January 18, 2005

David J. Brailer, M.D., Ph.D.
Office of the National Coordinator for Health Information Technology
The Department of Health and Human Services
Hubert H. Humphrey Building, Room 517D
200 Independence Avenue, S.W.
Washington D.C. 20201

RE: NHIN RFI Responses

Dear Dr. Brailer:

The undersigned organizations, members of the Confidentiality Coalition, chaired by the Healthcare Leadership Council (HLC), appreciate the opportunity to comment on the Office of the National Coordinator for Health Information Technology's (ONCHIT) Request for Information regarding the development and adoption of a National Health Information Network, as published in the federal register on November 15, 2004.[1]

HLC is a not-for-profit membership organization comprised of chief executives of the nation's leading health care companies and institutions.[2] In 1996, HLC began chairing the "Confidentiality Coalition," a broad-based group of organizations who support workable national uniform privacy standards. Through the years the Confidentiality Coalition has played a leadership role in this area as we work with Members of Congress and the Administration to promote this goal. The Confidentiality Coalition includes physician specialty and subspecialty groups, nurses, pharmacists, hospitals, nursing homes, medical colleges, biotechnology researchers, employers, health plans, pharmaceutical companies, and PBMS.

The coalition supports the efforts of ONCHIT to create a national health information infrastructure and believes that any regional or national system designed to facilitate the sharing of electronic health information must take into account the privacy and security challenges associated with exchanging patient information among health care providers, consumers, payers and other authorized entities. Addressing these issues appropriately will be essential to achieving the interoperability necessary to improve the quality and cost effectiveness of the health care system.

Of particular interest to the Confidentiality Coalition are specific requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

---

[1] 69 Fed.Reg. 65599 (Nov. 15, 2004).
[2] We have attached a list of HLC's members.

statute and the privacy regulation promulgated thereunder[3] (the "Privacy Rule") and how these provisions may affect efforts to establish a national health information network (NHIN). Our comments focus on several questions which relate to the privacy and security issues posed by the creation of the NHIN, including how compliance with HIPAA and implementing regulations will interact with the NHIN as well as regulatory requirements that might be perceived as barriers to the formation and operation of a NHIN.

COMMENTS

Our comments address the following questions in the RFI:

Question 2. What type of model could be needed to have a NHIN that: allows widely available access to information as it is produced and used across the health care continuum; enables interoperability and clinical health information exchange broadly across most/all HIT solutions; protects patients' individually-identifiable health information; and allows vendors and other technology partners to be able to use the NHIN in the pursuit of their business objectives? Please include considerations such as roles of various private- and public-sector entities in your response.

Question 7. What privacy and security considerations, including compliance with relevant rules of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), are implicated by the NHIN and how could they be addressed?

Question 15. How should the development and diffusion of technically sound, fully informed interoperability standards and policies be established and managed for a NHIN, initially and on an ongoing basis, that effectively address privacy and security issues and fully comply with HIPAA? How can these standards be protected from proprietary bias so that no vendors or organizations have undue influence or advantage? Examples of such standards and policies include: secure connectivity, mobile authentication, patient identification management and information exchange.

Question 21. Are there statutory or regulatory requirements or prohibitions that might be perceived as barriers to the formation and operation of a NHIN, or to support it with critical functions?

Question 22. How could proposed organizational mechanisms or approaches address statutory and regulatory requirements (e.g., data privacy and security, antitrust constraints and tax issues)?

*** * * ***

[3] 45 C.F.R. pts. 160 and 164.

There are four areas in which HIPAA may significantly impede development and adoption of the establishment of a NHIN. First, although HIPAA establishes a federal privacy standard, it permits significant state variations that we are concerned will create serious impediments to sharing or sending information, particularly across state lines. Second, participation in a NHIN may impose significant and unmanageable burdens on health care providers attempting to comply with the Privacy Rule requirements regarding the accounting of disclosures of protected health information. Third, we believe that the Privacy Rule's minimum necessary standard – which already poses significant burdens for covered entities – will be unworkable in the context of disclosures made through a NHIN. Fourth, current law restrictions in the area of research will prevent NHIN from achieving its ultimate objective as a tool to improve quality of care. Each of these issues is discussed in detail below.

I. Preemption of State Laws

In the Request for Information, ONCHIT recognizes that "interoperability requires a set of common standards that specify how information can be communicated and in what format."[4] This is true not only with respect to the technical standards employed through information technology, but also with respect to the privacy standards that govern information disclosures.

HIPAA required the Secretary of HHS to adopt standards for the electronic exchange, privacy and security of health information. In general, HIPAA supersedes contrary provisions of state law. For example, the HIPAA provisions requiring the use of certain electronic standards preempt state laws that require medical records or billing records to be maintained or transmitted in written rather than electronic form.[5] Congress, however, set a different preemption standard for privacy protections.[6] The law states that the Privacy Rule shall not supersede state laws that are contrary to and more stringent than the federal standard. As a result, providers, clearinghouses and health plans are required to comply with the federal law as well as any state privacy restrictions that are contrary and more stringent. In the context of HIPAA implementation this has been extremely difficult. In the context of a NHIN it is potentially impossible.

State health privacy protections vary widely and are found in thousands of statutes, regulations, common law principles, and advisories. Health information privacy protections can be found in a state's health code as well as laws and regulations governing criminal procedure, social welfare, domestic relations, evidence, public health, revenue and taxation, human resources, consumer affairs, probate and many others. The rules typically apply either to specific entities – such as hospitals or county

---

[4] 69 Fed.Reg. at 65,600.
[5] 42 U.S.C. § 1320d-7(a)(1).
[6] *Id.* at § 1320d-(a)(2)(B).

health departments – or to specific health conditions, and no two states are the same in this regard. Virtually no state requirement is identical to the federal rule.

According to HHS' National Committee on Vital and Health Statistics (NCVHS), the multiplicity of applicable privacy rules and the lack of regulatory guidance on preemption have made compliance with the HIPAA Privacy Rule "difficult, costly and complicated." In a letter to the Secretary of HHS, NCVHS wrote:

> "To determine whether state privacy laws or the HIPAA Privacy Rule applies to the multitude of health privacy issues, covered entities must obtain a comprehensive preemption analysis, detailing whether state or federal law applies. These analyses are often lengthy documents, expensive to research, highly technical, and not binding on any enforcement agency or the courts. Large, multi-state covered entities need to have such an analysis for every jurisdiction in which they do business. There is no national coordination on the issue of preemption, and state and local efforts vary widely in their degree of completion and, for those already completed, in the cost to obtain copies. A related issue involves conflicts and overlaps between HIPAA and other federal laws dealing with privacy, including Gramm-Leach-Bliley, the Family Educational Rights and Privacy Act (FERPA), the Privacy Act, and other statutes and regulations."[7]

HHS has made clear that the Agency will not provide a comprehensive preemption analysis[8]. Moreover, single state and private sector efforts have been extremely costly and do not utilize consistent standards. State medical societies, hospital associations and other entities have commissioned single state studies. A national study commissioned by three health plan trade associations covering only health plans cost a reported $2 million dollars. Because state requirements change frequently, that study quickly became outdated and in any event could not be used by providers, researchers and others affected by the Privacy Rule. Several provider organizations investigated the cost of conducting a nationwide survey for their specific type of entity and found that the study would cost in excess of $1 million. Costs for a preemption analysis for a single entity in a single state can total $50,000 or more. Finally, the multitude of public and private studies that have been done do not utilize a consistent methodology and are generally not publicly available. HLC attempted to address this problem directly by commissioning a multi-jurisdiction study of state privacy laws, case law and regulations that analyzes the relationship between the federal Privacy Rule and the state laws. The study initially cost more than $1 million and costs $100,000 to update annually. Many organizations, particularly smaller provider groups,

---

[7] NCVHS Letter 11/25/02, available at www.ncvhs.hhs.gov/021125lt.htm.

[8] *See* 65 Fed.Reg. 82,462, 82,481 (December 28, 2000).

do not have the resources to contribute to or access the study, although they recognize that they need the information.

The issues associated with privacy compliance within a single state are greatly magnified in the context of a NHIN. The creation of a successful NHIN will require a national system of interoperable systems that can exchange health information. Making information available through or to a NHIN conceivably could require entities to comply with a range of different state laws each time they disclose information in the context of a federated system. The current patchwork of applicable state and federal laws will likely be a significant disincentive to participation for virtually all stakeholders. Indeed, already members affiliated with emerging regional consortia are reporting difficulty in accessing the targeted expertise needed to navigate the variations in state privacy laws across regions and indeed across the country. It is not clear how interoperability can be achieved without a more uniform framework for the protection of patient privacy. Absent such a framework, the barriers to using health information technology to improve the quality and efficiency of health care will be substantial and covered entities will be discouraged from participating. Federal preemption provisions that go further toward eliminating state variation in privacy standards will help ensure the viability of a NHIN.

II. Accounting of Disclosures

The Privacy Rule requires covered entities to provide individuals with an accounting of disclosures of their protected health information. Experience with this requirement among Confidentiality Coalition members shows that the accounting of disclosures imposes undue administrative costs on covered entities and erects barriers to quality health care while providing little if any added privacy protections. Although disclosures for treatment, payment and health care operations are exempt from the accounting requirement, other disclosures that are critical to public health, quality initiatives, health oversight, and research are not. The burdens associated with the accounting of disclosures provisions grow more complex when considered in the context of a NHIN, and will likely serve as a barrier to participation by covered entities.

Under the Privacy Rule alone, the accounting of disclosures requirement has, in our view, unnecessarily diminished access to health information for purposes essential to improving health care and health care quality. For example, some hospitals have stated that they will no longer participate in the QIO quality improvement projects as they relate to non-Medicare patients, because of the onerous administrative burdens imposed by the accounting of disclosures requirement. The large number of patients whose information is disclosed to QIOs makes the record keeping required unduly burdensome. Similarly, health care providers are more reluctant to make health information available to researchers because of the accounting of disclosure procedures associated with disclosing data sets to researchers pursuant to an IRB waiver of authorization.

Health plans have also faced difficult challenges implementing the accounting of disclosures standard – challenges that have raised costs. For example, State Insurance Departments require health plans to turn over thousands of records every year to facilitate DOI market conduct reviews, claim verifications and other auditing functions. Also, health plans and providers are sometimes required to turnover immunization records and other records to state authorities. Tracking tens of thousands of records every year – because of government requests – is extremely costly. In addition to the cost of tracking, there is an enormous storage cost as health plans and providers must secure gigabytes and terabytes of computer storage for this very significant level of records.

In a more limited context, the Government Accountability Office (GAO) recently recognized the detrimental effects of the provision and recommended modifying the Privacy Rule to exempt public health disclosures from the accounting of disclosures provision.[9] GAO urges HHS to take immediate action to implement this change to the Privacy Rule, noting that the current accounting of disclosures requirement, particularly in reference to mandatory disclosures to public health authorities, could interfere with critical public health initiatives. The Confidentiality Coalition supports the GAO recommendations and is writing to the Secretary of HHS asking that the Department move expeditiously to implement this recommendation. However, the Confidentiality Coalition recommends that exemptions for accounting of disclosures not just be limited to public health disclosures, as GAO has suggested, but to all mandatory or routine disclosures, including those to government entities.

Efforts by ONCHIT to promote a nationwide efficient and interoperable health information system should include consideration of how the accounting of disclosures requirement could pose a significant barrier to participation. Although the issues are somewhat different depending on whether the system creates centralized data repositories or operates as a series of switches that utilize some type of master index function, the accounting of disclosure provisions will operate as a barrier to participation. For example, to the extent a centralized data repository is acting as a business associate of the data submitters, disclosures would need to be screened as to type, accounting records generated, and provided to either individuals or covered entities depending on the terms of the business associate contract. The technical and administrative hurdles posed by such a requirement would be immense. Alternatively, if the system operates as series of switches the functionality required to generate accounts of disclosures will again be technically and administratively onerous unless the requirements are eliminated or significantly narrowed.

---

[9] GAO, *Health Information: First-Year Experiences under the Federal Privacy Rule*, GAO-04-965 (September 2004) at 24.

III. Minimum Necessary

The Privacy Rule provides that covered entities must make "reasonable efforts" when using, disclosing or requesting protected health information, to limit the information to the "minimum necessary" amount needed to accomplish the intended purpose of the use, disclosure, or request. In addition, the regulation provides that covered entities may not use, disclose, or request an entire medical record unless the entire record is "specifically justified" as the amount of information reasonably necessary. Disclosures to, or requests by, a provider for treatment purposes are exempt from the standard as are uses or disclosures made pursuant to a written patient authorization. A covered entity may rely on a requested disclosure of protected health information from another covered entity as being the minimum necessary amount.

This standard puts covered entities receiving requests for information in the position of determining whether the requested information is the "minimum necessary" amount, when only the entity making a request for information has an informed basis for determining whether the information is the minimum necessary for its purposes. The legal uncertainty and risk created by this standard already has led to some "defensive" information practices that restrict the appropriate flow of information within the health care system. For example, some providers, citing the need to comply with the HIPAA Privacy Rule, have limited access by health plans to protected health information needed to perform quality assessment and improvement programs, utilization review, case management, disease management, and other functions related to maintaining the affordability of health coverage and improve outcomes.

For participants in a national or regional health information network, making minimum necessary determinations – or even determining if a requesting party or provider is a HIPAA covered entity – is likely to be extremely challenging. The uncertainty and resultant liability exposure associated with the minimum necessary standard is likely to serve as a barrier to participation in a NHIN. In its Request for Information, ONCHIT states that interoperability is "necessary for compiling the complete experience of a patient's care, for maintaining a patient's personal health records and for ensuring that complete health information is accessible to clinicians as the patient moves through various healthcare settings."[10] These goals simply cannot be fully met if a physician is required to adhere to a nebulous minimum necessary standard. The application of the minimum necessary standard to this effort may in fact increase medical error rates by limiting the flow of medical information in the health care system in a manner that is inconsistent with the provision of quality medical care. Consideration should be given to eliminating the standard, or creating a safe harbor for when personal health information is exchanged through a national health information network or regional health information exchange.

[10] 69 Fed.Reg. at 65,600.

IV. Research

Research uses and disclosures are an essential part of the National Health Information Infrastructure envisioned in the seminal report "The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care" ("Report") published by ONCHIT. The Report clearly contemplates that research, including data research, will be crucial to achieving key objectives of a NHIN, particularly the goal of improving population health. The Report for example recognizes that streamlining and standardizing quality-monitoring data will allow information on quality to be more completely aggregated and analyzed, "providing a comprehensive picture of quality both at the point of care and for research purposes." The Report notes further that: "Eventually an interoperable network of electronic health records would be able to accelerate translation of research into practice by tapping into national databases of clinical decision support and delivering the latest clinical knowledge to clinicians at the point of care."

The HIPAA Privacy rule also recognizes the importance of research to improving the quality of health care and took steps to ensure that researchers would have continuing access to health information. Under the Privacy Rule, numerous entities, including non-covered entities, receive and analyze de-identified data or limited data sets to assist health care providers, health plans, government, the health care management communities and manufacturers conduct market, utilization and outcomes research, implement best practices, and apply and benefit from economic analyses. Data researchers have helped implement prescription drug recall programs, performance of pharmaceutical market studies, and assessment of drug utilization patterns. In these areas and many others the HIPAA framework took care to protect patient privacy while permitting data use for research where appropriate. Ensuring that such access continues will be critical to realizing the goals set forth in the ONCHIT Report.

We are concerned, however, that in some instances the HIPAA Privacy Rule failed to achieve the proper balance and is inappropriately restricting access to health information for researchers. In particular, requiring expiration dates or events on all research authorizations and prohibiting individuals from granting authorization to use their health data in unspecified future studies is limiting the on-going use of research data in ways that are detrimental to the health care system. Under the Common Rule that has governed human subjects research for decades, it is generally permissible to obtain informed consent from a participant to use data for future research on data or biologic materials stored in databases or tissue banks. The Privacy Rule does not permit authorization for virtually any unspecified future uses. The Secretary's Advisory Committee on Human Subjects Protections (SACHRP) has recommended that the HIPAA Privacy Rule permit future uses that are allowed under the Common Rule. We agree that the Privacy Rule needs to be modified in this area and note that these restrictions, if not addressed, will have a significant impact on the ability of stakeholders to achieve critical goals set forth in the ONCHIT Report.

V. Liability Concerns

Liability concerns related to privacy and security breaches are already emerging as a barrier to participation in local and regional health information sharing initiatives. Addressing these concerns from a legal and regulatory perspective as described above will help these efforts and facilitate the emergence of a national health information infrastructure. Finally, we note that in the past there have been calls to create a federal private right of action for unlawful uses and disclosures of health information. We strongly oppose creating a federal cause of action and believe such a step would create a significant barrier to participation among the many stakeholders whose cooperation is essential to developing a national electronic system that will reduce dangerous medical errors, lower costs and improve care.

VI. Conclusion

We appreciate the opportunity to comment on ONCHIT's efforts to develop a meaningful and interoperable NHIN. As described above, we are concerned about the implications that the HIPAA Privacy Rule may have for such a system. Modifications to the Rule and/or significant clarifying guidance can help eliminate current barriers to participation in a NHIN.

Any questions can be addressed to Ms. Theresa Doyle, Senior Vice President for Policy, Healthcare Leadership Council (telephone 202-452-8700, e-mail tdoyle@hlc.org).

Sincerely,

AdvaMed
American Benefits Council
American Clinical Laboratory Association
American Hospital Association
America's Health Insurance Plans
Blue Cross and Blue Shield Association
ERIC – The ERISA Industry Committee
Healthcare Leadership Council
National Association of Healthcare Access Management
National Association of Health Underwriters
Premier, Inc.
U.S. Chamber of Commerce
VHA