Patient Identifiers and the National Health Information Network: Debunking a False Front in the Privacy Wars

Michael D. Greenberg & M. Susan Ridgely

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) of 1996\(^2\) did not mandate the creation of a National Health Information Network (NHIN), but it did address two of the key building blocks for developing such a network—electronic health records and a unique patient identifier (UPI) for every individual in the country.\(^3\) By putting these building blocks in place, the aim was to provide better infrastructure support for the linking of an individual's medical records across health care

---

\(^1\) Michael D. Greenberg is Policy Analyst, RAND Corporation; Research Director, LRN-RAND Center on Corporate Ethics, Law and Governance; and Adjunct Professor of Law, University of Pittsburgh School of Law; A.B., Cornell University; M.A., Duke University; Ph.D., Duke University; J.D., Harvard Law School. M. Susan Ridgely is Senior Policy Analyst, RAND Corporation; A.B., Bryan College; M.S.W., University of Maryland; J.D., University of Maryland. The authors thank Richard Hillestad, Ph.D., Jeffrey Rothenberg, Ph.D., and Roger Taylor, M.D. for their review and helpful comments. We also gratefully acknowledge the research assistance of Jane McClure, J.D. and Maggie Wu. This policy analysis was supported by grants from a consortium of health information technology companies, including: Cerner Corporation; Computer Program and Systems, Inc.; Intel; IBM; Microsoft; MISYS Healthcare Systems; Oracle; and Siemens. The views expressed are those of the authors and do not represent the views of the study sponsors.


organizations and jurisdictions. It was widely believed that a range of potential benefits might accrue as a result, including improved quality of medical care and reduced administrative costs.

According to Section 1173(b) of HIPAA, the Secretary of Health and Human Services (HHS) is required to adopt a standard for a unique health identifier "for each individual, employer, health plan, and health care provider for use in the health care system." Despite this provision in the statute, and the success HHS had in developing the standards for employer, provider, and health plan identifiers, Congress and HHS nevertheless put the development of a unique patient identifier on indefinite hold "until after comprehensive privacy protections [are put] in place." Since 1999, Congress has adopted legislative language to ensure that no such standard is promulgated without Congressional approval. Although there is considerable support in the health information technology industry for adoption of unique patient identifiers, it has become one of the most controversial aspects of HIPAA.

To date, the prospect of a UPI standard has generated considerable policy debate and political resistance, even though UPI itself represents only one of several methods for searching and linking electronic medical records. Concerns about UPI derive from its potential to drive new levels of interoperability for health information systems. In this vein, UPI can be viewed as a technology linchpin, the implementation of which might herald a new generation of health information networks, with downstream privacy and security implications that are difficult to foresee. Thus, although the federal government was empowered by HIPAA to adopt a UPI standard, it remains unclear how such a standard would ultimately affect the privacy and security of personal health information. Nor is it clear how other aspects of federal and state

---

4 See id. at 568-69.
5 See id.
8 See H.R. REP. NO. 105-825, at 1319 (1998) (Conf. Rep.). The report states, in part, “agreement includes a general provision proposed by the Senate modified to provide that none of the funds in this Act may be used to adopt a final standard providing for a unique health identifier for an individual until legislation is enacted specifically approving the standard.” Id.
privacy law might impact on a future NHIN, built on the backbone of a UPI-enabled architecture.

The main cautionary voices with regard to the development of the UPI have been health privacy advocates, and their supporters in Congress, who fear that federal privacy protections are insufficient to protect personal health information in the current environment—much less in a fully interoperable, web-based environment. Privacy advocates need look no further than recent newspaper headlines for substantial evidence of the failure of current protections in the public and private health care sectors. Meanwhile, the status quo of protection for health information is arguably more related to inefficiencies in local (and sometimes paper-based) record-keeping, rather than to robust legal privacy safeguards. A fully interoperable national network could easily exacerbate current privacy risks, by making identifiable health information far more widely available, and subject to the vicissitudes of local access controls and security protocols across tens or hundreds of thousands of institutional and regional data systems.

Far less political attention has been paid to other methods for searching and retrieving electronic medical records, such as the use of existing identifiers (e.g., names, birthdates, Social Security numbers (SSNs)) to link records by means of a matching algorithm. Obviously, these sorts of conventional identifiers themselves constitute sensitive information, and they entail privacy and security risks that go beyond the health care system. In the context of an emerging NHIN, the algorithmic solution to identity establishment could plausibly involve massive trafficking in demographic information across distributed health information networks, strictly for the purpose of identifying individual records in local databases (again, by searching records using probabilistic algorithms). Algorithmic matching also raises a series of questions about how future data and transmissions might be safeguarded, how access to local and regional networks should be controlled, and what sorts of authentication procedures should be incorporated into network architecture.

Although the central focus in the debate around UPI has involved privacy concerns, we suggest that those concerns may be substantially misdirected. When viewed narrowly, UPI might actually be superior to alternative techniques for linking

---

9 See, e.g., Gail White, Data Breach Involves Recent Births; Parents' Personal and Medical Information Improperly Discarded, Posing a Risk of Fraud, ATLANTA JOURNAL-CONSTITUTION, May 17, 2007, at 3B; Jennifer Gonzalez, 3rd Computer Breach at OU; Records Involve 60,000 Who Used Health Center, CLEVELAND PLAIN DEALER, May 12, 2006, at A1; Joe Rojas-Burke, Breach Fuels Privacy Legislation, THE OREGONIAN, May 23, 2006, at A03.
medical records, in regard to the protections UPI can offer for privacy and security. Viewed more broadly, the UPI debate is connected to a deeper set of unresolved privacy and security issues regarding the nascent National Health Information Infrastructure. Blocking the implementation of UPI has probably had the effect of slowing development of the NHIN, and limiting the interoperability of local networks. And although this might seem like a desirable goal to some advocates who fear that the risks to privacy of an NHIN are simply too great, we suggest that it may eventually be self-defeating as a strategy for protecting medical records. A better approach would involve addressing systematically the privacy and security challenges posed by the NHIN. As we will explain, UPI may paradoxically offer a helpful tool in building more robust privacy safeguards into the NHIN architecture.

In Part I of this paper, we briefly describe the concept of the NHIN, and the basic privacy problem that is posed by any technique for identifying and matching patients' electronic medical records. In Part II, we review the adequacy of current legal protections for privacy, in connection with interoperable health information systems such as the NHIN. This material provides necessary context for Part III, in which we assess the relative merits of the two main identity establishment models, UPI and algorithmic matching, on the criteria of privacy and security for personal health information. In Part IV, we outline a series of legislative and policy options that have been advanced by advocates to address legitimate privacy concerns, as the United States moves toward establishing an NHIN. We conclude this paper with some final observations about UPI, the NHIN, and reframing the policy debate in regard to the future of health information privacy.

Part I. NHIN, Patient Identification, and the Problems of Privacy

In adopting a national health information technology (IT) strategy, the Bush Administration, through the Office of the National Coordinator for Health Information Technology (ONC), is currently in the process of developing standards and a proposed "architecture" for a NHIN. The NHIN would facilitate interoperable health

10 The Office of the National Coordinator for Health Information Technology (ONC) was created by President George W. Bush in 2004 to "provide counsel to the Secretary of HHS and Departmental leadership for the development and nationwide implementation of an interoperable health information technology infrastructure." See Health and Human Services, Health Information Technology, Office of the National Coordinator: Mission, http://www.hhs.gov/healthit/onc/mission (last visited Apr. 19, 2008); see also President Bush's State of the Union, 2006 U.S.C.C.A.N. D3 (Jan. 31, 2006).
information exchange across the United States. An NHIN would link together local health IT systems across the country to allow authorized users (e.g., physicians, hospitals, public health agencies) to share clinical information in “real time.” The ultimate goals of the NHIN, as part of President Bush’s ten-year commitment to the promotion of health IT, are to improve administrative efficiency, reduce medical errors, improve quality of care, and provide better information for patients and physicians.

In undertaking this effort, the United States has joined a number of national governments in pressing health care systems into the 21st century using health information technology. However, unlike virtually all of the other countries, the U.S. is not developing a unique patient identifier to use as the singular key to file and retrieve individual health records. By contrast, most European Union and British Commonwealth countries have implemented or are developing UPI schemes to identify and match records across networked health information systems. HHS, which houses the ONC, has not funded any development work on the UPI since the late 1990s. None of the current NHIN architecture contracts funded by HHS has employed a UPI approach—thereby limiting the key purpose of those contracts, which was to experiment with and develop the best approaches to interconnectivity and interoperability among local health IT systems.

In addition, the United States’ strategy for developing the national health information network itself has evolved somewhat since its initial conception. The current view of ONC is that the NHIN should be developed through an incremental approach—that is, by knitting together regional health information organizations (RHIOs) that are currently being developed in states and local communities around the country. Rather than creating a truly national network, the ONC is content to let RHIOs develop their own health information exchange networks, as well as strategies

---

11 By “interoperable,” we mean that local health IT systems would share basic data standards and architectural features, so as to support the direct electronic exchange of information across local systems.
14 A regional health information organization (RHIO) is a collaborative, nongovernmental, multi-stakeholder organization, which operates to support the electronic exchange of health information across local institutional systems, and which seeks to ensure that such communications are both secure and in compliance with law.
for patient identification. Presumably, then, pairs of RHIOs will engage in bilateral contracts for information exchange across state boundaries, which implicitly will require protocols for electronic queries and identification of records between RHIOs. Over time, this will result in a “patchwork” NHIN, in which pairs of RHIOs can develop rules for information exchange that are compliant with local privacy and security requirements in each of their home states.

Under this kind of NHIN model, there will be no single strategy or technology for identifying patient records, and interoperability will be more limited and less elegant than in a “true” national network (i.e., one with uniform standards defining the basic parameters for systems architecture). Thus, the de facto national strategy for identification of patient health records is not UPI, but rather an unspecified, decentralized mechanism still to be determined, and one which will probably involve a mix of algorithmic matching techniques and local indexing of records, drawing on lots of different patient identifiers (including names, birthdates, addresses, SSNs, etc.). Unless federal policymakers do something to prevent it, or to change course, it is expected that a patchwork NHIN will gradually emerge on its own—although this evolution may take a long time, particularly if legal concerns undermine the adoption of electronic health records by medical providers. By implication, then, we can assume that: (1) we will eventually see an NHIN develop that is capable of supporting

15 See OFFICE OF THE NATIONAL COORDINATOR, ONC GOALS, OBJECTIVE, AND STRATEGIES 1, 9 (2006), available at http://www.hhs.gov/healthit/documents/ONCGoalsObjStr061306.pdf (last visited Apr. 19, 2008). The Office of the National Coordinator states, in part, “[h]ealth care continues to be delivered locally and regionally, and it is difficult for a top-down federal solution to meet the need of America’s diverse communities. Many states are developing strategies to foster health information exchange, but local and regional efforts are occurring as well....the states are the natural units for health information exchange customization, and should be supported and guided in this new role.” Id. On the other hand, ONC is funding a group of consortia to develop and test NHIN models with the intent to use what is learned from those efforts to describe best practices, common frameworks and, potentially, standards. See NEWS RELEASE, U.S. DEP’T OF HEALTH & HuMAN SERVICES, HHS AWARDS CONTRACTS TO DEVELOP NATIONWIDE HEALTH INFORMATION NETWORK, (Nov. 10, 2005) available at http://www.hhs.gov/news/press/2005pres/20051110.html.

16 Concerns about medical malpractice standards, Stark requirements, and anti-trust laws have been widely noted. “Stark” and “Stark II” refer to the Physician Self Referral Act, 42 U.S.C. § 1395nn (2000). Many have argued that Stark is impeding the establishment of health care arrangements that promote the adoption of HIT. See U.S. GOV’T ACCOUNTABILITY OFFICE, GAO 04-991R, HHS’S EFFORTS TO PROMOTE HEALTH INFORMATION TECHNOLOGY AND LEGAL BARRIERS TO ITS ADOPTION 1, 45 (2004), available at http://www.gao.gov/new.items/d04991r.pdf. Although Stark II created a “safe harbor” for “community-wide health information systems,” Congress did not define the term and there is no parallel exception under the federal anti-kickback law, which is codified at 42 U.S.C. § 1320a-7b(b) (2000).
automated exchange of records across state lines; (2) that the NHIN is likely to be "patchy" in the way that it implements patient identification, record queries, and retrievals, and consequently in the nature and degree of privacy risks that it poses; and (3) to the extent that privacy concerns about UPI basically derive from the establishment of any kind of national network, those concerns will become more salient and problematic over time, even while the federal government forecloses itself from implementing a federal UPI scheme.

It is also important to recognize that a patchwork NHIN model does not foreclose the assignment of unique identifiers to tag consumers' medical records, but merely implies that the federal government will not be involved in doing this on a national scale. In particular, HIPAA imposes no federal bar against RHIOs, states or private corporations developing their own patient identification strategies and unique identifiers. When Congress barred HHS from dealing with the UPI problem, they essentially abdicated federal control in favor of action by private-sector entities and/or by other government actors or non-governmental organizations (NGOs). So the chief question for privacy advocates is not so much whether a particular UPI scheme might be legal under federal (or state) rules, but instead to determine what the privacy implications are of a patchwork NHIN, in connection with its need to match and link electronic records on national scale. By corollary, the patchwork model implicitly invites comparison with a hypothetical NHIN that identifies individual records by drawing on a federal UPI.

Any method of patient identity establishment—whether it draws on a UPI scheme or on an algorithm-based method for searching records using demographic information and/or existing identifiers (i.e., SSNs)—presents a set of challenging questions under privacy law. What limits, if any, do federal and state laws potentially impose on different identity establishment models? And what kinds of liability risks, if any, would RHIOs and their member organizations assume through participation in health information exchange? Moreover, what liability risks would they assume through their adoption of a specific identity establishment framework? We address

---

17 For example, in testimony before the Electronic Health Records Workgroup of the American Health Information Community (which is an advisory panel to ONC), Michael Kidney of Hogan & Hartson LLP advised that while there was not much case law on electronic health records, lawsuits based on alleged negligence in checking a patient’s medical history often hinged on the accessibility of the records. Therefore he suggested that if EHRs [and by extension health information exchange] make records more accessible, “the burden on providers will potentially increase exponentially.” Andis Robeznieks, *EHR Legal Issues Unclear*, MODERN HEALTHCARE, Jan. 12, 2007.
these questions in subsequent sections of this paper. At the outset, we would emphasize that the meaning of existing privacy rules is necessarily speculative and frequently unclear, as applied to future health information technologies that have not yet been implemented.\textsuperscript{18} In the face of similar ambiguity, researchers have suggested that law sometimes exerts its effect on the healthcare system by influencing the perceptions and expectations of market actors, in ways that can change their business practices based on anticipated (but not necessarily realized) adverse legal outcomes.\textsuperscript{19}

Regardless of whether Congress chooses to revisit the UPI issue nationally, the emerging NHIN will force the federal government to deal with legal concerns that have been raised by various privacy advocates (for example, the need to modify the HIPAA Privacy Rules in light of exigencies posed by networked information sharing). Otherwise, the NHIN will almost certainly end up degrading existing federal privacy protections for health information, by making the transfer of medical records and sensitive identifiers more fluid, while attenuating the responsibilities of individual participants within the national network.\textsuperscript{20} Similarly, in the absence of a comprehensive review and approach to "harmonizing" current state laws around health information privacy and security, the evolving NHIN will also run the risk of precluding or significantly restricting the sharing of certain kinds of sensitive records (e.g., on HIV, STDs, and mental health treatment) across state lines. Here again, the ultimate question posed by the NHIN is not whether one method of patient identity establishment is more acceptable under federal or state law, but rather whether an incremental approach to patient identification and record safeguarding in the NHIN—built RHIO by RHIO—is better for privacy and security than a uniform national approach.\textsuperscript{21}


\textsuperscript{19} M. Gregg Bloche & David M. Studdert, A Quiet Revolution: Law as an Agent of Health System Change, 23(2) \textit{HEALTH AFFAIRS} 29, 30, 39 (2004).

\textsuperscript{20} See Greenberg, Ridgely & Bell, supra note 18, at 466-67.

\textsuperscript{21} It is also important to acknowledge that there are other models for patient data storage and exchange that are not centered on RHIOs and the NHIN. Such models include personal health records (PHRs) that may be portable (USB ports) or web-accessible (such as those currently being developed by employers and insurance companies). A discussion of the legal issues attendant to these alternatives is beyond the scope of this paper. We would note, however, that federal regulators have cautioned consumers to consider carefully whether to participate as their health information in PHRs may not be protected under HIPAA. See Audio Tape: Remarks of Sue McAndrew, Deputy Director for Health Information Privacy, HHS Office of Civil Rights, Personal Health Records & The New Risks Over Privacy, Security and HIPAA (Melamedia, L.L.C. 2007) (on file with author). See also Letter from Rose Marie Robertson & Nancy Davenport-Ennis, Co-chairs, Consumer Empowerment Workgroup, to The Honorable Michael O. Leavitt, Chairman, American Health Information Community (Jan. 23, 2007) (on file with...
Part II. The Adequacy of Current Privacy Protections for the NHIN

Any discussion of medical records privacy has to begin with an acknowledgment: safeguards for health information privacy and security are currently imperfect, and they will remain imperfect in the future. Therefore, the assessment of technical alternatives for patient identity establishment in the NHIN involves a discussion of trade-offs in privacy, security, and functionality in medical record-keeping. Again, in large measure, the current state of protection for personal health information is more a function of the inefficiency of our paper-based medical records systems, rather than any particular strength in the legal safeguards for health information now in place. Notwithstanding the current federal and state law framework for protecting health information privacy, the existing safeguards have already been described as “surprisingly fragile.” Multiple commentators have outlined the additional risks to privacy posed by a fully interoperable system without good access restrictions, focusing on the potential for decentralized control, diffusion of responsibility, and ambiguity of legal obligations in an environment where providers are disclosing to, and drawing from, a network of national scope.
A brief review of existing federal and state protections helps to explain the concerns of privacy advocates, the Congress, the Government Accountability Office (GAO), and other stakeholders regarding the continued development of the NHIN in the absence of ONC having first developed a "comprehensive federal privacy approach." Although Congress stopped funding for the implementation of a federal UPI standard based on privacy concerns in 1999, ONC has nevertheless continued work on the NHIN, arguably without adequately addressing the same privacy concerns that caused Congress to table the UPI in the first place.

The HIPAA Privacy Rules

Federal law provides some protection for health care information that identifies, or could be used to identify, individuals. In 1996, Congress passed HIPAA to ensure the portability of health coverage and to set standards for administrative simplification. As an integral part of HIPAA, Congress set in motion the development of the first comprehensive set of federal privacy rules for identifiable health care information.

scenario of privacy advocates. Making patient safety information available to all healthcare providers that are even tangentially involved in a patient's care renders the level of privacy and security afforded that data a function of the weakest link in the system. Fully interoperable data is also immeasurably more valuable for secondary uses (e.g., marketing) and is an irresistibly tempting target for commercial aggregators." See Testimony of Nicholas P. Terry, supra note 22.

25 GOVERNMENT ACCOUNTABILITY OFFICE, HEALTH INFORMATION TECHNOLOGY: EARLY EFFORTS INITIATED BUT COMPREHENSIVE PRIVACY APPROACH NEEDED FOR NATIONAL STRATEGY, GAO-07-238, (2007). In addition to officials at the GAO, members of federal advisory panels have publicly criticized ONC for the lack of progress on privacy issues. See Letter from Janlori Goldman and Paul Feldman to Dr. Robert Kolodner, (Feb. 21, 2007) at http://www.healthprivacy.org (announcing resignation of Paul Feldman). Paul Feldman, the Chair of the Privacy and Security Workgroup of the American Health Information Community, which HHS appointed to provide guidance to its HIT efforts, resigned in frustration this spring stating that the panel had met infrequently and then only to focus on formulating policy based on limited case studies. See id. The letter from Feldman, the Director of the Health Privacy Project at Georgetown University, states that "the failure to achieve a privacy framework acts as a significant barrier to a robust and secure environment for e-health." Id.

26 Mark Rothstein, who chairs the NCVHS Subcommittee on Privacy & Confidentiality, was recently quoted as saying that "a sense of urgency is lacking" at HHS and that "time is of the essence" as the private sector "is racing ahead" to establish interoperable networks and data banks. See Robert Pear, Warnings Over Privacy of U.S. Health Networks, N.Y. TIMES (Feb. 17, 2007) available at http://www.nytimes.com/2007/02/18/washington/18health.html. Rothstein also suggested that Congress should not provide more money for the development of the NHIN unless HHS "[does] more to protect the privacy of electronic medical records." Id.

27 The HIPAA Privacy Rules define "individually identifiable health information" as "a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2)
However, it has previously been observed that HIPAA did not anticipate the development of fully interoperable health care networks. Also, privacy advocates have complained that the final Privacy Rules (as opposed to the draft rules) involved a significant re-balancing of interests, with the effect of favoring the efficiency of health care institutions at the expense of privacy rights for individuals. The prospect of an NHIN brings these privacy issues into the spotlight once again, regardless of whether the NHIN eventually incorporates a UPI technology.

A host of concerns have been raised about the application of existing federal privacy laws to the emerging NHIN. Chief among the concerns is that the HIPAA Privacy Rules apply directly only to a limited number of entities—health care providers, plans, and clearinghouses (collectively, “covered entities”)—and not to the full panoply of organizations that will be involved in collecting, processing, and using health records in regional interoperable systems and the NHIN. In particular, the status of RHIOs is notably ambiguous under the HIPAA Privacy Rules, and in many instances RHIOs may be regulated only indirectly as “business associates.”

related to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (i) that identifies the individual; or (ii) with respect to which there is reasonable basis to believe the information can be used to identify the individual.” 45 C.F.R. § 160.103 [emphasis added].

28 Greenberg, Ridgely & Bell, supra note 18, at 462.
29 HHS promulgated draft Privacy Rules in 2000. See 65 Fed. Reg. 82,462, 82,810-11 (Dec. 28, 2000). The draft Privacy Rules made the use of protected health information for purposes of treatment, payment and operations (TPO) contingent on written consent by the patient. However, after receiving public comment that such a requirement would be onerous, in the Final Privacy Rules patient consent was not required as a predicate for using protected health information for TPO. See Standards for Privacy of Individually Identifiable Health Information 45 C.F.R. § 164.506(a). However, the Final Rules included a strengthened notice requirement intended to preserve some aspects of the patient consent process. See 45 C.F.R. § 164.520.
30 See 45 C.F.R. § 160.102(a)(1)-(3). Providers who transmit health information in electronic form are covered entities, meaning that, unless a healthcare provider refuses to accept health insurance or refuses to participate in any HMO networks, it may be impossible to avoid regulation under the Rules. See § 160.102(a)(3). However, it has been noted that there are organizations that receive and use protected health information that are not covered entities, including workers compensation carriers, researchers, life insurance issuers, employers and marketing firms. See Joy Pritts, Assistant Research Professor, Health Policy Institute, Georgetown University, Testimony Before the Subcommittee on Health of the House Committee on Ways and Means (Jul. 27, 2005), available at http://waysandmeans.house.gov/hearings.asp?formmode=view&id=3950.
31 See 45 C.F.R. § 160.103 (defining a business associate as a person who on behalf of a covered entity “performs, or assists in the performance of...a function or activity involving the use or disclosure of individually identifiable health information”). The Privacy Rules require that covered entities engage their business associates in data sharing agreements, to establish
ambiguity in the HIPAA status of RHIOs could become a significant source of future problems for the NHIN. More generally, the National Committee on Vital and Health Statistics (NCVHS) has suggested that the current “business associate” rules under HIPAA are unlikely to be sufficient to protect privacy of personal health information, given a developing NHIN, increasing interoperability of local health information systems, and more and more participants in the national network. Given this vision of the future, privacy advocates might reasonably fear that confidentiality of health information in the emerging NHIN will only be as strong as “the weakest links” within the network.

The growth of the NHIN poses a number of other fundamental challenges under current federal privacy rules. For example, medical providers presumably have an obligation to ensure that downstream network recipients of protected health information will also take reasonable steps to safeguard it per HIPAA mandates, but the contours of required due diligence have never been defined. Meanwhile, expanded contractual obligations for the business associates to protect health information. See 45 C.F.R. § 164.502(e)(1).

See GAO, supra note 25, at 23. The GAO investigation noted that “[a]n official with one information exchange organization stated that he found it hard to determine if his organization was a covered entity or a business associate. In some cases, according to an official with a health information privacy professional association, health information exchange organizations may not even be business associates as defined by HIPAA.” Id. The GAO went on to conclude that “[t]he differences between, or uncertainty regarding, the extent of federal privacy protection required of various organizations may affect providers’ willingness to exchange patients’ health information, if [providers] do not believe it will be protected to the same extent they protect it themselves.” Id.

The NCVHS suggested that protected health information “may lose its protection as it travels from a [HIPAA] covered entity to a non-covered entity.” NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS, RECOMMENDATIONS TO THE SECRETARY OF HHS REGARDING PRIVACY AND CONFIDENTIALITY IN THE NHIN, June 22, 2006, at http://www.ncvhs.gov/, at 12. In a similar vein, at least one legal analyst has noted that many web sites that host personal health records do not fall into any of the existing categories of covered entities, and thus information posted in the PHRs on these web sites is not covered by the HIPAA Privacy Rules – and is unlikely to be covered by state privacy statutes. See Joy Pritts, Testimony Before the NCVHS National Health Information Infrastructure Workgroup, Hearings on Health and the National Information Infrastructure: The Personal Health Dimension (Jan. 27, 2003), available at http://www.ncvhs.gov/030127p2.htm, at 3.

See Testimony of Nicholas P. Terry, supra note 22, at 8.

See Greenberg, Ridgely & Bell, supra note 18, at 465. The legal expression “due diligence” refers to the prudence and care that is properly to be expected from a reasonable person when confronting a particular set of circumstances. Id. As applied to a HIPAA covered entity making disclosures of PHI into a computer network, we ask what level of prudent investigation or “due diligence” is required by HIPAA on the part of the disclosing entity, in order to ensure that all
access to information through the NHIN will likely diminish the ability of any particular covered entity to supervise the activities of its own business associates, much less to validate the legitimacy of other participants or of record queries within the national network. The probable result will be to expand privacy risks for protected health information. In a related vein, the “treatment, payment, and operations” (TPO) exemption under HIPAA, which allows covered entities to use protected health information without patient authorization, threatens to become extremely broad in the context of a highly interoperable national network, to which all providers contribute protected information, and in which no provider exerts control over distributed records. The ultimate concern is that the TPO exemption might eventually swallow the general requirement for patient authorization, and that increasingly fluid exchange of records over the national network might eventually come about as a result.

Another key aspect of the Privacy Rules is the “minimum necessary” standard, which requires covered entities to refrain from using or disclosing any information that is not necessary to satisfy a particular, legitimate purpose in communicating protected health information. Covered entities are generally required to enact safeguards to limit the scope of their disclosures accordingly, but communications in the course of treatment fall outside the scope of the minimum necessary provision. In the context of the emerging NHIN, it is not clear how covered entities would even attempt to comply with the minimum necessary rule, given increasingly automated information sharing with large numbers of other parties in a distributed network. There is also the possibility that the existence of a national network may itself expand the scope and volume of “treatment related” communications, in a way that further erodes the protection that the minimum necessary rule was intended to convey.

In addition to concerns about the regulations, advocates have expressed possible recipients of information on the network have instituted HIPAA-compliant safeguards for privacy and security. Id.


37 See Greenberg, Ridgely & Bell, supra note 18, at 465. See also Testimony of Nicholas P. Terry, supra note 22, at 10.

38 See 45 C.F.R. §§ 164.502(b), 164.514(d); see also OFFICE OF CIVIL RIGHTS, STANDARDS FOR PRIVACY OF INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION 8 (Dec. 3, 2002, revised Apr. 4, 2003), at http://www.dhhs.gov/ocr/hipaa/guidelines/minimumnecessary.pdf. The minimum necessary standard does not apply to disclosures by a provider for treatment purposes, disclosures to the patient, disclosures pursuant to a patient’s authorization, disclosures required by law, or those required for compliance with the HIPAA administrative simplification rules or enforcement activities. Id.
concerns about the regulators. Possibly the complaint most consistently lodged against HHS, as the chief federal privacy regulator, has been lack of enforcement of the Privacy Rules.\textsuperscript{39} Although HIPAA provides for both civil and criminal penalties\textsuperscript{40} for wrongful disclosure or use of protected health information by covered entities,\textsuperscript{41} advocates complain that HHS has declined to enforce the law.\textsuperscript{42} HHS has chosen, instead, a non-adversarial approach to compliance that "seek[s] the cooperation of" covered entities—even providing "technical assistance" to help them comply.\textsuperscript{43} For a variety of reasons already discussed, privacy and security risks to information are likely to increase as a patchwork NHIN comes into being. Weak enforcement of HIPAA requirements gives privacy advocates yet another reason to be concerned about the development of the NHIN.

Perhaps the most notable observation about these various HIPAA-related concerns is that \textit{none of them is affected directly by the technology of patient identity establishment or whether the national network makes use of a UPI scheme}. If we are correct in the presumption that a patchwork NHIN will emerge regardless of the federal prohibition against UPI, then these sorts of privacy concerns and legal ambiguities will need to be handled through future policy reforms.

\textbf{State Privacy Laws and the Conflict of Laws Problem}

Of course, students of HIPAA will be quick to point out that federal privacy rules establish only part of the legal framework for privacy protection in the United States. In particular, HIPAA is notable for including a "floor" pre-emption provision; the federal law supercedes state law only in establishing a baseline of privacy protection for personal health information, but allows the states to enact and enforce stricter

\textsuperscript{39} Note that the Privacy Rules provide a process for individuals to file complaints with HHS (under 45 C.F.R. § 160.306), but do not create a private right of action under federal law. \textit{See} 45 C.F.R. § 160.306.

\textsuperscript{40} The Secretary of HHS is empowered to impose a civil monetary penalty of $100 per violation for at least some parts of the HIPAA statute (fines are capped at $25,000 per violator per year) and the statute provides that a person who knowingly obtains or discloses health information may face criminal penalties including fines and imprisonment, with stiffer penalties for those who obtain and/or disclose under false pretenses or for purposes of commercial advantage. \textit{See} 42 U.S.C. § 1320d-5, 1320d-6 (2008).

\textsuperscript{41} By contrast, if business associates violate their contracts with covered entities, HHS is powerless under the Privacy Rules to impose civil or criminal penalties.


\textsuperscript{43} \textit{See} OCR Privacy Brief, \textit{Summary of the Privacy Rule: HIPAA Compliance Assistance}, at 17 (last revised May 2003), \textit{available at} http://www.hhs.gov/ocr/privacysummary.pdf.
privacy regulations and rights. The result has been to inject even more ambiguity into applicable legal safeguards and standards concerning medical information in different parts of the country. Several commentators have noted that states are all over the map in the degree to which they have instituted their own privacy rights and requirements, as by state legislation, regulation, or (in a few instances) constitutional provisions. In connection with the developing NHIN, there are two implications to the heterogeneity of state privacy laws: (1) that the NHIN may be even “patchier” and slower to develop than it otherwise would be, and (2) that inconsistent legal standards may contribute further to erosion in the existing privacy protections.

The GAO picked up a related theme in criticizing the lack of federal action on privacy, emphasizing the need to reconcile differences in state law privacy requirements as a “widely acknowledged challenge to ensuring the privacy protection of health information exchanged on a nationwide basis.” The GAO noted that the health information exchange officials with whom they spoke had concluded that states will need to make their own assessments about privacy law in other states and ultimately to determine the extent to which they can exchange information with providers beyond their own borders. Consequently, legal counsel for RHIOs and providers might plausibly decide that there are states whose laws will not provide a sufficient level of privacy protection for identifiable health information—and therefore refuse to share health information with other RHIOs and health care providers based in those states. It has even been suggested that the “multiplicity and inscrutability of [privacy] laws” may preclude the development of a fully interoperable health information system at the national level.

NCVHS brought the problem into sharp relief by focusing on the concrete dilemma that providers will face in an NHIN. NCVHS asked, “what law would apply to an individual’s health records created in states A and B, stored or accessed through a

44 Section 264 under HIPAA states, in pertinent part, “(2) PREEMPTION. --A regulation promulgated under paragraph (1) shall not supersede a contrary provision of State law, if the provision of State law imposes requirements, standards, or implementation specifications that are more stringent than the requirements, standards, or implementation specifications imposed under the regulation.” Pub. L. No. 104-191, § 264 (1996).
46 GAO, supra note 25, at 23.
47 GAO, supra note 25, at 23.
RHIO in state C, disclosed to an entity in state D for use in state E?"\(^{49}\) At least one legal scholar anticipated this kind of question, suggesting that patients should be concerned about the transit of their personal health information across state boundaries because "whatever privacy laws exist in their state may not protect their records once those records cross the state’s border," and concluding that the current patchwork of state laws is "not a viable means of enforcing the privacy of medical records in such a nationwide network."\(^{50}\) Another legal scholar agreed, and suggested that a state-by-state approach to regulation "is not compatible with modern methods of health care finance and delivery."\(^{51}\) She continued, "Lack of uniformity of privacy protections may also impair a patient’s ability to make meaningful consent to disclosure, because of failure to understand which [substantive privacy] regulations apply, and [the lack of uniformity] may [therefore] undermine efforts to automate health care information."\(^{52}\)

To date, federal efforts to address the problems of inconsistent state privacy laws have been limited at best. According to information provided by ONC to NCVHS and the GAO, the ONC’s original plan was to address the conflict-of-laws issue through one of several multi-million dollar contracts let during the past four years.\(^{53}\) Most important in this regard, the ONC awarded a contract on privacy and security issues to Research Triangle Institute (RTI) and the National Governors Association (NGA) in September 2005.\(^{54}\) Under that contract, RTI formed the Health Information Security and Privacy Collaboration (HISPC), consisting of "a multidisciplinary team with

\(^{49}\) Nat'l Comm. on Vital and Health Statistics, Recommendations to the Secretary of HHS Regarding Privacy and Confidentiality in the National Health Information Network (June 22, 2006), available at http://www.ncvhs.hhs.gov/0606221t.htm.

\(^{50}\) Wymore, supra note 3, at 565.

\(^{51}\) See Patricia I. Carter, Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age”?, 25 WM. MITCHELL L. REV. 223, 284 (1999).

\(^{52}\) Id. at 284-285.


\(^{54}\) According to the RTI website, the HHS contract was awarded for a collaborative project with the Office of the National Coordinator for Health Information Technology (ONC) and the Agency for Healthcare Research and Quality (AHRQ), and:

[The parties intended] to implement a process to facilitate the assessment of variation in business policies and practices regarding the privacy and security of health information exchange by individual states and territories. The goal is to develop a process that will allow states to identify and resolve barriers to health information exchange on a nationwide basis.

expertise in privacy and security law and in health care management as well as up to 40 state or territorial governments.” The aim of the HIPSC collaboration was to facilitate interoperable health information exchange nationally, by identifying and resolving privacy and security issues.

Surprisingly, though, the conflict of laws among the states specifically was not on the agenda of the HISPC. While individual state and territorial research sub-contracts have focused attention on identifying all relevant statutes and regulations within their state or territorial boundaries, conflict of laws across boundaries has not been a primary focus of the HISPC project. We were told instead that the State Alliance for eHealth, another HHS contract with the National Governors Association, would take up the conflict-of-laws issue during its one-year duration. According to a recent news article, however, preliminary efforts of the State Alliance project have focused instead on developing “safe harbor” legislative language to protect health care providers from penalties if they break a state law while exchanging information across state lines, creating definitions for the terms “consent” and “authorization,” and recommending content for patient authorization forms.

Although the HISPC chose not to deal with the issue of conflict of laws, at a “reporting out” meeting the HISPC director and HHS project officers suggested that the solution to the conflict-of-laws problem lay in the development of a single model privacy statute that would then be enacted in all fifty states. The proponents seemed unaware that a similar effort by the National Conference of Commissioners on Uniform State Laws to enact a model health care privacy statute had occurred in the 1980s, but was a failure—with only two states enacting the model code.

55 Id.
56 Personal communication: Linda Dimitropoulos, Project Director for HISPC, Research Triangle Institute (RTI) International; Michelle Lim Warner, Senior Policy Analyst, National Governors Association (NGA); Susan Christensen, Project Officer, Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services; and Jodi Daniel, Project Officer, ONC, U.S. Department of Health and Human Services.
59 Personal communication, supra note 56.
Ultimately, it is likely that the federal courts will become the venue for parsing out a complex soup of conflict-of-law and pre-emption issues, in connection with future disputes over privacy standards and violations within the NHIN. As suggested by Professor McLaughlin, however, ONC still has an important role to play in the meantime, in seeking proactively to address ambiguities in privacy requirements and mitigate potential legal conflicts.\textsuperscript{61} He concludes that, "[a]lthough federal courts are certain to wrestle with how the NHIN, HIPAA, and state medical privacy laws intersect, the federal government must empower and assist local organizations in preparing for this foreseeable legal uncertainty."\textsuperscript{62}

Here again, the ambiguity around state privacy laws and the NHIN appears to have little to do with UPI, or with the technical methods of patient identity establishment within computer networks. Regardless of how medical records are identified and indexed, states' differences in privacy laws are likely to create a host of barriers and risks connected with the emergence of the NHIN. For patients, these risks include the possibility that records generated in one jurisdiction may lose some of their protections when transported to other locales—a risk exacerbated by the fact that the NHIN may well involve lots of record queries and transmissions between states, with attenuated local control over records. On the other hand, inconsistent state laws will also likely restrict the flow of protected health information across at least some state lines. That result could be desirable to some stakeholders, for the same reason that stonewalling a federal UPI scheme has been desirable—namely, as an indirect way to limit the growth of truly interoperable health networks nationally.

**Part III. The Relative Merits of the Two Main Identity Establishment Models**

The idea of a federal UPI, as prescribed by HIPAA, quickly became a lightning rod for concerns about privacy and security within a hypothetical NHIN. However, most of the concerns raised by opponents of the UPI have little to do with identity establishment per se, and more to do with access, authorization, authentication and consumers' control over their own private health information. Although meritorious, many of these concerns about health information privacy can better be addressed through the development of a strong architecture for the NHIN, while other concerns will need to be addressed by making improvements in current legal protections at the

\textsuperscript{61} See McLaughlin, \textit{supra} note 36, at 55.

\textsuperscript{62} See McLaughlin, \textit{supra} note 36, at 55. McLaughlin notes that in 2003 a federal district court initially held that the Commerce Clause of the U.S. Constitution prohibited state medical privacy laws from regulating interstate transmission of personal health information. McLaughlin, \textit{supra} note 36, at 55 n. 202 and accompanying text.
federal and state levels. Importantly, none of these concerns derives from UPI itself; nor are they resolved by foreclosing UPI in favor of an alternative technical method for searching and retrieving medical records over computer networks.

Elsewhere, we and our colleagues have described how systems architecture for the NHIN might be constructed to enhance both privacy and security. Nevertheless, it is clear that whatever the eventual NHIN architecture, health information should be legally restricted to prevent use other than for health purposes—and to prevent cross-linking with other sensitive information (such as financial data). In the next section of this paper, we will address policy options in the legal arena for accomplishing these restrictions in the context of the NHIN. Here we discuss the narrower question of patient identity establishment, and the relative merits of two competing models of identity establishment, focusing primarily on privacy concerns and liability issues. We first examine the legal implications of a UPI-enabled NHIN architecture. We then compare the implications of an NHIN architecture based on an algorithmic approach to identity establishment.

Unique Patient Identifier

To analyze the merits of a specific method for establishing patient identities within electronic records, one must ask the question, "is it better, as compared to what?" It is an understatement to say that privacy and security of identifiable health information in the current paper-dominated system is less than perfect. It has been argued that the use of a UPI would, in fact, reduce risks in the current system:

"[B]ecause identifiers differ across organizations... Records... contain


64 Our analysis in this article is specific to HIPAA, but we would note that other federal laws could limit participation by some healthcare providers in patient identity establishment schemes. The Privacy Act of 1974 (Pub. L. No. 93-579, § 788 Stat. 1896, 1909 (1974), reprinted in 5 U.S.C. §522(a) (2003)) limits the ability of the federal government to use and disclose personal information, including SSNs. Conceivably, Privacy Act restrictions on using or disclosing SSNs and other demographic identifiers could apply to federally funded healthcare facilities (e.g., VA hospitals). In addition, according to an analysis by Donna Boswell of Hogan & Hartson LLP, exchange of health care records by institutions could, under some circumstances, be subject to regulation under several other federal laws, including GLB (Gramm-Leach-Bliley Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338), FERPA (Family Education Rights & Privacy Act of 1974, codified at 20 U.S.C. § 1232g), and/or FCRA (Fair Credit Reporting Act, codified at 15 U.S.C. § 1681). See Boswell, supra note 48, at 9.
more elements of identifying information than might be necessary with a [UPI]. A typical health record contains a patient’s name, gender, address, phone number, birth date, Social Security number, health insurance number, employer and relationships to other family members. These elements are necessary to promote the correct matching of a particular individual with an individual record. Additionally, a paper medical record that bears a patient’s name on the outside of the folder is much more ‘open’ to anyone who deliberately or accidentally comes into contact with it. Ironically, this use of personal information for matching people and records generates little controversy despite the lack of security standards and privacy protections in place today.”

A comprehensive analysis of unique patient identifier options, commissioned by HHS before the Congressional ban on development of standards for the UPI, supported the use of a UPI and concluded that among its strengths was accurate identification without the “repetitive use and disclosure of an individual’s personal identification information,” thereby preserving anonymity, protecting privacy, and preventing unauthorized access to health information. While acknowledging the possibility of risks associated with misuse of the UPI, the author stated, “[s]ince access to healthcare information is possible even without the use of a [UPI], the solution to this and other legitimate concerns does not lie in eliminating the use of a [UPI],” and, quoting from a contemporaneous National Research Council report, suggested that the threat of “rigorously enforced” legal sanctions would limit the potential for abuse.

By contrast, in 2005, when HHS solicited comments from the public via a Request for Information (RFI) on the NHIN, ONC reported that a leading privacy concern discussed by many respondents was the use of a national patient identifier. A

---

67 *Id.* at pt. 4 (quoting COMM. ON MAINTAINING PRIVACY & SEC. IN HEALTH CARE APPLICATIONS OF THE NAT’L INFO. INFRASTRUCTURE, NAT’L RESEARCH COUNCIL, FOR THE RECORD: PROTECTING ELECTRONIC HEALTH INFORMATION 188 (National Academy Press 1997)).
68 OFFICE OF THE NAT’L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEPT OF HEALTH & HUMAN SERV., SUMMARY OF NATIONWIDE HEALTH INFORMATION NETWORK (NHIN) REQUEST FOR INFORMATION (RFI) RESPONSES 22 (2005), available at
number of respondents stated that the risk of accidental and intentional privacy and security breaches would be heightened with a UPI, and some were of the opinion that a UPI was not needed from a technical perspective. However, the ONC report also notes that an almost equal number of respondents supported using a UPI, with some arguing that with use of an algorithmic identifier the “management of false positive identifications (i.e., where the wrong patient record is provided) and false negatives (i.e., where the patient’s record exists, but is not found) could be extensive and difficult to manage.”

In analyzing the relative merits of the UPI from a legal perspective, we begin with a few assumptions. For the sake of argument, we assume that there is a federal UPI scheme (i.e., a single standard for generating unique patient ID numbers with consistent application throughout the United States). A federal UPI would have some important technical advantages, and would be the first step toward a “true” NHIN (i.e., a national health information network with uniform data standards for all kinds of health information). We also assume that any federal UPI scheme would be “voluntary,” in the sense that it would allow some people to opt-out of having a UPI, which either means that the NHIN would have to support algorithmic matching for the opt-outs, or that the opt-outs effectively would have chosen to forfeit participation in the NHIN itself (and therefore their records will have to travel in old fashioned and inefficient ways). Given these assumptions, what legal issues does the UPI model of patient identity establishment pose?

First, as we have already discussed, HHS is currently foreclosed from implementing a federal UPI scheme by federal legislation. Congress suspended funding for the implementation of a UPI standard in 1999, and therefore development of a federal UPI would either require that Congress revisit this issue, or else would require agreement and implementation through non-governmental entities—such as the UPI proposal offered by ASTM. Note again that there is no federal law barring states or


69 Id.

70 Id. at 22-23.

71 For purposes of brevity this will be a simplified discussion based on a few generic assumptions. More complicated variations will undoubtedly raise additional legal issues. Since no national UPI currently exists, and algorithmic systems are only beginning to be tested, our ability to state what will be the influence of current law on future technologies is speculative at best.

72 See supra note 30, 65-66 and accompanying text; see infra text accompanying notes 106-07; see infra note 108 and accompanying text.

private entities from creating their own UPI standards.

Second, any actual identifiers under a UPI scheme would immediately become protected health information under HIPAA, just as any demographic information collected by HIPAA covered entities is already protected, and a UPI (if unencrypted) would obviously be sensitive in itself. That means that all of the current privacy and security obligations for HIPAA covered entities under federal law with regard to identifiable health information would extend to the new identifiers. Likewise, any state laws concerning the privacy of health information would also potentially extend to cover new identifiers as well. Even though the HIPAA Privacy Rules would protect the UPI, as well as the health information linked via the UPI, the fact that HIPAA fails to impose privacy obligations on non-covered entities would remain a problem in a UPI-enabled interoperable health care network. Consequently, related privacy risks might be exacerbated by UPIs, particularly to the extent that UPIs facilitate distributed networks within the NHIN, and that UPIs themselves become a target for illicit access.

This latter point deserves further comment. Unlike SSNs, which are especially sensitive because they can be used to link to individual financial records, and which have become a target for organized crime, access to UPIs would not necessarily provide access to anything other than medical records. As a result, their attractiveness to criminals, and their sensitivity if breached, are arguably diminished by comparison with SSNs. Moreover, UPIs might not even grant illicit access to medical records, if encryption is widely employed within a future NHIN. For example, public key encryption (PKE) is a type of cryptography that uses a public/private key pair of mathematically related numbers. The public key can be made available to anyone without risk, because it cannot be used to decrypt information without the corresponding private key, which the system administrators keep private. Thus, even if UPIs did become a target for criminal misappropriation in the future, security techniques like PKE encryption might nevertheless limit the risks to personal health information.

numbers because the system has no facility to guarantee that a patient does not already have an identifier obtained from another provider, and a separate identifier can be used to protect certain very sensitive information (such as HIV status or mental health treatment) without revealing that such information exists. In that sense, the ASTM UPI is not truly a unique identifier and health care providers would need all of the patient's UPIs in order to access their complete record. The positive aspect from the patient's point of view is that the patient can control access to very sensitive information by simply not sharing the additional UPI(s).


75 For a further discussion of the merits of PKE in this context, see HILLESTAD, ET AL., supra note 63.
Regardless, unapproved access to medical records could clearly have devastating consequences for some people (e.g., in situations where genetic information could conceivably be used by employers or insurers to deny employment or insurance to individuals who have markers for expensive, chronic health conditions). In addition, theft of medical information could also be used to support illegal directed marketing—a problem which might be considered by some more of a nuisance than a threat. We acknowledge, however, that it is difficult fully to anticipate the transformational effect of having all of an individual's medical records tagged with a single identifier. Such records plausibly could become more attractive as targets for illicit marketing and commerce over time.

Because a UPI-enabled NHIN implies that large amounts of healthcare information will be passed back and forth using standard identifiers, the privacy risks of (and opportunities for) large-scale theft or misappropriation of the identifiers themselves appears greater than in the case of a balkanized health care system without a common identification scheme. Although we have argued that UPIs would likely be less attractive than SSNs as a target for theft, UPIs might nevertheless still be attractive to criminals, given a future NHIN with a universal indexing scheme for health information.

Unless Congress or HHS moves to address the outstanding HIPAA concerns around distributed information access under an NHIN model, future misappropriation of UPIs in the context of the NHIN raises the probability of litigation on a variety of issues connected with networked information and patient identification. For example, in a distributed network, who would have ultimate responsibility for safeguarding UPIs? We imagine that the responsibility could attach to the providers who send a UPI out into the network to locate records, and/or to the downstream providers who respond to requests for information, and quite likely to the RHIOs or network administrators who transmit the queries as well. On a different note, given the adoption of a network UPI scheme, it is far from clear who would have responsibility for ensuring that patient information has been indexed appropriately across many institutions and computer systems—but easy to imagine tort claims that might emerge from indexing errors or other mistakes in dealing with UPI-tagged records. Presumably, participants at all levels of the NHIN will share responsibility for appropriately limiting access to UPI-tagged records and for handling patient opt-outs to a UPI-scheme in a way that is fair and that doesn’t nullify the opportunity to opt-out.

No discussion of UPI would be complete without acknowledging the putative clinical and administrative benefits that a UPI-enabled NHIN might offer. One of these benefits comes simply as a by-product of settling on a basic, consistent element for
nationwide systems architecture. We could readily imagine that a federal UPI scheme might facilitate greater interoperability and functionality in other elements of the NHIN, which is a possibility that we describe in more detail elsewhere. On a narrower point, a UPI scheme might very well help to improve the fidelity of medical records matching across local computer systems, with positive impact on the rate of medical errors as a result. Although these sorts of benefits do not relate directly to privacy, they nevertheless reflect a set of competing interests that need to be factored into policy decisions about whether the pursuit of a federal UPI is a good idea.

Algorithmic Model

Next, we contrast the UPI with an algorithmic model for patient identity establishment. Under an algorithmic model for matching records, we assume that a rudimentary NHIN supports distributed searching for patient records through the use of a series of existing identifiers, which would likely include names, addresses, zip codes, birthdates, social security numbers, and other pieces of demographic information (e.g., race, gender, etc.). What kinds of legal and privacy problems does this sort of algorithmic model pose?

First, demographic data, including SSNs, already constitute protected health information under the HIPAA Privacy Rules, which means that covered entities already have responsibilities with regard to the use and transmission of these sorts of identifiers. Although such identifiers can clearly be acquired and disclosed without patient consent under the TPO exemption, it is less clear that "broadcast" transmission of SSNs and other identifiers in order to locate relevant records would necessarily qualify as TPO. One certainly could argue that it should qualify as an exempted activity under the TPO rule, and HHS could change the rules to make it clear that the exception does apply.

But even if the definition of TPO were entirely clear in the Privacy Rules, there would still be questions about who is responsible, and what safeguards are required, in broadcasting demographic identifiers for purposes of algorithmic matching over a distributed health information network. HIPAA requires that covered entities take "reasonable safeguards" to protect demographic and other health information, but what does that actually mean, given a hypothetical NHIN in which every records query involves transmitting an SSN to thousands of other health care providers (or, at a minimum, fifty to one hundred other RHIOs) in order to locate an individual's medical

76 See generally HILLESTAD ET AL., supra note 63.  
77 See infra notes 81-84 and accompanying text.
Note that, by contrast with a UPI scheme, in which a unique medical ID number has no connection to records outside the healthcare system, the aggregation of name, date of birth, and SSN is a far more potent and potentially risky combination. These identifiers are linked to myriad other legal and financial records. SSNs in particular present an obvious target for computer theft and are a commodity for which there exists an already established black market.

In addition, a few states, like Arizona and California, prohibit the use of SSNs as health care identifiers. State laws may also restrict “broadcast” transmissions of identifiers like SSNs. Many states have implemented laws that forbid public postings of SSNs or have enacted requirements that forbid private-sector entities from transmitting SSNs over the Internet other than by secure or encrypted channels.

It is not at all clear how these sorts of statutes and defined terms, taken together with state common law tort remedies, might apply to create pockets of liability in the context of an algorithmic model NHIN. It is easy to imagine, for example, hackers stealing demographic identifiers for large numbers of people from an algorithmically-enabled RHIO. If such information were then used to perpetrate financial fraud on the victims, it seems likely that tort actions might follow, alleging that sensitive information was handled inappropriately by the RHIO, the provider(s) that supplied the demographic information to the RHIO, or both. Given that sophisticated organized crime groups already exist to steal sensitive identifiers and perpetrate financial fraud, what would happen if a criminal enterprise set up a decoy mechanism to steal all identifiers transmitted to a RHIO within the NHIN? Would victims be able to bring tort actions against providers or other network participants for lack of due diligence in security?

Beyond the risks associated with theft of sensitive identifiers like SSNs, algorithmic matching methods would also create another set of legal risks. In particular, it seems likely that participants in interoperable networks may find themselves responsible for the accuracy of the matching of individuals to their records. Possible errors in matching of health records are of two types—linking the wrong person’s health records (false positive errors) and not finding some of a patient’s records (false negative errors).
errors). Either could potentially lead to life-threatening treatment errors, such as causing the wrong medical condition to be treated or the wrong drug to be administered.

To assess the probability of false positive errors when combinations of personal attributes (such as name, date of birth, zip code and partial SSN) are used as search keys, our colleagues conducted an analysis using the Social Security Death Master File, a large national demographic database. Although the rates of errors can be reduced by using more and more personal attributes to make the match, our colleagues' analysis suggests that as databases get larger, as would be the case in an NHIN, some almost-unique attribute, such as the SSN, would almost certainly be required to keep the false positive error rate small.

In evaluating the potential for false negatives, which typically result from medical records that are mislabeled or that omit or modify identifying personal attributes, our colleagues described high rates of these sorts of errors in the use of existing medical record databases as indicated by published empirical studies. For example, consider a person who undergoes a legal name change and who then has electronic medical records under both her old and new names. Those inconsistent records do not themselves reflect any error in data entry or processing, but they nevertheless can present a problem for algorithmic matching, and a greater likelihood for false negative errors and failure to retrieve pertinent medical records. The data used for algorithmic matching changes over time (names, addresses, even gender or date of birth may be revised), which makes the error rate increase over time, and creates a need for a process to continually renew and validate the demographic data stored for identification purposes, which exacerbates the matching problems. While noting that false negative errors are not caused by algorithmic matching, and that such matching is actually designed to reduce false negative errors, our colleagues also conclude that driving such error to zero would require the adoption of a UPI.

In sum, although algorithms could be "tuned" to identify a "region of ambiguity" that could be resolved by humans, some rate of matching error seems inevitable. And if imperfect algorithmic matching gives rise to harm to patients, as when a physician receiving misidentified records administers a lethal medication or combination of medications as a result, then victims and their families will eventually

81 See Hillestad et al., supra note 63.
82 See Hillestad et al., supra note 63.
83 See Hillestad et al., supra note 63.
84 See Hillestad et al., supra note 63.
85 See Hillestad et al., supra note 63.
litigate, and someone will likely be found responsible. Potentially, such mismatches could also result in product liability lawsuits against the vendors who sold the record-matching software, and/or malpractice suits against providers who either relied upon, or supplied, the mismatched medical records. While false matches could also occur in a UPI-enabled NHIN scheme, such mismatches appear far more likely given an architecture based on algorithmic matching (and absent the use of SSNs).

Finally, and by extension, the algorithmic model for patient identification does not resolve any of the gaps in HIPAA coverage with regard to non-covered entities, or with regard to covered entities participating in interoperable health care networks. One result is to create ambiguity about the liability implications of participating in a network that employs algorithmic matching for identification of records. What obligations, if any, does each participant have for the conduct of algorithmic identification methods by other participants? Again, at both the level of the RHIOs and of individual providers, there is presumably some degree of responsibility on the part of anyone who transmits sensitive identifiers and for how those identifiers are handled and safeguarded once they reach downstream participants in the network. The due diligence requirements connected with this sort of network participation, and particularly with the “broadcast” of algorithmic identifiers to large numbers of recipients, remain undetermined. The answer to these sorts of legal questions eventually may be clarified through revised rules under HIPAA, but some of the civil liability parameters ultimately may await determination under state tort laws. An important corollary of this kind of ambiguity is to create a disincentive for participation by provider institutions in a national network. In turn, this again would lead us to expect the development of an NHIN to be even "patchier," slower, and more incremental than it otherwise would be.

**Summary on UPI vs. Algorithmic Matching**

From the foregoing analysis, we can draw several conclusions. First, under current federal and state privacy rules, the NHIN is likely to generate legal problems regardless of whether the national network employs UPI or algorithmic matching to identify patient records. Second, UPI probably offers some marginal benefit in improving the fidelity of record matching, which could likely result in clinical improvements in patient safety, and in reduced tort liability risks for malpractice as a result. It also appears plausible that UPI might facilitate the development of a more fluid, national system for exchanging health information, which could indirectly have a negative impact on privacy interests. On the other hand, some of the privacy concerns attached to UPI could be addressed directly through other aspects of computer systems architecture, including encryption, strict access controls, and audit trail mechanisms.
Notably, UPI might actually help to improve privacy in the NHIN by limiting the transmission of other, more sensitive identifiers, including names, addresses, SSNs, and demographic information. By contrast, an NHIN based on algorithmic matching could involve massive transmission of existing identifiers (including SSNs), simply for the purpose of locating records in a distributed network. Arguably, that kind of transmission of conventional identifiers might pose a bigger risk to individual privacy interests, particularly if we assume that theft of sensitive identifiers to perpetrate financial fraud presents a greater risk to more people than does the misappropriation of medical records (say, to perpetrate genetic discrimination by insurance companies or employers).

Part IV. Options for Protecting Privacy Under Either Model of Identity Establishment

As illustrated in the discussion above, UPI and algorithmic matching both raise privacy and security concerns in the context of an NHIN. Either method of patient identity establishment would still require changes in federal law to ensure adequate privacy protection. Many corresponding reforms in privacy policy have already been proposed and analyzed by a wide variety of governmental and non-governmental organizations. Most of the proposed reforms would require action either by the Administration (e.g., modifying the HIPAA Privacy Rules) or by Congress (e.g., passing additional legislation to clarify the rules for acquisition and use of health information in an interoperable world). We review a series of proposed reforms below.

Modifying HIPAA to Protect Privacy Under the NHIN

Starting first with HIPAA, a number of specific changes have been suggested, the most important of which include:

- Expanding the definition of "covered entities" in the Privacy Rules to include RHIOs, the NHIN, and all other major generators and holders of health information, including all organizations involved in collecting, processing, storing, transmitting and using health care information, as well as (specifically) employers and life insurers.

---

86 See Dep't of Health & Human Serv., 45 C.F.R. § 160.102(a)(1)-(3) (2002); see also supra notes 21-22 and accompanying text.
87 See, e.g., Terry, supra note 23, at 164-165; Sonia W. Nath, Note, Relief for the E-patient? Legislative and Judicial Remedies to Fill HIPAA's Privacy Gaps, 74 GEO. WASH. L. REV. 529, 537 (2006); Janlori Goldman & Zoe Hudson, Perspective: Virtually Exposed: Privacy and E-Health: Privacy Concerns Are
financial institutions, commercial data providers, application service providers, and schools; 89

- Expanding the provisions of the Privacy Rules to regulate directly the actions of Business Associates; 90 or, in the alternative,

- Amending the Privacy Rules to increase the responsibility of covered entities to control the privacy and security practices of their Business Associates; 91

- Modifying the TPO exception/“minimum necessary rule” to limit the dissemination of patient treatment data to those providers directly involved in the patient’s current treatment (their “circle of care”). 92

---

89 NCVHS, supra note 33. On June 21, 2007, NCVHS sent another letter to Secretary Leavitt calling for “quick action” to expand the scope of entities under the rule, based on three additional hearings held by NCVHS to get more information about how entities that are not currently covered by the Privacy Rules handle health information. Id. The letter suggests that “time is of the essence” and that HHS and Congress should move “expeditiously.” See Letter from National Committee on Vital and Health Statistics to Secretary of Health and Human Services, Update to Privacy Laws and Regulations Required to Accommodate NHIN Data Sharing Practices (June 21, 2007), available at http://www.ncvhs.hhs.gov/070621lt2.pdf. On the other hand, some stakeholders are concerned about the implications of such regulatory expansions because of some of the specific Privacy Rule requirements. Id. For example, covered entities are required under the Privacy Rules not only to protect personal health information, but to make such information accessible to patients upon their request and to allow patients to amend their health records. Id. Questions arise as to whether such a role would be appropriate for data vendors (as opposed to medical institutions and health professionals). If all generators and holders of health information are to be regulated by the Privacy Rules, it may mean that the Rules would need to be amended as to specific roles and responsibilities of different types of organizations. Id.
90 NCVHS, supra note 33; McLaughlin, supra note 36, at 43-44.
91 See NCVHS, supra note 33. This recommendation may also pose practical problems for some Business Associates. See id. For example, IT and other vendors are likely to have Business Associate agreements with a wide variety of health care institutions simultaneously, and each of those customers will likely have their own specific policies and procedures – which may conflict with one another. See id. Having a host of customers simultaneously directing the activities of a vendor would likely be unmanageable. See id.
92 See SUBCOMMITTEE ON PRIVACY AND CONFIDENTIALITY, supra note 22, at 10; see also McLaughlin, supra note 36, at 45-46.
All of these proposals involve expanding the reach of the current Privacy Rules, recognizing that they neglect adequately to govern the key players who may have access to protected health information in a national network. Among these policy proposals, the first and second more directly address the basic problem of inadequate regulatory protection for privacy, given the likelihood of an increasing number of participants to the NHIN who are not currently regarded as "covered entities" under HIPAA. The fourth proposal, (i.e., revising the TPO exception) appears to be very limited as a reform and insufficient to protect privacy interests, given that broadcasting of sensitive identifiers over regional and national networks will itself present significant risks to privacy, apart from any disclosures of treatment data.

On another point, some commentators have asserted that enforcement of the current Privacy Rules has essentially failed, and thereby created public doubt about the government's intention to enforce the law. Consequently, some have suggested re-evaluating current policy on the enforcement of the Privacy Rules, or in the alternative, amending the HIPAA statute to create a private right of action so that individuals will have a remedy under federal law for violations of their privacy.\textsuperscript{93} Enforcement issues are somewhat removed from broader questions about appropriate privacy standards for the NHIN, but we would observe that creating new civil claims for privacy violations would likely impede the development of a national network, and therefore seems inconsistent with the vision for an NHIN that many policymakers have advocated. Better government enforcement of the Privacy Rules (together with targeted revision of the rules) seems more consistent with establishing a balance between developing the NHIN, on one hand, and protecting personal health information, on the other.

Finally, in response to the confusion about partial preemption and the state conflict-of-laws problem, some have suggested amending HIPAA to provide full preemption,\textsuperscript{94} or in the alternative, working toward a harmonization of state laws by identifying those states with the most restrictive privacy laws and "nudging" others toward adopting those standards.\textsuperscript{95} Either of these reforms would facilitate development of an NHIN, by establishing a single, consistent regulatory standard on

\textsuperscript{93} Nath, supra note 87, at 545-46; Goldman & Hudson, supra note 87, at 145 (regarding the internet).
\textsuperscript{94} ONC, supra note 68, at 22. Other respondents recommended either repealing HIPAA or retaining as is. Id.
\textsuperscript{95} ONC, supra note 68, at 6-7, 22. It is also at least theoretically possible to develop software that could determine where health information is being sent and that would protect or release it in accordance with appropriate state laws. Id. at 14, 18, 20. Whether this would actually be practical for use at either the RHIO or NHIN level is unknown. Id. at 57.
health information privacy. We are dubious, however, about the prospects for achieving either of them. While a fully pre-emptive federal health privacy statute would be easy to write, it would be difficult to pass, if prior experience with HIPAA and the Privacy Rules is any indication. Federal pre-emption continues to be controversial, especially among privacy advocates who have the ear of Congress. In the alternative, passing a uniform model privacy code through the states, which already has been tried once, has proven exceedingly difficult to accomplish. What remains, in the alternative, is the shepherding of state legislatures toward the creation of a single national standard, which at best will be time consuming and politically difficult as well. 96

Legislating Against the Misuse of Personal Health Information

Beyond proposing changes to the basic structure of privacy regulations under HIPAA, advocates have also pointed to a number of ways that Congress could address concerns that health information transmitted via interoperable networks might be misappropriated or misused. Related policy proposals include criminalizing unauthorized access to medical information; 97 requiring organizations that traffic in health care information to notify patients of breaches of security; 98 prohibiting the misuse of patient care information; 99 prohibiting secondary uses and/or commercial

96 See NCVHS, supra note 33. The movement toward a pseudo-national standard for privacy is not necessarily supported by all factions in the debate over privacy protections. Id. For example, the NCVHS, in its recommendations to HHS, allowed that “a single national standard would facilitate compliance, but the price of uniformity would be a loss in flexibility and the ability of the states to implement policies that reflect local conditions and values.” Id. While “look[ing] forward to the results of [the National Governor’s Association’s study on variability in state privacy law],” NCVHS nevertheless recommended that HHS “explore ways to preserve some degree of variation without losing technical interoperability and essential protections for privacy and confidentiality.” Id.


98 This requirement would be similar to California’s consumer protection statute which requires financial institutions to notify their clients of breaches in security that have put their identifiers at risk. See Cal. Dep’t of Consumer Affairs, Office of Privacy Protection, Recommended Practices on Notice of Security Breach Involving Personal Information, Feb. 2007, at 7 (appending CAL. CIV. CODE § 1789.29 (West 2008) which applies to government agencies and §1789.82 and §1789.84 which apply to any person or business doing business in California); Dixon, supra note 97, at 15-16. The World Privacy Forum has recommended that “a clear and effective pathway of recourse needs to be developed for victims of medical identity theft that is at least equal to protections that victims of financial identity theft have.” Id. at 15.

99 Appavu, supra note 66, at 29.
aggregation of patient-specific information;\textsuperscript{100} prohibiting employer or insurer access to patient-specific genetic information;\textsuperscript{101} and prohibiting discrimination on the basis of medical information.\textsuperscript{102}

It goes beyond the scope of this paper to address the merits and drawbacks of these specific proposals. But collectively, we observe that these kinds of proposals shift the focus somewhat from protecting medical information directly, to controlling how medical information might be exploited in the context of a future NHIN. Apart from stronger legal privacy protections for health information itself, it also makes sense that as the emerging NHIN transforms the delivery of healthcare, and results in a more fluid exchange of sensitive information, stronger and more specific controls limiting appropriate uses may become needed.

\textbf{Enacting Federal Rules to Govern the NHIN}

In addition to other proposed legislative and regulatory changes, the NCVHS recognized that HHS will need to develop specific regulations to govern the operation of the NHIN, and that these rules will need to be "harmonized" with existing federal law. To that end, the NCVHS advocated the following:

- Developing regulations to govern the NHIN using an "open, transparent, and public process" involving a wide array of stakeholders;\textsuperscript{103}

- Working toward harmonization with the existing HIPAA Privacy Rules, as well as other relevant federal law – specifically the existing federal

\textsuperscript{100} Terry, \textit{supra} note 23, at 162-64.

\textsuperscript{101} In April of this year, the U.S. House of Representatives passed the Genetic Information Nondiscrimination Act which would amend the Employee Retirement Income Security Act of 1974 (ERISA), the Public Health Service Act (PHSI), the Internal Revenue Code of 1986 and title XVIII of the Social Security Act relating to medigap to prohibit discrimination on the basis of genetic information or services by group health plans, health insurance issuers and employers. See H.R. 493, 110\textsuperscript{th} Cong. (1\textsuperscript{st} Sess. 2007), \textit{available at} http://www.govtrack.us/data/us/bills.text/110/h/h493.pdf. The bill has been placed on the legislative calendar in the Senate. \textit{Id.} While some have suggested that these fears are exaggerated, Nath cites Congressional testimony by Janlori Goldman of the Health Privacy Project at Georgetown University reporting that a survey found that thirty-five percent of Fortune 500 companies use personal medical records in making hiring and promotion decisions. Nath, \textit{supra} note 87, at 530.

\textsuperscript{102} Appavu, \textit{supra} note 66, at 29; Netter, \textit{supra} note 65, at 179; NCVHS, \textit{supra} note 33, at 11.

\textsuperscript{103} NCVHS, \textit{supra} note 33, at 10.
rules regulating disclosure of substance abuse treatment records;\textsuperscript{104} and

\begin{itemize}
  \item Developing a set of “strong enforcement procedures” – including appropriate penalties for “egregious violations” of privacy and security rules – designed to produce good compliance without imposing cost.\textsuperscript{105}
\end{itemize}

In practice, it is not clear what additional regulations HHS might eventually need to develop to govern the operation of the NHIN. Basic, consistent data standards seem like a threshold area where regulatory involvement might be needed, and where NCVHS has already done significant development work. Of course, the UPI issue is itself partly a question of instituting a consistent data standard in tagging records with identifiers. Given that it is the prospect of the NHIN, rather than UPI per se, that presents the major new risks to health information privacy, we could imagine a variety of other technical regulatory standards that could become politically controversial in the future, as these offer bottlenecks that might slow or derail the NHIN from going forward.

**Restricting the UPI to Health Care**

In the event that Congress and the Administration change course and pursue the development of a federal UPI scheme (as originally intended under HIPAA), some commentators have suggested that one way to protect privacy would be through legislation, along with strict enforcement, to limit the use of UPIs to health care, and to prevent their use as identifiers for other purposes.\textsuperscript{106} This is an obvious step to prevent the UPI from taking on additional administrative functions in government and the private sector: an otherwise foreseeable possibility that would exacerbate privacy risks by making UPIs both more accessible, and more attractive, as a target for criminals.

Although restricting the use of a federal UPI to healthcare seems like a reasonable thing to do, we reiterate that there is no single solution to the privacy problems of the NHIN attendant on how the UPI issue is handled. In the absence of

\textsuperscript{104} NCVHS, \textit{supra} note 33, at 10.

\textsuperscript{105} NCVHS, \textit{supra} note 33, at 10.

\textsuperscript{106} Appavu, \textit{supra} note 66, at 29; Netter, \textit{supra} note 65, at 176. It is possible, however, that future Congresses could remove any such restrictions as was done to allow the SSN to be used for purposes beyond its original intended purpose (to track earnings). For a discussion of the history of the SSN, see American Health Information Management Association e-HIM Work Group on Regional Health Information Organizations (RHIOs), \textit{Using the SSN as a Patient Identifier}, 77(3) J. of AHIMA 56A-D (Mar. 2006).
UPI, algorithm-based systems of patient identity establishment will involve massive trafficking in personal information, including the association of name with address, birth date, and (very likely) SSN. As a result, enhanced privacy and security protections will need to be extended, not only to health care data, but to the personal data elements used in the identification process. Even under a UPI-enabled NHIN, because any health care identification system in the U.S. would likely need to use both UPI and algorithmic matching methods at least for some initial period of time, an either/or discussion about the relative difficulty of protecting the integrity of the UPI versus the conventional identifiers used in algorithmic matching may be moot.

Building Privacy Rights Directly Into the Architecture of the NHIN

Beyond the controversy over the UPI, some advocates have focused their attention on other features of an NHIN, expressing concern that as the technical framework of the NHIN is beginning to be defined, little or no attention has been paid to building appropriate privacy safeguards into the systems architecture. These advocates view with skepticism the idea that needed technical safeguards for privacy can be “layered on” after the fact. Perhaps most important among the issues of concern to advocates is patient choice and, in particular, the “granularity” of choice.

The first level of choice has to do with decisions about “opt-in/opt-out.” An opt-in mechanism would require advance permission from an individual to her share information on the NHIN. By contrast, opt-out mechanisms place the burden on the individual to indicate unwillingness to participate in the NHIN. Given that individuals will often opt for the default mechanism, some have argued that an opt-out would result in unwitting consent to participating in the NHIN on the part of large numbers of people. So the threshold question that the NHIN raises is whether patient participation will be required, or whether the NHIN will have a process that allows patients to decide for themselves whether to participate, and how much risk they are willing to bear in order to gain the benefits of the system. Having a full opt-in process would address some privacy concerns connected with the NHIN in that individuals could simply refuse to have their health care providers make their health

107 For example, encryption of the UPI (whether by PKE or symmetric cryptography methods) would add considerable protection for patients, but would also require significant public investment to build it into the NHIN. See HILDESTAD ET AL., supra note 63.
108 For a discussion of these issues in the context of consumer data profiling, see Andrew J. McClurg, A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 NW. U. L. REV. 63 (2003).
109 Netter, supra note 65, at 181-83.
information available via a RHIO or the NHIN. But even though a full opt-in model may be most consistent with principles of patient autonomy, it would also likely be much more burdensome for getting an NHIN off the ground. The practical operational implications of an opt-in might plausibly overwhelm the system and, should large numbers of patients decide not to participate, would undermine the utility of the system, at least for emergency and public health purposes. Whatever policy the NHIN architects might choose, it would minimally be desirable to protect the right of patients to opt-out without penalty (such as denial of insurance or denial of care). One approach for encouraging voluntary consumer participation in the NHIN might be to allow providers or health plans to give incentives to patients to opt-in (for example by offering reduced premiums), rather than attempting to mandate participation in either the NHIN or UPI.

Beyond giving consumers the initial choice of whether to participate, the architecture of the NHIN could help to maximize consumer choice by allowing patients to participate in decisions about who would be able to access their treatment information, and what information could be accessed. For example, some have argued that NHIN policy should guarantee that certain types of private information can be excluded by patients from interoperable systems. Professor Terry, testifying before the NCVHS, has suggested that this could be effectuated in a number of ways, including by allowing patients to “carve out” or restrict very sensitive data (such as psychotherapy notes) from being released from their electronic health record into the NHIN, by having patients determine together with their physicians what information can be pulled via the NHIN, or by setting up additional access controls so that only certain NHIN participants (i.e., treating psychiatrists and emergency room providers in the case of psychiatric medications) can access certain data. Others have suggested that the NHIN could establish policies for a “multi-tiered authorization structure,” with one tier for categories of information (e.g., sensitive reproductive, mental health, infectious disease, medications) and a second tier for categories of users for which different levels

---

110 The NCVHS stated that individuals should have the right to decide whether their medical records would be accessible via the NHIN, but reported that they were unable to agree—even after five public hearings and an 18 month process of deliberation—on whether to endorse an opt-out or opt-in approach. They recommended that ONC monitor the development of different approaches as they occur in states and localities. See NCVHS, supra note 33, at 5.

111 NCVHS, supra note 33, at 5.

112 Netter, supra note 65, at 176. It should be noted, however, that this could also be viewed as a penalty for choosing not to opt-in.

113 Terry, supra note 23, at 181.

114 Terry, supra note 23, at 186-87; see Subcommittee Hearing, supra note 22, at 8-9.
of access could be authorized by the patient. Such control might be designed to be incident or episode-specific as well, given that a single agent may require different levels of access for different functions. The purpose would be to enhance privacy and patient confidence in the system by using a combination of data restrictions and user privileges.

While NCVHS supported "role-based access" technology in their recommendations to the Secretary of HHS, they nevertheless suggested that there was a lack of consensus on whether patients should fully control access to their records at either the provider or NHIN level. For example, NCVHS noted that state law, professional standards, and current practices require that changes to the content of a record be done by amendment rather than removing or deleting information. Without taking a position on the issue, NCVHS reflected on testimony by providers that giving patients the right to limit access to their records "may interfere with the ability of providers to make appropriately informed decisions," resulting in the potential for increased "malpractice liability stemming from errors in health care caused by accessing incomplete or filtered personal health information via the NHIN."

There is some evidence that ONC is responding to this issue. In public statements, Dr. Kolodner stated that the NHIN Prototype Architectures that are being developed under contract with HHS should "give [consumers] the capability to decide how they view, store and control access to their own information. A person could say how that information flows to specific entities or completely block the flow of information." These comments reportedly received a mixed public reaction, with privacy advocates praising the Director of ONC, but with a member of the NCVHS

---

115 ONC, supra note 68, at 24.
116 NCVHS, supra note 33, at 8. NCVHS stated that "contextual access criteria could be developed and integrated into the architecture of EHRs [electronic health records] and the NHIN to permit disclosure of only the information needed by the user" and suggested that HHS should support research and technology as well as feasibility testing of the inclusion of such in the NHIN. Id.
117 NCVHS, supra note 33, at 5.
118 NCVHS, supra note 33, at 5.
questioning whether this kind of policy would make any difference.\(^{121}\) In our view, although it may be possible to set up an NHIN architecture that supports these sorts of exotic access controls, it is far from clear that 300 million Americans (many with limited computer literacy and access) would be able and willing to use a complicated access control scheme of this kind.

Finally, perhaps reflecting an erosion of faith in government's ability to protect private information, still others have suggested that the public's confidence would be enhanced if HHS were to create a governing body or privacy board for the NHIN, whose role it would be to ensure patients' access to their health information, their rights to review and annotate their records, and their rights to review a log of their accessed records to determine what organizations and individuals had obtained their records and for what purposes.\(^{122}\) The NCVHS also recommended that public confidence might be improved if meaningful numbers of health care consumers were appointed to serve on any such governing board, and if in addition HHS strengthened its enforcement measures and established an ongoing program to assess the effectiveness of the privacy and security protections of the NHIN.\(^{123}\)

**Conclusion**

The prospect of a federal UPI has been one of the more controversial elements of the HIPAA regulatory scheme, going back to the original Congressional mandates of 1996. Like the SSN, a UPI would have the potential to link enormous amounts of data across information systems, with the possibility of a mushrooming set of applications (and security risks) not in the contemplation of its original proponents. UPI as Frankenstein's monster is a large part of what privacy advocates are concerned about. And without doubt, there will be new risks associated with more fluid exchanges of sensitive medical records over distributed networks and with the tagging of such records with a unique identifier that might itself become an attractive commodity for theft or misuse.

That being said, most of the controversy attached to UPI has very little to do with a specific technical method for identifying and retrieving electronic records over a network. Instead the controversy has much more to do with the characteristics of an emerging national health information infrastructure, for which existing privacy regulations and legal safeguards are manifestly inadequate. Prohibiting the development

\(^{121}\) *Id.*

\(^{122}\) ONC, *supra* note 68, at 24.

\(^{123}\) NCVHS, *supra* note 33, at 13.
of a UPI actually sidesteps the larger problem—that the federal government is proceeding with the development of a NHIN without first establishing a legal environment that best protects privacy and that balances privacy interests with the advances that interoperability would bring to health care quality and efficiency. We therefore frame our discussion in this paper by starting with a review of the status quo of federal and state privacy protections, and aspects of those protections that appear ambiguous or problematic in light of the developing NHIN. In assessing the relative merits of the two main approaches to patient identity establishment from a legal perspective, we find that both methods raise privacy concerns, but that the UPI is certainly not inferior—and may in fact be superior—from a privacy perspective, especially if public key encryption were also employed in a national network.

In considering the development of the NHIN more broadly, we describe a series of legislative and policy options that, if enacted and/or implemented, could go a long way toward increasing public confidence in the ability of government to ensure the safeguarding of their sensitive health information. Without advocating for specific proposals, we believe that increased public confidence is a necessary foundation for developing a viable NHIN, regardless of the method of patient identity establishment that is ultimately adopted.

In sum, the Administration and Congress should revisit the issue of patient identity establishment, recognizing that there are deeper privacy problems concerning the NHIN that lurk at the periphery of the UPI debate. In all likelihood, a series of modifications to the federal Privacy Rules will be needed to protect the privacy and security of personal health information, given an increasingly fluid, networked environment for processing health information. Efforts to stonewall the UPI may have succeeded to date, but privacy advocates may find they have made a Faustian bargain in supporting algorithmic methods instead of a UPI, especially if the SSN, of necessity, becomes the cornerstone of a working algorithm for patient identity establishment. In our view, it would make more sense to allow the development and testing of a federal UPI to go forward, while also recognizing that some of the basic legal contours under HIPAA and state privacy law will need to change, as NHIN technology and communication practices continue to emerge and evolve.