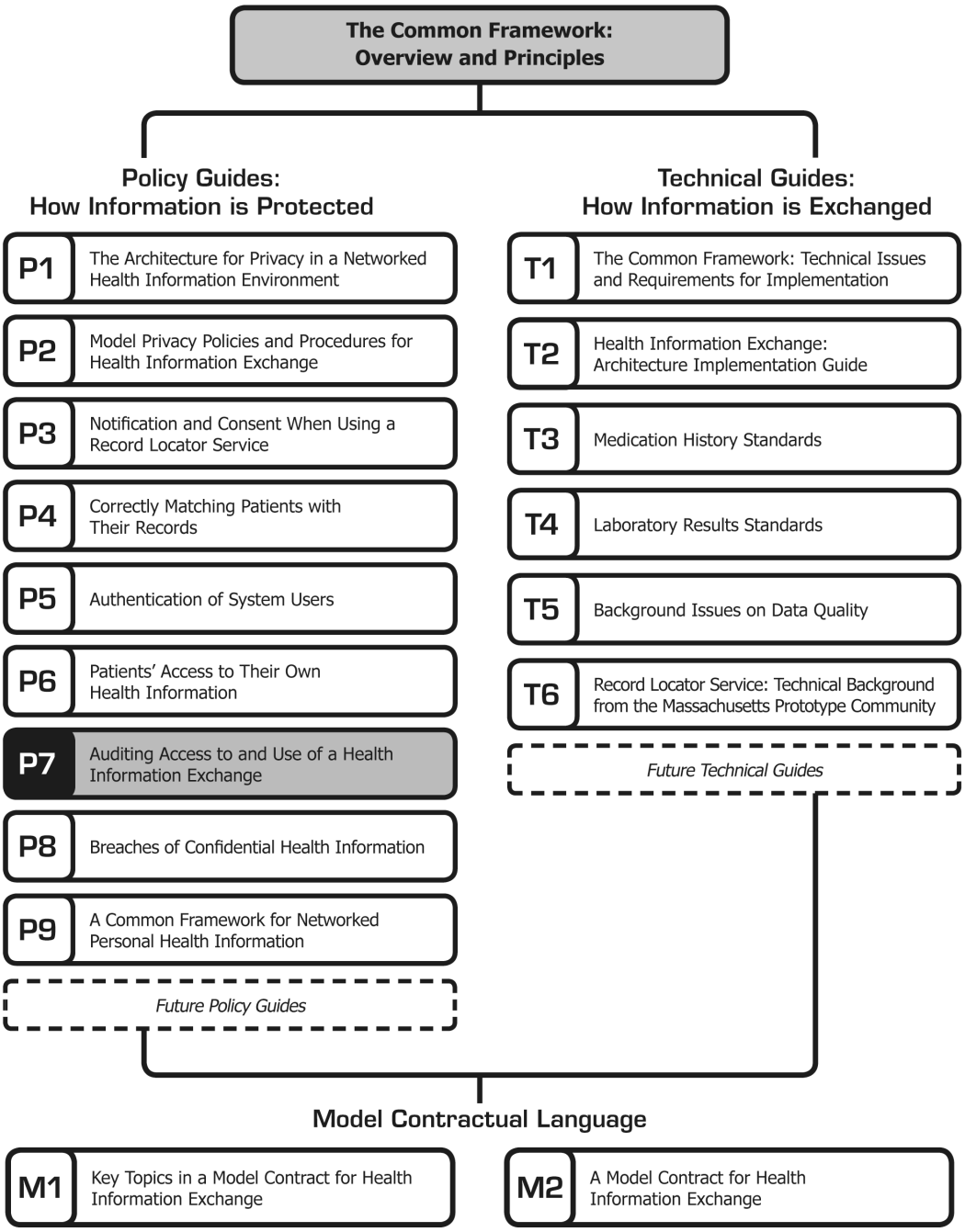
P1 P2 P3 P4 P5 P6 **P7** P8

T1 T2 T3 T4 T5 T6 M1 M2

Auditing Access to and Use of a Health Information Exchange

Auditing Access to and Use of a 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 October 2006, the Common Framework included the following published components:



Auditing Access to and Use of a Health Information Exchange*

This document recommends an initial set of logging and audit practices for a National Health Information Network (NHIN). Effective logging and audit practices are essential safeguards as electronic protected health information (ePHI) is shared at the regional and national levels, and can assure participating institutions that there is compliance with legal requirements for technical, physical, and administrative safeguards. At least as importantly, publicly announced audit and logging practices can foster trust among individual patients and the general public that their data is being used only in appropriate ways.

Part I explains the logging and other audit requirements under HIPAA. These legal requirements form the baseline for auditing in any eventual system for sharing ePHI.

Part II sets forth the general conclusions concerning logging and auditing at the level of covered entities, of each sub-network organization (SNO)[1] and for the Record Locator Service (RLS). The principle conclusion is that HIPAA should form the baseline for individual covered entities, but that logging and auditing practices, which may go beyond HIPAA requirements, should be in place for SNOs and the RLS.

Part III implements those general conclusions by setting forth a checklist for auditing and accountability for each SNO and the RLS. It supplements the checklist with a list of recommended additional measures, including independent third-party auditing for the RLS.

I. Logging and Audit Controls under HIPAA

It is useful to understand current law before deciding what new logging and audit control requirements, if any, should be used when handling ePHI. The HIPAA Privacy Rule does not specifically mention logging or audits. It does provide that "a covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 CFR § 164.530 (c)(1). An effective audit and logging system will often be part of the overall set of safeguards expected under the Privacy Rule.

The HIPAA Security Rule is more specific. Section 164.312(b) requires audit controls as a standard: "Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." The United States Department of Health & Human Services explained that the nature of the audit controls will depend on the context: "We believe that it is appropriate to specify audit controls as a type of technical safeguard. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses." 68 Fed. Reg. at 8355 (Feb. 20, 2003).

The HIPAA Security Rule also mandates "information system activity review" as an element of administrative safeguards:

* **Connecting for Health** thanks Peter Swire, C. William O'Neill Professor of Law, Moritz College of Law, Ohio State University, for drafting this paper.

[1] A sub-network organization (SNO) operates as a health information data exchange organization (whether regional 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."

"Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports." 45 CFR § 164.308(a)(1)(ii)(D). Once again, the sophistication of the required safeguard depends on the setting: "Our intent for this requirement was to promote the periodic review of an entity's internal security controls, for example, logs, access reports, and incident tracking. The extent, frequency, and nature of the reviews would be determined by the covered entity's security environment." 68 Fed. Reg. at 8347.

One additional relevant provision in the HIPAA Security Rule is Section 164.308(a)(5)(ii)(C), which concerns log-in monitoring. The Rule sets forth an addressable implementation specification (i.e., good practice but not necessarily required), which covers "[p]rocedures for monitoring log-in attempts and reporting discrepancies."

Beyond these federal requirements, there may be state and local laws that create requirements in the areas of logging and audit controls that will need to be assessed by individual SNOs and their participants.

II. Logging and Audit Controls in a National Health Information Network

With these HIPAA requirements as a baseline, audit and logging practices will differ in important respects among the various actors in a National Health Information Network. This section will provide a general analysis of the level of logging and audit controls to be expected among covered entities within each SNO, at each SNO itself, and for inter-SNO sharing. The next section will recommend specific logging and audit practices to apply at the SNO and inter-SNO levels.

For covered entities within each SNO, the baseline will be the requirements of the HIPAA Security Rule, discussed briefly in the prior section. The Security Rule contemplates that the level of audit controls required varies with the security environment. Throughout HIPAA, requirements are "scalable," which means that large and sophisticated entities are expected to establish more rigorous safeguards than small entities. For audit, scalability means that small entities often have less thorough safeguards than large entities.

In setting policy for logging and audit control practices for covered entities within each SNO, it is important to recognize the small scale of many covered entities. Even for many large covered entities, current logging and audit control systems likely do not match the rigor and complexity of the best practices of large institutions. Given these current practices, it would likely be difficult to insist on heightened logging and audit control standards for each covered entity within SNOs. Any attempt to require such standards would quite possibly discourage participation in the overall system and further delay participation. Our recommendation at this time is thus not to require heightened logging and audit control standards for each covered entity or other participant within a SNO.

The analysis shifts, however, for logging and audit control practices at the level of each SNO in order to best safeguard ePHI. Each SNO is expected to be a sophisticated entity, operating at a scale that is consistent with rigorous audit and other security practices. Compared with individual providers, who often depend largely on paper records, SNOs are likely to rely more heavily on electronic health records, which are typically more suitable than paper records for enhanced and automated logging and audit control approaches. In order to promote trust among patients and participating institutions, we therefore recommend excellent logging and audit control practices at the SNO level, as described in the next section.

The case for strong logging and audit control standards is even stronger for inter-SNO sharing through the RLS. As discussed in previous documents of **Connecting for Health**, the RLS will provide a means for locating records of an individual patient that

are held by different data providers, including in different SNOs. It will be crucial to build public confidence in the good data handling practices of the RLS. A transparent and effective method for logging and audit controls is one important component of the case that the public deserves to trust the RLS. The next section recommends specific practices, notably including an independent, third-party audit on a regular basis.

In establishing these strict logging and audit practices at the SNO and inter-SNO levels, it is important to clarify what types of records are likely to move through such information systems. As contemplated in the **Connecting for Health** Common Framework, the RLS itself will *not* contain clinical data. Instead, the RLS will contain demographic data, in order to identify and provide contact information for the actual holders of clinical records. Transfer of clinical records will be "point to point." That is, an entity seeking the records of a particular patient may learn about other record holders through the RLS. That entity then will directly contact the other record holders in order to receive the clinical records. For purposes of logging and audit controls, this structure means that the flows of demographic information will be carefully tracked at the RLS level.

Transfers of clinical records, however, will not take place through the RLS itself, and will thus be subject to the logging and audit practices at the level of each entity. As a related point, SNOs may operate in a similar way. Whatever demographic (or other) information moves through the SNO would be subject to audit under the strict logging and audit standards contemplated here for SNOs. Transfers of clinical records, however, may take place through paths that do not include a SNO.

III. Specific Logging and Audit Recommendations

In preparing this paper on logging and audit practices, it has been helpful to review the actual audit documents of some large, cutting-edge health care organizations. The discussion here draws on those documents, as well as some publicly available materials.[2]

A. Audit and Accountability Checklist

We first put forward a recommended audit and accountability checklist. This checklist is intended to apply at least to SNOs and the RLS, and it represents good practice for a broader range of covered entities.

[2] One helpful, published source of information on audits is "Security and Privacy Auditing in Health Care Information Technology." This paper was published in 2001 by the Joint Security and Privacy Committee of three organizations, the National Electrical Manufacturers Association, the European Coordination Committee of the Radiological and Electromedical Industry, and the Japan Industries Association of Radiological Systems, available at: http://www.nema.org/medical. The paper provides a useful synopsis, in six pages, of the elements of an audit for health care information technology.

For additional background, there is a recent paper on "Immutable Audit Logs" by Jeff Jonas and Peter Swire for the Markle Task Force on National Security in the Information Age. See http://www.markle.org. The paper analyzes the heightened auditing procedures that can be used to increase public confidence about systems that are not transparent to the public.

For more information on industry best practices in healthcare security auditing, see RFC 3881 (http://www.faqs.org/rfcs/rfc3881.html), Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications.

Audit & Accountability Checklist

Audit and Accountability. Audit is the practice of recording the occurrence of selected system events; management uses reports/alerts generated from audit records to monitor the appropriateness of activities. Accountability results when activities are attributable to individuals.

	Yes	NO	N/A
1. The system is required to log users' system login and logoff with date and time, or, if the system does not have the capability to record login/logoff activity, it may rely on an external security system's access control logging function to record access.			
2. The system must have the ability to log read, create, update, delete, forward, and print access initiated by individuals and processes for systems containing confidential and restricted data. For data warehouses, data marts, and operational data stores, the system must have the ability to log queries, or alternatively the tables read must be logged. Row-level logging must be available on demand.			
3. All audit records must be identified by a unique record key or number, and include: • User identifier/name of user • Time/date • Device identifier (when used to access) • Source (i.e. subsystem or system of origin of the event [access request]) • Content (type of data being accessed or activity being performed) • Type of action (e.g. read, write, update, delete, or copy) or access for diagnostic purposes.			
4. Unsuccessful login attempts and access violations within the system must be logged.			
5. Security administrative functions must be logged.			
6. System administrative functions must be logged.			
7. Audit records must be protected against unauthorized access, modifications, and deletion.			
8. Audit records must be readily available for 90 days and archived for a minimum of two years, or up to the six years used for the archiving of HIPAA disclosures.			
9. Security administrators and auditors can request or generate reports which may consist of any or all of the audit record elements for any or all types of actions.			

B. Categories of Logging and Audit Controls

In addition to the checklist, there are additional logging and audit control functions that are generally recommended at the SNO and RLS level. Some of these functions are included in other papers of the **Connecting for Health** Policy Subcommittee, such as tracking of authentication or responses to security breaches, but the list here errs on the side of inclusion:[3]

1. Audit of VIP records.
2. Procedures for follow-up on suspicious activity, such as indications of possible privacy or security breaches.
3. Review of network intrusion detection system activity logs.
4. Review of system administrator authorizations and activity.
5. Review of physical access to data centers.
6. Other review of technical, physical, and administrative safeguards as established by the policies of the organization.

Beyond these sorts of compliance efforts, it is recommended that SNOs and the RLS have random audits of demographic and clinical records, based on the level of risk for that portion of the system. SNOs may wish to provide for some level of random audits (sampling) of the participants in the SNOs. Random audits should be done for records held at the SNO level and within the RLS. For the RLS (and where appropriate for each SNO), an independent third-party should perform such random audits, with public reporting of at least the principal results.

Conclusion

This paper provides a general template for assessing where excellent logging and audit practices are especially essential, at the SNO and RLS levels. It then recommends a checklist for audits, as well as a supplementary list of measures to be taken at the SNO and RLS levels to ensure an overall high quality of audit and accountability.

Under the HIPAA Privacy and Security Rules, a legal argument can be made that the high-quality practices set forth in Section III of this paper are approximately what is required by the scalable requirements of those rules. Whether or not this legal position is correct, the practices set forth in this paper provide significant detail to assist organizations in developing their own logging and audit practices. A transparent and effective logging and audit control approach can help assure trust in the expanded use of electronic health records by patients and the general public.

[3] See **Connecting for Health**, "Authentication of System Users," and "Breaches of Confidential Health Information."

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*