example: "[c]onducting quality assessment and improvement activities, including outcomes evaluation…[and] population-based activities relating to improving health or reducing health care costs."[5] The

[2] We note that the RLS index is not a facility directory. A facility directory maintains information about the location and general condition of patients presently at or being treated by an institution whereas the RLS index identifies patients that have received care at an institution and about which the institution maintains records.

[3] 45 C.F.R. § 164.506.

[4] 45 C.F.R. § 164.501.

[5] Id. § 164.501.

information sharing that the RLS is designed to facilitate falls squarely within the HIPAA sanctioned uses and disclosures that do not require patient authorization. Therefore, the following proposed notice and patient choice policies go above and beyond what is required by the federal HIPAA privacy law and further than what a number of local and regional interoperable systems, such as the Indiana Network for Patient Care, currently require.

## Proposed Privacy Policy Architecture Regarding Posting of Information to the Record Locator Service

In accordance with the principles of openness and transparency, purpose specification and minimization, collection limitation, use limitation, and individual participation and control, discussed in detail in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment," the **Connecting for Health** Policy Subcommittee first notes that it is firmly committed to a policy supporting notice to patients and patient choice as to whether to participate in the RLS. In this regard, the **Connecting for Health** Policy Subcommittee recommends that patients be given notice that their health care provider or health plan participates in a system that provides an electronic means for locating their medical records across the providers they are seeing (the RLS). Individuals should also be provided with an opportunity to choose not to have such information about them included in the system. Moreover, the Policy Subcommittee recommends that patients should retain the ability to choose not to participate in the RLS system at any time. It is noted again that these policy recommendations apply only to patient information contained in the RLS; the decision as to whether or not to release *clinical* records in a given circumstance remains with the individual institution or provider holding the records, acting in compliance with its own disclosure policies, the stated desires of patients, when relevant, and applicable federal and state laws.

The Policy Subcommittee also understands, however, that the operational burden created by requiring that notice be given to patients *prior* to an institution's initial loading of patient information into the RLS index might not be practical in some settings and might threaten the robustness and viability of the two-step approach articulated in the **Connecting for Health** architecture. The two-step approach was designed to separate actual clinical data from information about the location of that data in order to limit risk of exposure while at the same time enabling early and significant value in health information exchange.

The Policy Subcommittee therefore proposes that information regarding patients of a participating institution generally be included in the RLS index on day one and going forward. The index would include only patient names, non-clinical details used to identify the patient (name, date of birth, etc.), and participating institutions where that patient has had care. The index would not include patient clinical records. The question of whether information regarding patients previously seen at the participating institution should be posted to the index, and the details of that information (age of information, etc.), would be left to the participating institution.

Further, the Policy Subcommittee encourages participating institutions and providers to exercise additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate. For example, institutions could choose to provide for written notice and the opportunity to choose not to participate in the RLS to patients prior to an institution's initial loading of patient information into the RLS index, either *en masse*, or on an individual basis during patient encounters. An institution or provider might also choose to contact patients via electronic means for those patients for whom it has such information. Finally, as noted above, the design of the RLS relies in the first instance on the participating institution or provider to decide whether to load patient information into the RLS at all. Additional privacy practices that participating institutions and providers might choose to implement are listed in Section B below.

**Notice of Privacy Practices.** In accordance with these recommendations, Participants must revise their HIPAA Notice of Privacy Practices to include provisions describing the RLS and to offer an opportunity for

individuals to choose not to be included in the RLS. The description must include: (1) what information is included in and made available through the RLS; (2) who is able to access information in the RLS; (3) for what purposes such information can be accessed; and (4) how the patient can choose not to have his or her information from that institution included in the RLS. All patients must be given the HIPAA Privacy Notice during their initial encounter with a provider. Many institutions provide notice at every service delivery date. In addition, the notice must be available at the institution and on request, posted "in a clear and prominent location where it is reasonable to expect individuals seeking service…to be able to read the notice," and posted on the institution's web site.

**Initial Inquiry Audit.** In a further effort to implement the principles of openness and transparency and individual participation and control, as articulated in "The Architecture for Privacy in a Networked Health Information Environment," the **Connecting for Health** Policy Subcommittee recommends that individual participants and SNOs consider and work towards implementing a system that enables an "initial inquiry audit."

In such a system, individual participants and SNOs would work towards developing a method so that the first time an inquiry is made to the RLS index regarding a particular patient, the patient would be given notice explaining that information about them is included in a system that provides an electronic means for locating their medical records across providers they are seeing (the RLS) and explaining how the patient may choose to have that information excluded from the RLS in the future.

**Patient Access to RLS Record.** In the spirit of the openness and transparency and individual participation and control principles articulated in "The Architecture for Privacy in a Networked Health Information Environment," the **Connecting for Health** Policy Subcommittee recommends that Participants and SNOs consider and work towards implementing a system wherein, upon request, patients are provided direct access to the information contained in the RLS that is about them.

The Policy Subcommittee understands that current options for direct patient access and authentication to the RLS are not robust enough to be implemented without the possibility of introducing serious vulnerability to the security of the system.

For this reason, the Policy Subcommittee recommends that, at this point, each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient's behalf.

## Analysis

*The **Connecting for Health** Policy Subcommittee's Proposal Comports with the Principles of Openness and Transparency, Purpose Specification and Minimization, Collection Limitation, Use Limitation, and Individual Participation and Control.*

A. The RLS policy enables openness, transparency, and individual participation while also addressing the **Connecting for Health** principles of purpose specification and minimization, collection limitation, and use limitation.

- Provides for patient notification by each participating institution, allowing the patient to control whether information is included in the RLS index on a participant-by-participant basis.
- Provides for the development by individual institutions and SNOs of initial inquiry audit mechanisms that would allow additional patient notification and control opportunities at time of first query.
- Provides immediate benefits, including economic benefits, on day one. Information will be more complete and system will be more robust.
- Provides the greatest likelihood of meeting the goals of saving lives and decreasing health care costs through the efficient and timely exchange of information.

- Allows participating institutions to retain complete control over when and whether clinical records are disclosed.

- Imposes less administrative burden on participating institutions.

- Enables future expansion of system.

B. The RLS policy allows institutions to implement additional privacy protections as they deem appropriate.

Posting information to the RLS using a notice and patient choice regime sets a minimum standard for privacy protections that exceeds the requirements of federal law. Moreover, as noted above, Participants retain the authority and ability to be more proactive in their patient notice and individual participation efforts. The Policy Subcommittee encourages participating institutions and providers to exercise additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate. While the Policy Subcommittee is not currently taking a position on the institution-based implementation of any of the following, such possible additional protections could include:

- Mailing a revised notice or a notification and individual choice letter to every patient prior to the loading of patient information into the RLS or shortly thereafter.

- Excluding individuals from the RLS index unless individual consent is first obtained.

- Loading patient information into the RLS on a going forward basis only (i.e., do not post information regarding treatment prior to the creation of the RLS).

- Providing a mechanism for a patient to receive, upon request, a list of:
  - All providers or institutions which have posted a patient's demographic information to the RLS; and
  - All users who have requested record locations for that patient.

- Developing a method for time-stamping an RLS record to indicate when the record was loaded to the index, if technically feasible.

- Developing a method for allowing patients to limit access to their RLS records, if technically feasible.

- Developing a method for using a single indication of the existence of one or more patient records at a single location as opposed to reporting the presence of each patient record individually.

- Seeking individual patient participation prior to each inquiry to the RLS index by the participant or on a periodic basis.

C. The RLS policy recognizes that a requirement for prior individual consent to participate in the RLS would likely jeopardize the goals of the RLS framework.

The **Connecting for Health** Policy Subcommittee carefully considered the option of requiring individual consent prior to including a patient's information in the RLS. Some parties have referred to this type of consent as "opt-in" consent. While the Policy Subcommittee is firmly committed to a policy supporting notice to patients and patient choice as to whether to participate in the RLS, it also understands that a policy requiring individual consent prior to including a patient's information in the RLS might threaten the robustness and viability of the system at an early stage, in addition to placing large burdens on the institutions and providers involved. The Policy Subcommittee carefully considered the privacy protections enabled by the RLS architecture, which separates demographic from clinical data, thus minimizing risks associated with inclusion in it, in making its decision not to recommend a policy requiring prior individual consent. In addition, as discussed in Section B above, the Policy Subcommittee encourages participating institutions and providers to implement additional privacy protections and exercise

additional means of providing for notice and patient choice with regard to participation in the RLS as they deem feasible and appropriate.

Finally, the Policy Subcommittee considered the requirements of real-world implementation of the system in addition to the following issues in making its decision not to recommend a policy requiring individual consent prior to including patients' information in the RLS:

- Requiring patients' consent to be listed in the RLS prior to their inclusion in the index would create a significant barrier to establishing a functional system. The start-up time and cost associated with obtaining such consent and populating the index would likely be prohibitive. The RLS two-step process, which separates knowing where records are located from knowing what is in them, was developed in part to assure that the system would not lead to increased exposure of personal health information while at the same time providing a way that some information would be readily and efficiently available to locate records while clinical records and other personal information would be kept private. Providing some incremental and early value is of key importance to the success and utility of the system.

- Requiring consent prior to including a patient's information in the RLS might provide an incentive to obtain a broader consent than necessary due to the time and cost associated with the process, including consent to share the entire contents of clinical records for a broad range of purposes. Such a result would over-emphasize only one of the privacy principles articulated in the **Connecting for Health** "Architecture for Privacy in a Networked Health Information Environment"—individual participation and control—and could undermine certain of the others, such as purpose specification and minimization. Such consents, in practice, might promote the consolidation of full clinical records in repositories as opposed to fostering a layered architecture that protects privacy by its very design. A requirement for prior consent before posting information to the RLS could ultimately result in reduced privacy protections because such a requirement would stimulate the use of large, consolidated databases and effectively eliminate the rationale for the RLS architecture at all.

- It is administratively and operationally burdensome for participants to obtain, maintain, and track this type of individual consent.

- An approach requiring individual consent to participate in the RLS would likely require stripping local participants of the authority and flexibility to make policies regarding when and how often consent will be obtained (e.g., each time information is queried or retrieved through the system; initially; every year, etc.) and what the policy ought to be regarding revocation of consent.

- An approach requiring individual consent prior to including a patient's information in the RLS would not permit future expansion of the system without modifying such consent and, therefore, obtaining new consent from each patient.

- An approach requiring individual consent to participate in the RLS creates impediments to use of the system for any purpose, including treatment.

- If individual consent were provided only for certain purposes (e.g., treatment only), it would be difficult to ensure that participating institutions access information only for the permitted purposes.

- If details regarding use of a changing system are not described for a patient in the individual consent materials, the consent process could be considered misleading and raise consumer protection concerns.

## 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*