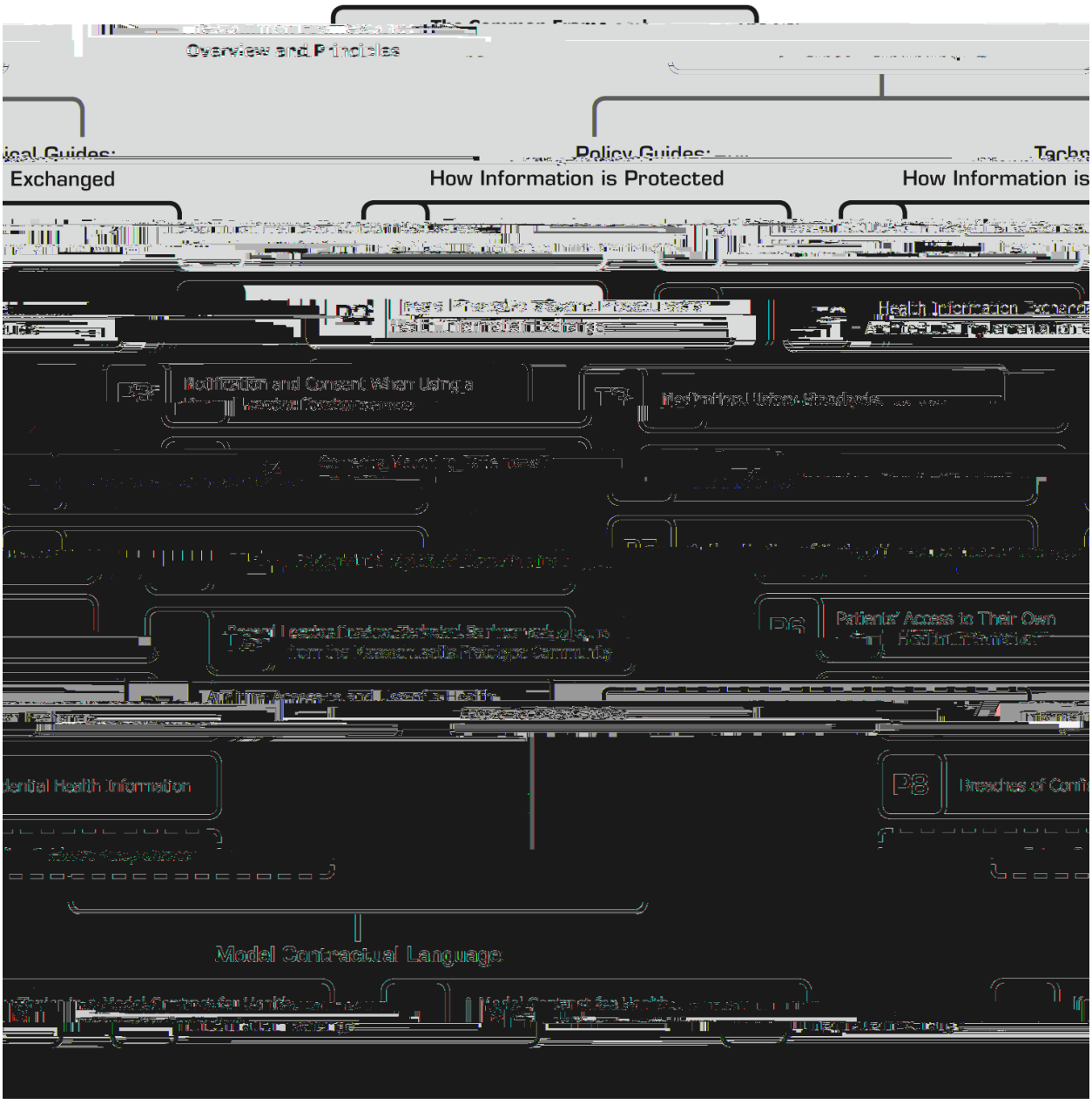
P1 P2 P3 P4 P5 P6 P7 P8

T1 T2 T3 T4 T5 T6 M1 M2

Model Privacy Policies and Procedures for Health Information Exchange

Model Privacy Policies and Procedures for Health Information Exchange

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:



Model Privacy Policies and Procedures for Health Information Exchange*

The model policies contained in this paper are recommended by the Connecting for Health Policy Subcommittee to be used in conjunction with the Connecting for Health "Model Contract for Health Information Exchange"[1] for those working to establish sub-network organizations (SNOs)[2] that will use a Record Locator Service (RLS) and operate as part of the National Health Information Network (NHIN). The policies establish baseline privacy protections designed to apply to all individuals receiving care from a SNO Participant (Participant). The goal of these policies is to provide a framework for protecting health information while simultaneously permitting use of the information that is both productive and meaningful. The policies are intended to be useful for SNOs whether or not they are using an RLS.

The federal HIPAA Privacy and Security Rules provide the baseline for the model policies, although in some cases greater privacy protections and individual rights are recommended by the Connecting for Health Policy Subcommittee. Where provisions are derived from the HIPAA Privacy or Security Rules, citations are provided. In no instance do these policies permit less protection of personal health information than those required by federal law; however, participation in a SNO is not a surrogate for determining whether a Participant is a HIPAA "Covered Entity" or is in compliance with the HIPAA regulations. Importantly, the model policies permit 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 laws. Many of these policies can and should already be in place at the Participant level. Some are aspirational and should be considered in the future as a networked environment for health information emerges and technology enables greater consumer access to their health records. The policies will need to be customized to reflect the Participants' unique circumstances and modified to take account of applicable state laws.

The model policies are deeply

* Connecting for Health thanks Marcy Wilder of Hogan & Hartson LLP for drafting this paper.

1 See Connecting for Health, "A Model Contract for Health Information Exchange."

2 A sub-network organization (SNO) is to 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."

protecting privacy. Individuals should be able to understand what information exists about them, how that information is used, and how they can exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence in individuals with regard to data privacy, which in turn can help increase participation in health data networks.

privacy requirements and identifying and correcting weaknesses in their security systems.

Remedies. The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization's commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

These nine principles underlie the recommended model privacy policies presented below. While certain principles are emphasized by each individual policy, the policies as a whole balance all of the principles equally so that certain principles are not emphasized over others—which would undermine the effectiveness of the overall approach. Moreover, the policies are individual elements of an integrated and comprehensive Connecting for Health policy framework—*The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*—that is intended to be considered in its entirety. In that regard, please refer to the following additional materials developed by the Connecting for Health Policy Subcommittee: "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," "Notification and Consent When Using a Record Locator Service," "Patients' Access to Their Own Health Information," and "Correctly Matching Patients with Their Records."

Although most of the recommended model policies can and should be implemented in the current technological environment, there are a few for which organizational and technical barriers may currently be prohibitive. For example, although patients would benefit from access to the RLS and the ability to obtain audit trails of those who have requested information about them from the index, technical and administrative barriers currently do not allow for such access. Health care participants, system vendors, and others should work toward implementing these functionalities as they will enhance privacy protections and help implement the privacy principles of openness and transparency, security safeguards and controls, purpose specification and minimization, use limitation, collection limitation, and accountability. Similarly, in the future, Participants and vendors should seek to realize the other policies that cannot be implemented at this time due to organizational and technical constraints.

The emergence of a networked electronic health information environment will transform patient care and improve the efficiency and effectiveness of the health system. At the same time, the emerging electronic health information infrastructure and the massive increase in the volume of health data that is easily collected, linked, and disseminated create unprecedented privacy and security risks that need to be adequately and appropriately addressed. By incorporating the principles outlined above and the basic requirements set forth in HIPAA, these recommended model policies seek to achieve a balance between maintaining the confidentiality of health information and maximizing the benefits of using such information. Integration of these privacy measures into the emerging networked health care environment can ensure that the benefits of electronic health information are realized while the confidentiality of health information is preserved.

Each of the recommended privacy policies outlined below contains an introductory section that provides background and explains the basis for the policy in law, the privacy principles described above, and other sources. The introductory sections are followed by recommended language for use by SNOs in drafting their own Policies and Procedures

oversight, and remedies, a requirement that Participants comply with applicable law and SNO policies and promulgate the internal policies required for such compliance is indispensable to the successful realization of essential privacy protections. In addition, the recommended model provision below governing conflicts between SNO policies and Participant policies, which states that the policy that is most protective of individual privacy should govern decision making, is designed to make clear that the policies provide a floor and Participants may choose to enhance privacy protections where appropriate. This deference to more protective policies echoes the HIPAA federal pre-emption requirements which do not preempt more protective state privacy laws.

through the SNO and RLS, who is able to access the information, and how they can have information concerning them removed from the RLS. These are not HIPAA requirements, but rather build and expand upon the privacy law to help incorporate information related to the NHIN and the RLS. This recommended model policy also exceeds HIPAA's requirements by providing suggestions for additional, voluntary protections that could be implemented on the Participant level to enhance consumer protections, such as excluding individuals from the RLS index unless prior consent is obtained or loading information into the RLS only after a notification and opportunity to decline participation has been provided to individual patients.

This recommended model policy promotes the privacy principles of openness and transparency, purpose specification and minimization, use limitation, collection limitation, and individual participation and control. In addition, the model policy helps ensure that information is collected and shared electronically in a fair manner with the knowledge of relevant individuals, which is particularly important in a networked environment where the technology may be unfamiliar to average users.

Recommended Language

Scope and Applicability: This Policy applies to all Participants that have registered with and are participating in the SNO and the RLS and that may provide or make available health information through the SNO and the RLS.

Policy:

Each Participant shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and this Policy.

1. Content. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[6] and comply with all applicable laws and regulations. The Notice also shall include a description of the SNO and the RLS and inform individuals regarding: (1) what information the institution may include in and make available through the SNO and the RLS; (2) who is able to access the information in the SNO and the RLS; (3) for what purposes such information can be accessed; and (4) how the individual can have his or her information removed from the RLS.

2. Provision to Individuals. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

   - For Participants that are health care providers, the Notice shall be: (1) available to the public upon request; (2) posted on all web sites of the Participant and available electronically through such sites; (3) provided to a patient at the date of first service delivery; (4) available at the institution; and (5) posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.[7]

   - For Participants that are health plans, the Notice shall be: (1) available to the public upon request; (2) provided to new enrollees at the time of plan enrollment; (3) provided to current plan enrollees within 60 days of a material revision; and (4) posted on the plan's web sites and available electronically through such sites. Participating health plan institutions also shall notify individuals covered by the plan of the availability of the Notice and how to obtain a copy at least once every three years.[8]

3. Individual Acknowledgement. Each Participant that is a health care provider shall make a good faith effort to obtain the individual's written acknowledgement of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgement of the Notice shall comply with all applicable laws and regulations.[9] Each Participant shall have its own policies and procedures governing obtaining an

[6] 45 C.F.R. § 164.520(b).

[7] See 45 C.F.R. § 164.520(c)(2), (3).

[8] See 45 C.F.R. § 164.520(c)(1), (3).

[9] See 45 C.F.R. § 164.520(c)(2)(ii).

acknowledgement, which policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

4. Participant Choice. Participants may choose a more proactive notice distribution process than provided herein and may include more detail in their notice of privacy practices. Possible additional protections for individuals whose information may be made available through the RLS (not all of which pertain to notice policies alone) could include: mailing the revised notice or a notification letter allowing for removal or exclusion of the information about that individual from the RLS to every individual prior to loading the information into the RLS or shortly thereafter; excluding individuals from the RLS index unless individual consent

about him or her included in the RLS. Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.

6. Provision of Coverage or Care. A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the RLS.

SNO Policy 400: Uses and Disclosures of Health Information

Purpose and Principles: Through a variety of mechanisms, this model policy reflects the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, collection limitation, accountability and oversight, and data integrity and quality. The recommended policy integrates HIPAA's general premise that health information may be used only for permissible purposes and its more specific requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[10] In general, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA, will be permitted.[11] Furthermore, subject to certain limitations and under certain circumstances, requesting disclosure of and using health information for law enforcement,[12] disaster relief,[13] research,[14] and public health[15] purposes also may be permissible. Accessing health information through either the RLS or the SNO for marketing or marketing-related purposes is prohibited without specific patient authorization.[16] Under no circumstances may health information be accessed or used for discriminatory purposes. For example, a health plan would not be permitted to use the RLS to determine if a member has visited a health care provider for whom the health plan has not been billed. Such activity would be an impermissible and discriminatory purpose and is prohibited by applicable law and under this Policy. SNOs may provide guidance to Participants detailing the permissibility or impermissibility of requesting or using health information for certain specified purposes under applicable law.

Requiring consideration of the purpose of a use and minimization of the use of information reduces the likelihood of inadvertent or intentional misuses of information. The model policy helps enhance the fair and legal collection and use of data, the oversight of data use and accountability for privacy violations by ensuring that Participants have legally required documentation prior to the use or disclosure of information.[17] In addition, the integration of HIPAA's accounting of disclosures and individual access to information requirements allows individuals to understand how health information about them is shared and to exercise certain rights regarding information about them with greater precision and ease.[18]

The recommended provision also requires security measures essential to identify and remedy loss, unauthorized access, destruction, use, modification, or disclosure of personal health information. The audit requirement reflects the HIPAA Security Rule's general

[10] 45 C.F.R. § 164.502(b).

[11] 45 C.F.R. §§ 164.502(1)(ii), 506. Under HIPAA, treatment is defined as "the provision, coordination, or management of health care and related services by one or more health care providers … " 45 C.F.R. § 164.501. Payment refers to "activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care." Such activities include eligibility and coverage determinations; risk adjustments; billing, claims management and collection activities; medical necessity review; and utilization review. Id. Health care operations includes activities related to covered functions for (i) conducting quality assessment and improvement; (ii) evaluating competence, qualifications and performance of health care professionals, evaluating health plan performance, training and credentialing activities; (iii) underwriting, "premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits"; (iv) "conducting or arranging for medical review, legal services, and auditing functions;" (v) business planning and development; and (vi) business management and administrative activities. Id.

[12] 45 C.F.R. § 164.512(f).

[13] 45 C.F.R. § 164.510(b)(4).

[14] 45 C.F.R. § 164.512(i).

[15] 45 C.F.R. § 164.512(b).

[16] **45 C.F.R.** 164.508(a)(3) & (b).

[17]

requirement that entities implement policies to prevent security violations, assess security risks, and examine data storage and access technology[19] but, in a manner more protective than HIPAA, would establish monitoring requirements as to when information is accessed and by whom. To prevent unauthorized access of information and maintain data integrity and quality the authentication provision of the model policy requires that both the identity and authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy Rule and Security Rule.[20]

The combination of this recommended policy's use and security provisions helps guarantee that health information is used and accessed only as authorized and that Participants have proper measures in place to identify

provide individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the HIPAA Privacy Rule's accounting of disclosures requirement.

6. Audit Logs. Participants and SNOs shall consider and work towards maintaining an audit log documenting which Participants posted and accessed the information about an individual through the RLS and when such information was posted and accessed.[25] Participants and SNOs shall consider and work towards implementing a system wherein, upon request, patients have a means of seeing who has posted and who has accessed information about them through the RLS and when such information was accessed.[26]

7. Authentication. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating those within their institutions who shall have access to, as well as other Participants who request access to, information through the SNO and/or the RLS.[27] [28]

8. Access. 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.[29] Participants and SNOs shall consider and work towards providing patients direct access to the information contained in the RLS that is about them.[30]

SNO Policy 500: Information Subject to Special Protection

Purpose and Principles: This model policy promotes the privacy principles of purpose specification and minimization, security safeguards and controls, use limitation, data integrity and quality, collection limitation, and individual participation and control. This recommended provision facilitates individualized privacy protections by requiring Participants to heed any special protections of certain information set forth under applicable law. In complying with these special protections, Participants' collection, use and disclosure of health information is limited to legitimate purposes. Moreover, in guaranteeing deference to the law or policy most protective of privacy, the provision below echoes HIPAA's federal preemption requirements which defer to state laws that are more protective than HIPAA's own privacy provisions.[31]

Recommended Language

Scope and Applicability: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide or make available health information through the SNO.

Policy:

Some health information may be subject to special protection under federal, state, and/or local laws and regulations (e.g., substance abuse, mental health, and HIV). Each Participant shall determine and identify what information is subject to special protection under applicable law prior to disclosing any information through the SNO. Each Participant is responsible for complying with such laws and regulations.

SNO Policy 600: Minimum Necessary

Purpose and Principles: To promote the privacy principles of collection limitation, use limitation, data integrity and quality, and security safeguards and controls, this recommended model policy incorporates HIPAA's requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[32] The policy exempts treatment disclosures from this minimum necessary requirement to balance the protection of privacy and the provision of quality

C.F.R§

C.F.R§

[25] See 45 C.F.R. §§ 164.316, 164.308(a)(1)(i).
[26] See Connecting for Health, "Auditing Access to and Use of a Health Information Exchange."
[27] See 45 C.F.R. §§ 164.514(h), 164.312(d).
[28] See Connecting for Health, "Authentication of System Users."
[29] See 45 C.F.R. § 164.524.
[30] See Connecting for Health, "Patients' Access to Their Own Health Information."

health care. In assessing the smallest amount of information that is necessary to accomplish a particular purpose, Participants are less likely to collect, use or disclose information for an unauthorized purpose. Minimal collection, access, use and disclosure increases public confidence in the privacy practices of Participants, enhances information privacy, and diminishes the potential for data corruption and security violations.

Recommended Language

Scope and Applicability: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

Policy:

1. Uses. Each Participant shall use only the minimum amount of health information obtained through the SNO as is necessary for the purpose of such use. Each Participant shall share health information obtained through the SNO with and allow access to such information by only those workforce members, agents, and contractors who need the information in connection with their job function or duties.

2. Disclosures. Each Participant shall disclose through the SNO only the minimum amount of health information as is necessary for the purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

3. Requests. Each Participant shall request only the minimum amount of health information through the SNO as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by health care providers for treatment purposes.

4. Entire Medical Record. A Participant shall not use, disclose, or request an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. This limit does not apply to disclosures to or requests by a health care provider for treatment purposes or disclosures required by law.

SNO Policy 700: Workforce, Agents, and Contractors

Purpose and Principles: By incorporating HIPAA's administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints,[33] this recommended model policy advances the privacy principles of use limitation, security safeguards and controls, accountability and oversight, data integrity and quality, and remedies. Because a Participant's workforce is responsible for implementation of privacy practices, proper training is vital to ensure the legitimate use of health information and the prompt identification, reporting, and correction of any security weaknesses. Individual accountability in the form of sanctions for those persons responsible for privacy violations is fundamental to encouraging compliance with privacy practices. Without such incentive for compliance, privacy violations and security risks may go unchecked and lead to larger privacy problems. Similarly, providing for the reporting of non-compliance enables Participants to discover and correct privacy violations and identify and sanction privacy violators. This model policy helps guarantee the legitimate use of health data, the proper implementation of Participants' privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

Recommended Language

Scope and Applicability: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide, make available, or request health information through the SNO.

Policy:

1. Access to System. Each Participant shall allow access to the SNO only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the SNO and/or

[33] 45 C.F.R. § 164.530.

release or obtain information through the SNO. No workforce member, agent, or contractor shall be provided with access to the SNO without first having been trained on these Policies, as set forth below.

2. Training. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the SNO to ensure compliance with these Policies.[34] The training shall include a detailed review of applicable Policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these Policies.

3. Discipline for Non-Compliance. Each Participant shall

requires Participants who agree to individuals' request for restrictions in accordance with the HIPAA Privacy Rule to comply with such request with regard to the release of information in the SNO.[39] Such compliance ensures permissible use of health information and accountability on the part of Participants who agree to individually requested use restrictions. Without the ability to request restrictions and without assurance that Participants will honor these agreed-upon restrictions, individuals may remain silent about important information that could affect their health. By creating confidence in Participants and their privacy protections and encouraging individual participation, this policy fosters dialog between individuals and Participants. Improved communications between a provider and patient improves the overall delivery of health care.

Recommended Language

Scope and Applicability: This Policy applies to all institutions that have registered with and are participating in the SNO and that may provide or make available health information through the SNO.

Policy:

If a Participant agrees to an individual's request for restrictions,[40] as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information through the SNO. If an agreed-upon restriction will or could affect the requesting institution's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting institution of the fact that certain information has been restricted, without disclosing the content of any such restriction.

SNO Policy 1000: Mitigation

Purpose and Principles: By incorporating HIPAA's requirement that entities have procedures to and take steps to mitigate harm resulting from an impermissible use or disclosure of health information,[41] this model policy reflects the privacy principles of remedies, accountability and oversight, security safeguards and controls,

[39] 45 C.F.R. § 164.522.

[40] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA.

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*