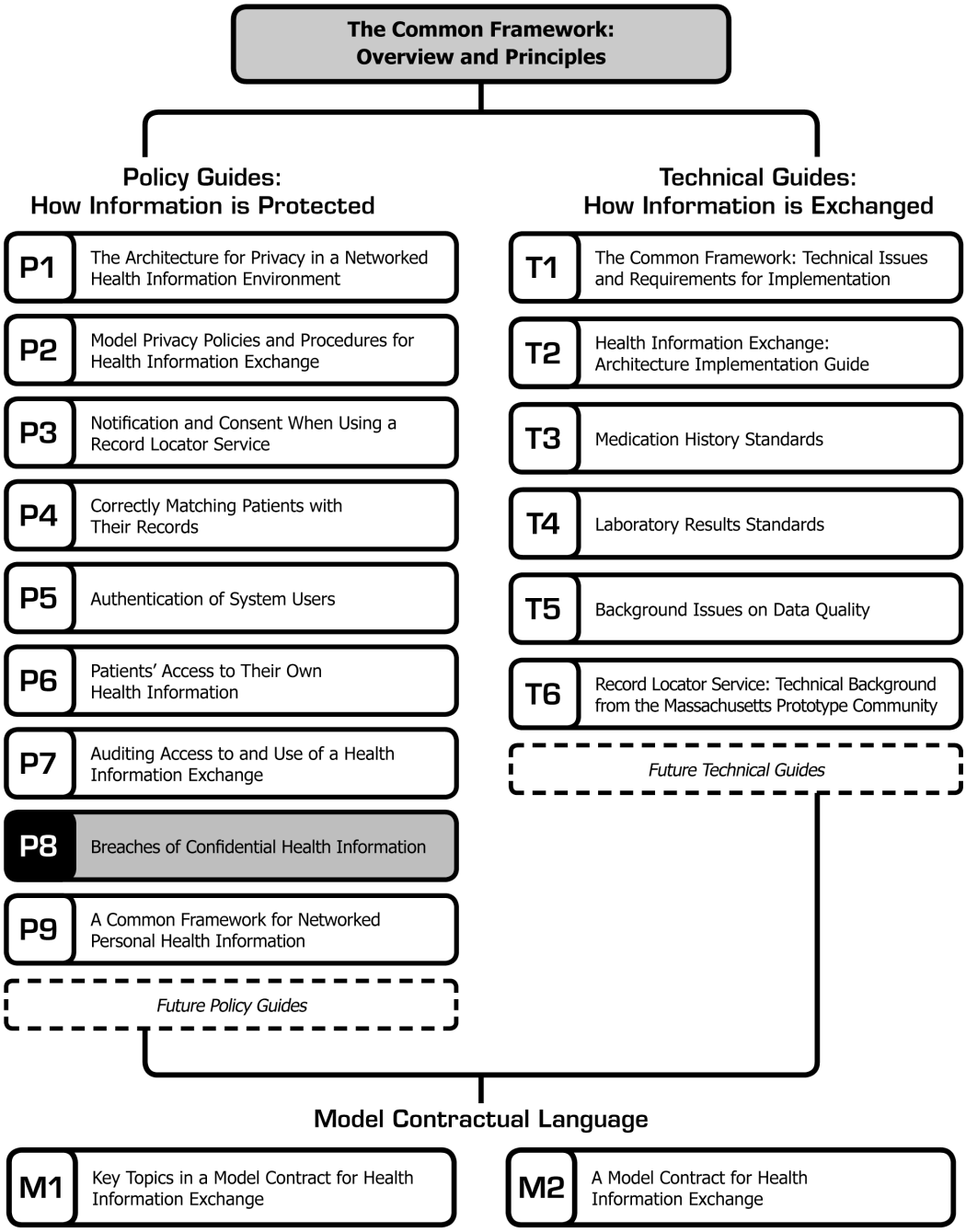
P1 P2 P3 P4 P5 P6 P7 **P8**

T1 T2 T3 T4 T5 T6 M1 M2

Breaches of Confidential Health Information

Breaches of Confidential Health Information

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:



Breaches of Confidential Health Information*

This document outlines a proposed policy for sub-network organizations (SNOs) regarding breaches of confidentiality of patient data.

Definitions

When used in this policy, the following words shall have the definitions indicated:

- *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."

- *Confidentiality* shall have the same meaning as in the HIPAA Security Rule, which is "the property that data or information is not made available or disclosed to unauthorized persons or processes."[1]

- *Breach of Confidentiality* shall mean that confidential data or information has been made available or disclosed to unauthorized persons or processes.

- *Participant* shall have the same meaning as in the **Connecting for Health** "Model Contract for Health Information Exchange," which is a party that is registered with the SNO to act as a Data Provider and/or as a Data Recipient.[2]

- *Security incident* shall have the same meaning as in the HIPAA Security Rule, which is defined broadly and includes "attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system."[3]

- *Treatment* shall have the same meaning as in the HIPAA Privacy Rule, which is "the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another."[4]

Executive Summary

This proposed SNO policy includes the following:

A. Compliance with HIPAA Security Rule: The SNO will comply with the HIPAA Security Rule. The SNO Participants will be required to comply with all applicable federal, state, and local laws.

B. Responsibility of Participants to Train Personnel and Enforce Policy: A SNO Participant that may have access to patient data via the SNO network, must appropriately train its personnel and inform them that any breach of confidentiality is actionable. Each Participant should follow and enforce its own institution's confidentiality policies and disciplinary procedures.

C. Notification of Breach: The SNO itself must report ***any*** breaches and/or security incidents to the particular data provider whose data was improperly used, as in most

* **Connecting for Health** thanks Victoria M. Prescott, General Counsel and Business Development Specialist, Regenstrief Institute for Health Care, for drafting this paper.

[1] 45 C.F.R. § 164.304.

[2] See **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 2 (Definitions).

[3] 45 C.F.R. § 164.304.

[4] 45 C.F.R. § 164.501.

cases the SNO is a business associate of some or all of its Participants. Each SNO Participant must agree to inform the SNO of any ***serious*** breach of confidentiality, but is not required to notify the SNO of minor breaches. [*Note: As mentioned earlier, any SNO policy should require that the Participants comply with all applicable federal, state, and local laws, which may include laws relating to notification of patients. Participants and SNOs should also work towards implementing a system that ensures affected patients are notified in the event of a breach.*]

D. Withdrawal from the SNO: Provisions could be included in SNO agreements relating to withdrawal from the SNO. The **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions that could allow Participants to terminate their participation freely at any time, require that termination be preceded by a substantial period of advance notice, or require that Participants maintain their participation for a certain period of time. The **Connecting for Health** "Model Contract for Health Information Exchange" also provides a model provision allowing for a Participant to withdraw from a SNO if a serious breach of its patient data has occurred.[5] SNOs and Participants are encouraged to consider the particular circumstances of small provider practices in developing relevant terms for withdrawal from SNO provisions in their SNO agreements.

E. Indemnification for Breaches of Confidentiality: The **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions concerning indemnification. A SNO may also choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information. For example, the SNO's agreement could provide for mutual indemnification between all Participants for breaches of confidentiality of patient data, with the scope of the indemnification to be determined by the SNO.

Detailed Discussion and Sample Contract Language

Compliance with HIPAA Security Rule

The SNO should comply with the HIPAA Security Rule and thus do the following: (1) ensure the confidentiality, integrity, and availability of all electronic protected health information the SNO creates, receives, maintains, or transmits; (2) protect against any reasonably anticipated threats or hazards to the security and integrity of such information; (3) protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under HIPAA; and (4) ensure compliance with this regulation by its workforce.[6] Of course, the SNO must also comply with other applicable federal, state, and local laws.[7]

Any SNO participation or vendor agreement should also require that the other parties comply with all applicable federal, state, and local laws.[8]

Responsibility of Participants to Train Personnel and Enforce Policy

The SNO policy should mandate that the SNO Participant appropriately train its personnel[9] and inform its personnel that any breach of

[5] See **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 4 (Registration Agreements).

[6] 45 C.F.R. § 164.306.

[7] This is already provided for by the **Connecting for Health** "Model Contract for Health Information Exchange," Section 9.2 (Additional Requirements).

[8] The HIPAA Security Rule may not apply to all Participants, because not all Participants are necessarily covered entities or business associates of covered entities. For example, public health is exempted from complying with the HIPAA Security Rule.

[9] Note that covered entities are already required to train their personnel with respect to protected health information pursuant to 45 C.F.R. § 164.530(b). See also **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 10.5 (Training), which has a similar requirement for all Participants, and **Connecting for Health**, "Model Privacy Policies and Procedures for Health Information Exchange," Policy 700 (Workforce, Agents, and Contractors).

confidentiality is actionable. *See relevant sample contract excerpt below*[10]*:*

> *Section 4.04 Access to Information By Participants' Personnel. Each Participant shall determine the personnel under its control (including any personnel of physician practice groups allowed to access Information pursuant to Section 4.01(b)) who may [have] access [to patient data via] the Network ... For Participants who are technically able to do so, each Participant shall provide daily electronic files to [the SNO] of the individuals it designates under this Section. If such electronic notice is not feasible, each Participant shall provide lists of such individuals through e-mail, hard copy, or facsimile to [the SNO] no less frequently than biweekly. Each Participant shall certify:*
>
> *(a) That such designated personnel have received training regarding the confidentiality of PHI under the Privacy Rule and all other applicable State and local laws and agree to protect the Information in compliance with the Privacy Rule, such laws and this Agreement;*
> *(b) That such designated personnel shall only access the Network for [allowable] purposes…;*
> *(c) That such designated personnel have agreed to hold any passwords, or other means for accessing the Network, in a confidential manner and to release them to no other individual;*
> *(d) … ; and*
> *(e) That such designated personnel agree and understand that their failure to comply with the terms of this Agreement may result in their exclusion from the Network and may constitute cause for disciplinary action by the Participant.*

Further, the SNO may also want to require that the SNO Participant enforce these confidentiality provisions by appropriately disciplining its personnel. No specific policy is set at the SNO level for Participants,[11] because each Participant should already have its own confidentiality policies and disciplinary procedures within its organization. *See relevant sample contract excerpt below:*

> *Section 5.02 Enforcement of Confidentiality by Participants. Each Participant agrees to enforce the confidentiality provisions of this Agreement by appropriately disciplining individuals within each Participant's organization who violate the confidentiality of the Information pursuant to each Participant's respective confidentiality and disciplinary policies. Such discipline may include, but not be limited to: warnings; suspensions; termination; or modification, suspension, or revocation of medical staff privileges.*

Notification of Breach

Notification of breach of confidentiality of patient data is impacted not only by HIPAA laws, but also by state breach notification laws that are becoming more common. Thus, any SNO policy should require that the Participants (and the SNO itself) comply with all applicable federal, state, and local laws.

In addition, the SNO must report any breaches to the particular data provider whose data[12] was improperly used. This would not be limited to serious breaches, but would include all breaches. Most SNOs will be a business associate of the Participants who provide patient data to the SNO, in which case the SNO is required under HIPAA to report all Security

[10] "The Indiana Network for Patient Care: A Case Study of a Successful Healthcare Data Sharing Agreement," ABA Health eSource, Volume 2 Number 1 (Sept 2005), re-printed in Healthcare Informatics Online (Sept. 28, 2005). All references in this document to "sample contract excerpt" refer to this document and are intended for illustrative purposes only.

[11] Of course, the SNO needs to establish its own internal policy for its own employees.

[12] Data here means patient data provided by the data provider to or through the SNO.

Incidents to the covered entity.[13] *See relevant sample contract excerpts below:* [14]

> *Section 8.03 Report of Improper Use or Disclosure. [The SNO] agrees promptly to report to a [Participant] any use or disclosure of the [Participant's] PHI not provided for by this Agreement of which [the SNO] becomes aware.*
>
> *and*
>
> *Section 8.14 HIPAA Security Rule Provisions.*
>
> *(a) …*
> *(b) [The SNO] agrees promptly to report to a [Participant] any Security Incident related to the [Participant's] ePHI of which [the SNO] becomes aware.*

Similarly, each Participant must agree to inform the SNO of any serious breach of confidentiality. It is not necessary for a Participant to inform the SNO of minor breaches of confidentiality (unless there is otherwise a legal duty to disclose such breaches to the SNO). While it is difficult to define what would rise to the level of a "serious" breach, SNOs and Participants might decide that the breaches of concern would be ones that impact: (1) the viability of the network, (2) the trust that other Participants have in each other, or (3) the legal liability of the SNO. In addition, SNOs and Participants might decide that repeated minor breaches that demonstrate a pattern of lax internal operations or enforcement may also rise to the level of a "serious" breach. *See relevant sample contract excerpt below:*

> *Section 5.01 Confidentiality. The Participants agree that any Information obtained from the Network will be kept confidential pursuant to the Privacy Rule and all other applicable federal, state, and local laws, statutes and regulations, as well as each Participant's own rules and regulations governing the confidentiality of patient records and information. Participants agree to report promptly to the Management Committee any serious breach of the confidentiality of the Information of which it becomes aware. …*

As mentioned above, some states have enacted laws that require the notification of individuals whose personal data is compromised.[15] Several federal bills have also been introduced that include breach notification (which could pre-empt state law if and when enacted).[16] SNOs must analyze any relevant state laws in this regard and what impact such laws may have on the SNO's operations. For example, a state law may require that a SNO notify a covered entity/Participant of a breach, but the burden to notify patients may fall on the covered entity/Participant rather than the SNO. In any event, procedures need to be in place that will address this scenario in advance of an event. Communities should be prepared to comply with evolving national norms regarding breach notification, and Participants and SNOs should work towards implementing a system that ensures affected patients are notified in the event of a breach.

Withdrawal from the SNO

SNOs may wish to consider including a provision in their Participant agreements allowing for withdrawal from the SNO. As noted above, the **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions that could allow Participants to terminate their participation freely at any

[13] 45 C.F.R. § 164.314(a)(2)(i)(C).

[14] Section 8.14 is a new amendment to Regenstrief's INPC Agreement that has not been published yet.

[15] In 2005, security breach notification legislation (also referred to as victim's rights laws) was introduced in at least 35 states. Nineteen states passed some form of legislation in this regard (including AK, CA, CT, DE, FL, GA (data brokers only), IL, IN (state agencies only), LA, ME, MN, MT, NV, NJ, NY, NC, ND, RI, TN, TX, WA). Several more state bills are under consideration. Web sites that summarize state laws include: http://www.ncsl.org/programs/lis/CIP/priv/breach.htm; http://www.sia.com/state_affairs/pdf/BreachofSecurityChart.pdf; and http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf.

[16] For federal bills introduced, see Senate Commerce Committee bill, S. 1408: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01408; Specter-Leahy bill, S. 1332: http://thomas.loc.gov/cgi-bin/bdquery/z?d109:s.01332.

time, require that termination be preceded by a substantial period of advance notice, or require that Participants maintain their participation for a certain period of time.[17] In general, SNOs and Participants are encouraged to consider the particular circumstances of small provider practices in developing relevant terms for withdrawal from SNO provisions in their SNO agreements.

The **Connecting for Health** "Model Contract for Health Information Exchange" also provides a model provision allowing for a Participant to withdraw from a SNO if a serious breach of its patient data has occurred, as described here. *See relevant sample contract excerpt below:*

> *Section 12.03 Withdrawal of a Participant. … The following shall constitute adequate cause for the withdrawal from this Agreement:*
>
> *(a) A significant breach of another Participant's duties of confidentiality under ARTICLE V of this Agreement with regard to Information stored on [or transmitted over] the Network by the withdrawing Participant, or a significant breach of [the SNO's] duties under ARTICLE VII or ARTICLE VIII with regard to Information stored on [or transmitted over] the Network by the withdrawing Participant (provided that the Participant has allowed a reasonable time for [the SNO] to cure any such significant breach). Any claim of a significant breach by a Party shall be submitted to the Management Committee which will determine, pursuant to Section 10.02 of this Agreement, whether a claimed breach is significant enough to constitute cause under this Agreement. This determination shall be an advisory opinion and shall not be binding on any party to this Agreement and shall not act as a waiver or determination of any Party's rights under federal, state, or local laws. In a vote to determine whether a breach is significant, the complaining party(ies) and the alleged-breaching party(ies) shall not participate. …*

Whether the SNO should have a mechanism for termination of a Participant for significant breaches of confidentiality could be an item for further discussion among Participants and SNOs. This typically would not be a problem in a model where individual users are not "Participants," but rather are part of a Participant's workforce. Thus, the Participant's own internal policies would be invoked in the event of a breach of patient data by the individual user. The **Connecting for Health** "Model Contract for Health Information Exchange" includes several model provisions that could allow for a SNO to terminate a Participant's Registration Agreement, including a model provision allowing for termination for cause.

Indemnification for Breaches of Confidentiality

Indemnification provisions may or may not be included in a SNO agreement. As noted above, the **Connecting for Health** "Model Contract for Health Information Exchange" provides a variety of model provisions concerning indemnification.[18] A SNO may also choose to adopt special rules governing indemnification for particular situations, such as a breach of confidentiality of protected health information. For example, the SNO's agreement could provide for mutual indemnification between all Participants for breaches of confidentiality of patient data, with the scope of the indemnification to be determined by the

[17] See **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 4 (Registration Agreements).

[18] See **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 15.2 (Indemnification).

SNO. *See relevant sample contract excerpt below:*[19]

> *Section 12.03 Indemnification by Participants. A Participant that breaches the confidentiality of the Information, or submits inaccurate, incomplete, or defamatory data to the Network ("Breaching Participant") agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought ("Sued Party") by any individual arising out of or resulting from such breach of confidentiality or submission of inaccurate, incomplete, or defamatory data by the Breaching Participant or any individual for whom such Participant is responsible. Such indemnification shall include the payment of all costs associated with defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against the Sued Party arising out of or resulting from any breach of confidentiality of the Information, or the submission of inaccurate, incomplete, or defamatory data to the Network by the Breaching Participant or any individual for whom such Participant is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, the Breaching Participant, at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to the Breaching Participant within a period wherein the Breaching Participant is not prejudiced by lack of such notice. If the Breaching Participant is required to indemnify and defend, it will thereafter have control of such litigation, but the Breaching Participant may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably withheld. This Section is not, as to third parties, a waiver of any defense or immunity otherwise available to the Sued Party; and the Breaching Participant, in defending any action on behalf of the Sued Party, shall be entitled to assert in any action every defense or immunity that the Sued Party could assert in its own behalf.*

SNO Participants might also require that the SNO have an obligation of indemnification in its role as Business Associate and/or as administrator of the network. *See relevant sample contract excerpt below:*

> *Section 12.04 Indemnification by [the SNO]. [The SNO] agrees to indemnify and hold harmless any other Party against whom any claim or cause of action is brought ("Sued Party") by any individual arising out of or resulting from any breach of confidentiality of the Information (whether through disclosure or through acts or omissions in the design and/or maintenance of the Network) by [the SNO] or any individual for whom [the SNO] is responsible. Such indemnification shall include the payment of all costs associated with defending such claims or causes of action, whether such claims or causes of action are meritorious, including reasonable attorney fees and any settlement by or judgment against any Sued Party arising out of or resulting from a breach of confidentiality of the Information by [the SNO] or any individual for whom [the SNO] is responsible. In the event a suit is brought against the Sued Party under circumstances where this Section applies, [the SNO], at its sole cost and expense, shall defend the Sued Party in such suit if written notice thereof is promptly given to [the SNO] within a period wherein [the SNO] is not prejudiced by lack of such notice. If [the SNO] is required to indemnify and defend, it will thereafter have control of such litigation, but [the SNO] may not settle such litigation without the consent of the Sued Party, which consent shall not be unreasonably*

[19] Note that this sample provision also includes indemnification for submission of inaccurate, incomplete, or defamatory data to the SNO network. Thus, the Participant who made an error in the data would have to hold harmless another Participant who acted on the erroneous data.

withheld. This Section is not, as to third parties, a waiver of any defense or immunity otherwise available to the Sued Party; and [the SNO], in defending any action on behalf of the Sued Party, shall be entitled to assert in any action every defense or immunity that the Sued Party could assert in its own behalf.

Note that these contract samples provide for full indemnification without a cap on liability or language limiting liability to gross negligence or some other threshold of culpability. What the SNO can negotiate, and what the Participants in the SNO's network feel comfortable with, will dictate the breadth and scope of the indemnification provisions. The broader the indemnification provisions, the stronger the incentive for security compliance.

Some entities, such as governmental entities, may be prohibited by statute from entering into an agreement requiring them to indemnify another party. There also may be entities that are willing to provide patient data for use on the SNO's network, but do not have any desire or need to access the network themselves. Whether an entity who merely stores data on the SNO network should be required to agree to an indemnification provision is also an issue for the SNO.

The SNO could consider adding a clause requiring Participants to carry certain levels of insurance.[20] However, this may not be viewed as a required provision, because the Participants likely already carry sufficient insurance to cover their obligations.

[20] See **Connecting for Health**, "A Model Contract for Health Information Exchange," Section 15.1 (Insurance).

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*