THE GEORGE WASHINGTON UNIVERSITY MEDICAL CENTER
WASHINGTON DC

THE ROBERT WOOD JOHNSON FOUNDATION

Charting the Legal Environment of Health Information

Sara Rosenbaum, JD
Phyllis C. Borzi, JD, MA
Lee Repasch, MA
Taylor Burke, JD, LLM
John F. Benevelli, JD, MPH (cand.)

The George Washington University
School of Public Health and Health Services
Department of Health Policy

May 2005

I. INTRODUCTION

Over the past several years, increased attention has been focused on the importance of health information to health care quality improvement. The level of focus on health information has increased with the advent of electronic medical records and electronic health information systems designed to facilitate the use of health care data. Although these systems are still in their relative infancy, they hold enormous promise for revolutionizing the availability and use of health information to improve clinical performance, empower employers and consumers to better understand health plan choices and facilitate health claims administration. Their potential has been a catalyst for change in a growing number of communities, with the emergence of private/public partnerships to develop regional health information systems.

At the same time, advances in health information technology reinforce many longstanding legal questions related to the provision, sharing, and disclosure of health information. Furthermore, the very technology that makes this revolution possible in turn raises legal questions of its own. This interaction between innovation and law is a common theme in American health care.[1] As innovation enables significant

[1] Rand Rosenblatt, Sylvia Law and Sara Rosenbaum. 1997. *Law and the American Health Care System* (Foundation Press, NY, NY, 1997); Rand Rosenblatt, Sara Rosenbaum and David M. Frankford. 2001. Law and the American Health Care System (Foundation Press, NY, NY)

improvements in the standard of care, the health care industry inevitably attempts to remove legal barriers that otherwise might impede its rapid adoption and diffusion. In a similar vein, consumers and patients come to expect that the standard of care will rise to the level made possible by innovation, thereby raising new questions of liability when the standard is not met or when other important patient protections (such as privacy) are unnecessarily compromised along the way. In this sense, innovation in health information can be expected to follow the same legal trajectory evident in other advances in health care quality and patient safety. In some cases the legal issues which arise are brand new. In others, they are a reflection of longstanding legal matters that must be revisited in new contexts.

This Policy Brief is part of a project supported by a grant from the Robert Wood Johnson Foundation that is designed to assess the legal environment for health information systems. The project also has received support from the Agency for Health Care Research and Quality (AHRQ), which has enabled us to convene periodic small meetings of legal and information experts in order to more closely examine the legal environment of the rapidly emerging electronic health information industry. (A list of participants from our initial meeting can be found in Appendix B).

This project has several phases. The first phase, reported on in this Policy Brief, offers a broad exploration of the legal environment of health information systems, examining many longstanding issues as well as recent matters that have arisen as a result of the new information technology that enables these systems to share health information among many users. Subsequent phases will report on the legal questions regarding the electronic medical record,[2] evolution of federal and state laws in response to a transformed information environment, as well as on legal tools and approaches being developed in order to aid in the transformation. This report focuses on the identification of legal issues affecting health information systems and potential implications arising from data collection, while the next phase of this project will propose potential solutions to the legal issues discussed herein.

Understanding how the law responds to and shapes change is essential to the process of social change itself. [3] Nowhere is this more in evidence than in the case of an industry that is so essential to individual well-being. Law has a profound impact on health care, since it offers a means of assuring that major advances in care are implemented in a manner consistent with equally important economic and social goals. At the same time, because the field of health law exists at the intersection of the entire legal system and the entire health care system, any particular change can trigger a daunting set of issues and challenges. This certainly is the case where health information is concerned, particularly when longstanding and traditional legal questions linked to patient information are coupled with the new legal questions that arise in the context of information technology. As the evolving health information enterprise transforms the

[2] It is important to emphasize that this report discusses the legal issues and implications as they relate to the emerging use of electronic health information systems. Legal issues specific to the "electronic medical record" are beyond the scope of this paper.

[3] Lawrence M. Friedman. 2002. *Law in America* (Modern Library ed., NY)

health care system from a series of isolated businesses into virtual, large-scale undertakings linking multiple actors (many of whom may be marketplace competitors), industrialization of this magnitude raises many legal questions. Some of the questions raised by this transformation may be new to health information law; others turn out to be enduring issues in health law, but nonetheless must be applied to a dramatically changing health care context. Because the interaction of law and society is so contextual, a "from the ground-up" exploration of the law itself becomes an essential part of the process of change.

Part II examines the transformation of the health information enterprise. Part III considers the key features of modern electronic systems, while Part IV explores the legal implications of this transformation of information within electronic health information systems. The Policy Brief concludes with a practical assessment of this analysis.

II. THE TRANSFORMATION OF THE HEALTH INFORMATION ENTERPRISE

Information is essential to health care. In the highly diverse, market-based, multi-payer system used in the U.S., the potential for an almost endless number of sources of information about patient health care to exist is enormous. Regardless of whether the topic at hand concerns individual patients, the performance in distinct clinical care settings, or the pattern of health care in institutions among and within health plans, or throughout or among geographic regions, the U.S. health care system generates extensive information, much of it un-tethered from other information concerning the same patient, clinical setting, health care institution or health plan.

In recent years much attention has been focused on the potential of timely and complete information to reduce errors, improve health care quality, and reduce racial, ethnic and other health care disparities unrelated to the need for care or the ability to benefit from treatment.[4] This focus underscores the link between the "professional standard of health care" (i.e., the legal standard used in U.S. law to measure the quality of care) and the extent to which health care providers and institutions are engaged in active efforts to secure and apply health information to inform and guide their practice.

The emergence of an electronic information industry vastly expands the potential to generate not merely information, but to put the information to use in health care settings. The uses of information range from measuring the health status of entire patient populations to understanding and selecting appropriate clinical interventions for different individual patients given their health and personal characteristics, their health care needs and preferences, and the particular setting and context of care. In other words, as the potential grows for health information to be incorporated into practice, so do social and legal expectations that health care providers in fact will do so. Despite the fact that a technology may just be emerging, the law views the rapid response to a promising new safety technology as an essential component of the professional standard of care,

[4] Institute of Medicine. 1999. *To Err is Human* (National Academy Press, Washington D.C.); Institute of Medicine. 2002. *Crossing the Quality Chasm* (National Academy Press, Washington D.C.)

particularly when the technology is accessible and available at a relatively reasonable cost. [5]

Despite the advent of an electronic information industry, a recent study by the Commonwealth Fund examining physicians' use of information technology suggests that physicians are only in the early stages of transitioning to electronic health information, with most users focused on use of electronic information in a billing and payment context.[6] Without a forceful presentation of a strong business case for using these systems, health professionals may reject active adoption of information systems, aside from perhaps facilitating insurance coverage determinations. Physicians and other health professionals continue to enter information by hand into paper medical records and cull information as needed – and using elementary techniques – in order to address clinical management needs. Much of this information never leaves individual patient medical records.

In a paper-driven system, health professionals have no ready means for comparing performance and outcomes across their patient populations, nor do they have a means of examining their patients against those cared for by other professionals and health systems. Insurers, employer and publicly sponsored health plans, and corporate suppliers of health care goods and services (such as diagnostic tests, medical equipment and supplies, and pharmaceutical products) may have more sophisticated information systems, and although some effort has been made to create clinical decision point of service support, these systems remain isolated and disconnected from the actual course of patient care, as well as from patient medical record information.

The importance of modernizing health information has been a focus of considerable analysis for a number of years, particularly since the publication of a series of seminal studies by the Institute of Medicine, including *To Err is Human*[7] and *Crossing the Quality Chasm.*[8] The role of electronic information in health care quality improvement has been a focus of extensive analysis by both private foundations[9] and the

---

[5] *The T. J. Hooper*, 60 F.2d 737 (2nd Cir. 1932); *Washington v Washington Hospital Center*, 579 A.2d 177 (D.C. App. 1990).

[6] Commonwealth Fund. 2004. *Information Technologies: When Will They Make it Into Physicians' Black Bags?* http://www.cmwf.org/publications/publications_show.htm?doc_id=251984 (accessed December 12, 2004).

[7] Institute of Medicine, Kohn L., Corrigan J., Donaldson M., *To Err is Human: Building a Safer Health System* (2000). Washington DC, National Academy Press.

[8] Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century* (2001). Washington, DC, National Academy Press.

[9] *See* The Markle Foundation, *Connecting for Health; Achieving Electronic Connectivity in Healthcare, A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders* (July 2004) available at www.connectingforhealth.org/resources/white_roadmap_072004.pdf.; J. Marc Overhage, Regenstrief Institute for Health Care, *Design and Implementation of the Indianapolis Network for Patient Care and Research*, 83 (No.1) Bull. Med. Libr. Ass'n 213 (Jan. 1995) available at www.pubmedcentral.nih.gov/picrender.fcgi?artid=225997&action=stream&blobtype=pdf. *See also* Markle Foundation*, Financial, Legal and Organizational Approaches To Achieving Electronic Connectivity In Healthcare* (October 2004) available at www.markle.org/downloadable_assets/flo_sustain_healtcare_rpt.pdf; David Brailer, *Moving Toward Electronic Health Information Exchange, Interim Report on the Santa Barbara County Data Exchange*

federal government. In its most recent study, *The Decade of Information Technology: Delivering Consumer-Centric and Information Rich Health Care,*[10] the United States Department of Health and Human Services called for the widespread creation of electronic health information as well as development of the capacity to transmit such information across many different groups of potential users in both the public and private sectors.

The cumulative effect of this body of work has been a rapidly increasing interest in the modernization of health information and the growth of an electronic information industry capable of enabling the use of health information to improve quality and better manage costs. Notwithstanding the reluctance and slowness with which physicians have embraced the use of electronic health information, the climate and culture of the health information world is changing.

Although sparked initially by private industry, a major driver of this change has been the federal government itself. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities, including health plans and most health care providers, to comply with electronic data interchange standards (EDI) as well as transmit health data electronically for claims payment and eligibility purposes.[11] More recently, the Medicare Prescription Drug, Improvement and Modernization Act (commonly known as the Medicare Modernization Act or MMA) authorizes the Centers for Medicare and Medicaid Services (CMS) to develop and administer electronic data systems to facilitate provider quality measurement activities in connection with Medicare program administration.[12] The law also directs the Secretary to condition hospital payment on the electronic reporting of quality indicators and to tie the level of payment to quality measurement (i.e., "pay for performance").[13]

One of the most significant new drivers of modern health information systems is the incorporation of health information measurement and reporting capabilities into national industry accreditation standards. For instance, the National Committee on Quality Assurance (NCQA), an industry-based quality measurement and accreditation organization, measures the performance of health care organizations, health care institutions, and health professionals against quality metrics. Another example of quality

---

(July 2003) available at www.chcf.org/documents/ihealth/SBCCDEInterimReport.pdf; Catherine Frey, *Wisconsin Patient Safety Institute: Striving for Positive Outcomes*, 100 (No. 6) Wis. Med. J. 14 (2001) available at http://www.wisconsinmedicalsociety.org/uploads/wmj/100-6-FA-Frey.pdf.

[10] Accessed November 30, 2004 at http://www.hhs.gov/healthit/frameworkchapters.html.

[11] Sections 261-262 of HIPAA (Public Law 104-191(1996)) provided for the adoption of national standards for certain financial and administrative health care data. The Secretary of HHS was required to adopt uniform national data elements and code sets to support the electronic exchange of information by Medicare, Medicaid and all private health care plans and providers. All governmental and private payers (including both self-insured and insured group health plans, health insurance issuers, FEHBP, CHAMPUS, etc.) are required to conform to these national standards. Transactions subject to these standards would include claims, enrollment and disenrollment, eligibility, payments and remittances, premiums, and claims status.

[12] The Medicare Prescription Drug, Improvement and Modernization Act (MMA), Public Law 108-173 (2003).

[13] *Id.* at Section 501(b).

measurement from a large purchaser perspective is the Leapfrog Group for Patient Safety, which has developed guidelines for hospital care and which is now focused on physician care.[14] Even more significantly perhaps from a legal standpoint, the Joint Commission on the Accreditation of Healthcare Organizations (JCAHO) has now proposed to make the collection of data on patient race, ethnicity, and primary language spoken a basic aspect of organizational accreditation for managed care organizations and integrated systems, and in both ambulatory and institutional settings.[15]

By themselves, industry accreditation standards do not have the force and effect of law, but standards such as practice guidelines prepared by the National Committee on Quality Assurance (NCQA), The National Quality Forum, The Leapfrog Group, and other measurement systems, as well as formal accreditation standards themselves, signal the increasing importance of quality benchmarking in practice and the need for effective information to support practice improvements. As government payers, private insurers, and industry-self monitoring enterprises all come to embrace information competency, these expectations become part of the standard of professional performance that patients come to expect.

III. EMERGING DISTINCTIONS BETWEEN ELECTRONIC HEALTH INFORMATION SYSTEMS

Because law is intensely contextual and fact-driven, it is important, before turning to the legal discussion, to describe the emerging electronic health information systems. This technology is obviously still in its infancy and can be expected to change dramatically in the coming years, understanding their structure and capabilities as a backdrop to any legal analysis is immensely valuable.

The systems that exist today show important differences, and these distinctions in architecture, connectivity, and operational capabilities have implications for the range of legal issues raised. All of the systems are similar in that they attempt to link together multiple health care actors, either within or between health care enterprises, in order to expand the pool of data about patients and services. For example, a health insurer may link to its provider network in order to administer its various health plans. But these information systems can differ in how many sources of data are linked, how many different health care enterprises in turn link themselves together (e.g., multiple insurers or payers), and the extent to which the information systems allow for the merger, aggregation, and de-identification of data so that aggregated data results and can be used for purposes beyond the simple act of claims review and payment.

Through consultation with experts in the field, we were able to identify several important distinct characteristics, each of which is briefly described below. While each system has unique properties which may give rise to specific legal questions, they all

[14] http://www.leapfroggroup.org/ (accessed January 25, 2005).
[15] JCAHO. 2004. *Joint Commission Seeks Input on Proposed MCO IDS Standard to Collect Information on Race, Ethnicity, and Primary Language* (Washington D.C.) http://www.jcaho.org/news+room/news+release+archives/nr_12_2.htm (Accessed, January 23, 2005).

share two fundamental qualities. The first is the potential to produce unprecedented amounts of information about the total health care process experienced by patients, across the domains of health care. The second is the ability to transfer massive amounts of information across and throughout the health care market, as well as to government agencies. We have summarized below some of the most important distinctions among existing health data systems. These distinctions are not mutually exclusive and a single system may embody several of these features.

a. Decentralized and Centralized Systems

A focus of discussion at our first meeting of experts was whether the electronic health information system in question was "decentralized" or "centralized." (Appendix A provides a detailed analysis of emerging decentralized and centralized electronic health information systems currently in use). In a decentralized system, the data generated from a health care provider's query are not stored in a permanent record or central database, but exist "virtually" and solely for the use of that specific health care provider making the request. In this type of indexing system, each system user possesses and houses its own data which are then indexed and accessible to other users that query the system, but the requested data are transitory in nature, existing within the entire system only for the moment in time when the query is made, and in a manner similar to an oral exchange of information between two individuals in an unrecorded conversation. Once the provider exits the screen, the information retreats back to its original source and out of the overall system until queried again through a separate request. There is an audit trail of who made the inquiry. This type of architecture allows a health care provider to confirm a patient's enrollment in a health plan as well as whether a particular procedure is covered. It also avoids computer hacking. But the information cannot be aggregated, and thus this limited function makes it inadequate for quality improvement and research.

In a centralized system, the data are standardized and stored in a central database, thus enabling research and quality improvement activities. Queries from providers to payers and vice versa are essentially captured and stored for further use; thus, for example, a centralized system can be used for health care quality improvement efforts and can produce real-time feedback reports and comparison data on population-wide performance benchmarks. The information is deposited into a central data warehouse, where it may be used for analysis.

b. Uses of Data: Administrative and Clinical Data Exchange Systems

A key distinction in considering legal issues arising from health information has to do with the purposes for which data are used. An *administrative data exchange system* seeks to reduce health care administration costs by enabling health care providers and insurance companies to exchange the information necessary to process and pay claims. This patient-specific administrative data can confirm a patient's insurance status for a particular service, the terms of coverage (e.g., coinsurance, co-payments, and coverage limits) and can capture other information such as patient address.

A *clinical data exchange system* offers patient-specific information at the point of care. This type of system shares patient demographics, medical records, medical transcription, eligibility and referral information, laboratory, radiology, and pharmacy data, as well as information concerning eligibility verification, online referrals or authorizations, and quality performance reporting. The exchange of clinical data generally occurs on an institution–to-consumer or institution-to-physician basis. This clinical data, as opposed to administrative data, serves as the critical resource for population-based research needed to address quality of care and disparities issues.

CMS also offers an electronic data exchange system for various entities participating in the Medicare program, which it uses to monitor the quality of care offered to Medicare beneficiaries. Through Quality Improvement Organizations (QIO), CMS collects data on specific illnesses and treatments in order to provide feedback to the participating hospitals regarding quality.

c. Access to the System

The method by which access to the health information system is determined constitutes another distinction among systems. One method to regulate access is by contracts that link health care payers and providers, all of whom agree to enter into legally binding agreements to be part of any particular health information exchange system. These contracts detail, among other things, who can (and cannot) use the system and for what purposes, what entity actually owns the system itself (the participants may or may not have an ownership interest), the software utilized to make the system run, and applicable security standards. Depending on the specific system, participants may include health insurers, physician groups, individual physicians, state and federal governments, employers, hospitals, local and state health departments, pharmacies, and public school clinics. Specific systems may allow any dues-paying entity to become a participant, while others restrict access only to those new participants that are approved by existing participants.

Access to a health information system can also arise from participation in an enterprise overseen by a single entity. In this scenario, the entity (for instance, a private foundation) finances the creation of a data exchange system and invites individual health care organizations to participate in the system, termed a "care data alliance."[16] Each common undertaking then agrees on unique data sharing goals based on individual member interests. These systems may or may not allow patient access to the data and may or may not relate to claims payment and insurance administration.

Medicare-participating hospitals can gain access to a data exchange system through QIOs for the purpose of quality improvement efforts. CMS contracts with QIOs to monitor and improve the care delivered to Medicare beneficiaries. Hospitals that choose to participate transfer certain health information to the QIO which then deposits the data into a central data warehouse. This data may be accessed by participating

[16] The term "care data alliance" is specific to the Santa Barbara County Care Data Exchange system and denotes specific groupings of entities engaged in electronic health information data exchange.

providers in the form of real time feedback reports, comparison data on statewide performance benchmarks, as well as clinical and analytical tools.

Table I presents a summary of some of the critical distinctions among electronic health information systems and provides examples of each.

Table 1. Distinctions Among Electronic Health Information Systems[17]

Distinguishing Feature	Example
Decentralized versus Centralized	Decentralized: New England Health EDI Network (NEHEN) Centralized: Medicare Health Care Quality Improvement Program (MHCQIP)
Uses	Administrative: NEHEN Clinical: Santa Barbara County Care Data Exchange (SBCCDE) Quality of Care: MHCQIP
Access to the System	Contract: NEHEN Care Data Alliance: SBCCDE Medicare Participating: MHCQIP

Depending on the system's innate structure and uses, as well as considerations related to access to the system, specific legal questions may arise. At the same time, certain common categories of questions apply across all systems. Examples of these cross-cutting questions are whether the system is structured to comply with all applicable state and federal laws, questions of ownership have been identified and resolved, information use procedures conform to applicable laws, applicable privacy safeguards are in place, and special procedures for information access under specific circumstances have been established.

IV. ASSESSING THE LEGAL ENVIRONMENT OF HEALTH INFORMATION

In General

For well over a hundred years, the production of written and personal health information has raised legal questions, and this longstanding link between health information and the law has been particularly visible in a privacy context.[18] While the law has been concerned with health information privacy for well over a century,[19] the

[17] See Appendix A for detailed descriptions of the electronic health information systems noted in this chart.
[18] *See De May v. Roberts*, 9 N.W. 146 (Mich. 1881) (holding physician liable for allowing a non-medical associate to attend physician-patient interview in non-emergent setting); Compare *Simonsen v. Swenson*, 177 N.W. 831 (Neb. 1920) (concluding physician is privileged to reveal patient's highly contagious and infectious disease to reasonably prevent its spread).
[19] For an extremely helpful article tracing the history of privacy law in numerous contexts, *see* Daniel Solove, "The Origins and Growth of Information Privacy Law", 748 PLI/PAT 29 (June 2003). Professor Solove, who writes on the extensive body of federal and state privacy law, traces its roots to Americans' focus on individual autonomy and privacy beginning in Colonial times, a fact which underscores the close relationship between society and law. Indeed, Professor Solove traces federal lawmakers' concern about the

arrival of electronic information technology has triggered even more intense debates, since the potential damage flowing from a failure of privacy safeguards can be far greater, simply because of the sheer volume and extent of information.[20] What a generation ago may have been an unsecured dumpster filled with abandoned patient psychiatric records from a single practice may now be an unsecured electronic database holding psychiatric care data on tens of thousands of individual patients gleaned from hundreds of practices. Although the general perception that the electronic transmission of data results in a more accurate, efficient, and secure system may not necessarily hold true in every case, it is also evident that electronic systems hold the promise of more reliable, and safer data, particularly with their capabilities in the areas of encryption protection and security software to protect privacy. Moreover, the HIPAA privacy, security and electronic data transmission regulations mandate standards for electronic improvements in electronic health data safety that in many respects, are more likely to provide greater protection for patients than those applicable to a paper-based system.

In the "pre-electronic" world of health information, breaches of privacy required overt physical acts of some sort. A health provider might impermissibly divulge information either orally or in writing, carelessly throw out medical records in unsecured trash receptacles, or leave files lying around. If the government wanted to seize private health information, authorities had to make a physical demand for it, thereby placing individuals or information custodians on notice that the information was being sought. But electronic information increases both the ramifications that can flow from a privacy breach (i.e., the number of persons injured through a single unauthorized disclosure), as well as the potential for government officials (and others) to obtain access to information without individual knowledge or consent (i.e., by culling the data from health data warehouses or central repositories). As the diagrams set forth in Appendix A suggest, the very existence of data warehouses could be perceived as creating unprecedented opportunities for privacy breaches.

The long-standing law of health information does not, however, stop at matters of information privacy. From an examination of numerous legal texts and treatises which address the issue of health information from various vantage points,[21] it is possible to

---

improper use of personal health information back to the first appearance of health questions in the 1890 census, which was followed by federal legislation at the turn of the 20th century aimed at proscribing improper use of data. By the early 20th century, courts were also modifying the common law to recognize the tort of invasion of privacy, with the common law tort of breach of confidentiality emerging in 1920. *Id*. at 45-50.

[20] *See* Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 Texas L. Rev. 1 (1997); Paul T. Kostyack, "The Emergence of the Health Care Information Trust," 12 *Health Matrix* 393 (Summer 2002); Daniel Solove, *Access and Aggregation, Public Records, Privacy, and the Constitution,* 86 Minn. L. Rev. 1137, 1140 (2002); Daniel Solove, "The Origins and Growth of Information Privacy Law," 748 PLI/PAT 29 (June 2003).

[21] *See, e.g.*, Barry Furrow et. al, *Health Law* (West Publishing, 5th ed.) 2001; Rand Rosenblatt, Sylvia Law, and Sara Rosenbaum, *Law and the American Health Care System* (Foundation Press, NY, NY) 1997; Rand Rosenblatt, Sara Rosenbaum, and David Frankford, *Law and the American Health Care System,* (Foundation Press, NY, NY 2001-02 Supplement); Kenneth R. Wing, *The Law and the Public's Health* (Health Administration Press, 5th ed.) 1999; Clark C. Havighurst, James F. Blumstein, Troyen A. Brennan,

group these longstanding legal principles into eight major categories related to the overarching themes of privacy and health care accountability. Each category raises distinct legal questions that are discussed in sections IV(A) and (B) below. The categories are as follows:

1. Questions regarding the ownership of health information (e.g., whether a patient owns his or her own medical records and the circumstances under which access to personal health information must be furnished);

2. Questions regarding the appropriate use and disclosure of personal health information to third parties (e.g., releasing prescription drug practices or psychiatric treatment notes in contexts other than treatment, payment, or health care operations);

3. Questions regarding the power of government to compel the collection and disclosure of personal health information as part of public health oversight or law enforcement (e.g., state law reporting mandates regarding sexually transmitted diseases, federal requirements related to the provision of treatment data for purposes of quality measurement or fraud investigations);

4. Questions regarding the power of health insurers to compel the collection and disclosure of data (e.g., patient treatment notes) as a condition of payment or for purposes of performance measurement or evaluation of the extent to which a health care provider is in compliance with governmental requirements;

5. Questions regarding data access as a result of privately-mounted civil litigation claims based on one or more theories of liability (e.g., demands for data as part of legal discovery requests, in order to aid an injured party in fashioning and proving a civil claim of medical negligence, breach of a legal duty, or violation of law, such as federal or state civil rights laws);

6. Questions regarding data access by government law enforcement agencies to support civil or criminal investigations (e.g. demands for medical records related to abortions performed late in pregnancy in order to investigate allegations of unlawful abortion procedures);[22]

7. Questions regarding the use and ownership of personal health information for biomedical, behavioral, and health services research as well as the corollary fiduciary duties of disclosure and notice of conflicts of interest to the patient when such health information yields important research potential[23] (e.g., the

---

Health Care Law and Policy (Foundation Press, NY, NY) 1998; Lawrence O. Gostin, *Public Health Law Power, Duty and Restraint* (University of California Press) 2000.

[22] *See National Abortion Federation v. Ashcroft*, 2004 WL 292079 (N.D. Ill. Feb. 6 2004) *affirmed by Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923 (7th Cir. 2004); *Planned Parenthood Federation of America, Inc. v. Ashcroft*, 2004 WL 432222 (N.D. Cal. March 5, 2004).

[23] *See Moore v. Regents of the Univ. of California*, 792 P.2d 479 (Cal. 1990).

circumstances under which researchers can gain access to personal health information data, when data must be de-identified, and restrictions on publication of information regarding research subjects); and

8. Questions regarding the legality of race and ethnicity data collection by the government or private industry for quality improvement purposes.

Furthermore, the emergence of an electronic health information industry can be thought of as having added a ninth category of law related to health information, namely, the "law of industrial design and corporate transactions." That is, as innovation leads to the growth of an actual electronic health information industry, numerous questions arise regarding the nature and design of the information system itself and the personal property versus intellectual property rights that arise from the very creation of the system. Many of these questions can arise in any type of corporate creation enterprise, but as noted previously, these questions may raise special issues where the enterprise has health information as its final product.

For example, the application of laws ostensibly prohibiting information sharing as a form of anti-competitive conduct may lead to one type of result where the information concerns a relatively fungible consumer product such as television sets. Where the information sharing enterprise concerns improved health care as the product, the result may be very different because of countervailing considerations specific to the health information industry. That is, the goal of improved health care quality may be so important to society that certain forms of information sharing among competitors will be tolerated – and even encouraged.

Similarly, corporate informational activities which may look suspect in other contexts become acceptable, and even desirable, in the context of health information. For example, questions designed to identify the race of individuals could be thought of as a form of "racial profiling" in violation of federal and state civil rights laws prohibiting discrimination on the basis of race or national origin. In that context, racial and ethnic data are being collected for an entirely impermissible use (i.e., to identify suspected legal violators or individuals who may be subject to service exclusion or discrimination). In the context of health care quality, however, a health care corporation may be seeking this same data in order to compare the experiences of individual patients and ensure care of equal quality. For instance, the Aetna Health Insurance Company has developed a data system for precisely this purpose.[24] In this context, the collection and use of the data would make the enterprise not only lawful but desirable.[25]

---

[24] The Robert Wood Johnson Foundation and America's Health Insurance Plans, *Health Insurance Plans Address Disparities in Care: Challenges and Opportunities*, June 2004; The Robert Wood Johnson Foundation and America's Health Insurance Plans, *Health Insurance Plans Address Disparities in Care: Highlights of a 2004 AHIP/RWJF Quantitative Survey Collection and Use of Data on Race and Ethnicity*, June 2004.

[25] Congressional Quarterly Healthbeat News, "Health Plans, AHRQ, Join Forces to Reduce Health Care Disparities," December 14, 2004, available at http://www.cq.com/display.do?dockey=/cqonline/prod/data/docs/html/hbnews/108/hbnews108-000001456690.html@allnews&metapub=CQ-HBNEWS&seqNum=2&searchIndex=&prod=5; The

The legal environment surrounding health information is made further complex by the fact that the U.S. legal system is dense, multi-level and multi-dimensional. Both federal and state law come into play where health information is concerned, and the sources of law can range from judge-made common law (the bedrock of the American legal system) to constitutional principles, federal and state statutes, and the regulations imposed by hundreds of public agencies operating at both the federal and state levels of government.[26] While the well-known federal laws regarding health information often become the focus, more stringent state laws that co-exist with the federal scheme can be the key hurdles to overcome.[27]

In every instance of health information collection and disclosure, resolving the legal issues is an intense and fact-driven exercise. Furthermore, the legal answer may depend not only on the specific factual context, but also on broader public policy considerations (e.g., whether the law should allow the collection or disclosure, or should be modified to do so because of larger societal interests that outweigh legal concerns).

In sum, many of the most important legal debates now arising in the current version of the discussion regarding the use of electronic health information raise questions and tensions that are long-standing and well-recognized in the law. What *has* changed, however, is the nature of health and health care information itself, and in this transformation, not only are many long-standing questions recast in seemingly new contexts, but the very nature of this changing information enterprise raises issues never before thought of as being part of the law of health information.

Specific Issues in Health Information Law

Our discussions with legal experts yielded a wealth of issues requiring careful study and further resolution. Many of the issues raised appear to be amenable to resolution through clarification of the requirements and provisions of a wide array of current law such as federal tax law, federal and state laws designed to prevent anti-competitive conduct, federal privacy law, and federal civil rights law.[28] Other issues may require the enactment of new legal standards or the legislative modification of existing standards. The following discussion aims to identify specific legal issues on the horizon, while the next phase of the project will propose options for addressing these legal issues.

A number of the legal issues which surfaced over the course of our discussions involve considerations of privacy and the use — and misuse — of personally identifiable health information. However, experts also focused on many other aspects of the legal

---

National Health Law Program and Summit Health Institute for Research and Education (SHIRE), *Racial, Ethnic, and Primary Language Data Collection: An Assessment of Federal Policies, Practices, and Perceptions*, October 2001.

[26] *See* Furrow, et. al., *supra* n. 21.

[27] For example, while most view the federal HIPAA law as the regulatory control over health information privacy, numerous state laws that are stricter must also be met.

[28] For example, the legality of the collection of race and ethnicity data for permissible purposes under federal civil rights law has been clarified. 42 U.S.C.A. §2000e et. seq. (2004).

environment, which may act as possible impediments to greater production and use of health information. One of these aspects is the potential for information to be used to pursue a variety of legal liability claims against health care professionals and institutions that voluntarily engage in health information practices, for conduct unrelated to health information privacy. A second area of focus was on the ways in which current legal standards related to the formation and operation of large industries may impede the development of the industry because of the absence of the types of clarifications which are necessary to stimulate and advance formation of a modern health information industry.

For ease of discussion, the following section is divided between legal issues which relate to health information privacy, and legal issues which entail non-privacy-related aspects of the legal environment for health information systems.

A. PRIVACY-RELATED LEGAL ISSUES

Constitutional Right to Privacy

Because certain electronic health data collection models described above involve state actors, a constitutional right to informational privacy could be relevant. The Constitution itself does not expressly provide for a right to informational privacy. Outside of the Fourth Amendment, the Supreme Court has not articulated a strong standard for a constitutional right to informational privacy.[29] However, the Supreme Court has recognized a limited right to informational privacy as a liberty interest within the Fifth and Fourteenth Amendments in the case of *Whalen v. Roe*.[30] Specifically, *Whalen* stands for a narrow right to informational privacy with regard to the disclosure and security of data held in governmental databases – a right that must be protected through adequate safeguards in the governmental system. Yet attempts to interpret the breadth of the constitutional privacy protections articulated in *Whalen* have been inconsistent at best,[31] leaving us with a right in progress. Thus *Whalen* has failed to create a powerful constitutional right to medical information privacy.[32]

Implications

What type of state involvement is necessary to trigger a potential constitutional issue? Is there a difference in the likelihood of implicating potential constitutional issues among the models? For example, if the data is not held in a government database, are the potential legal issues minimized? If the government is a contractual partner in the system

[29] For an excellent discussion of 4th Amendment protections – or lack thereof – with regard to information privacy, *see* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. Cal. L. Rev. 1083 (2002).
[30] *See Whalen v. Roe*, 429 U.S. 589 (1977).
[31] Paul M. Schwartz, *The Protection of Privacy in Health Care Reform,* 48 Vand. L. Rev. 295, 317 (1995) (*citing Walls v. City of Petersburg*, 895 F.2d 188 (4th Cir. 1990) (applying a non-disclosure interest to a right of privacy); *but see Gutierrez v. Lynch*, 826 F.2d 1534, 1539 (6th Cir. 1987) ("legitimate requests for medical information do not constitute an invasion of the right to privacy")).
[32] *Id.*

design, is state action present? As a practical matter, how can individual requests for confidentiality regarding certain medical data be honored? This issue is related to the potential interaction of state law protections for patients regarding sensitive medical information, such as diagnoses and treatment for medical conditions, such as mental health, substance abuse, HIV-AIDS, and family planning services. However, breaches of confidentiality become less likely in decentralized system since the requested data is only aggregated for a moment in time to respond to a particular query and then reverts to its original source.

Common Law Privacy Protections

The common law in most states recognizes the duty of confidentiality of certain health care providers not to disclose health information. However, this common law duty of confidentiality has been eroded and is not sufficient to protect the privacy interests of patients because this duty is predicated on the doctor/patient relationship. In the modern health care system, a great deal of data collection and transmission is based only in part on this relationship, thus creating gaps in the duty. Nevertheless, the common law duty of confidentiality must be considered in any electronic data exchange system.

Implications

To what extent does the doctor/patient privilege protect information necessary for quality assessment and improvement purposes? Can certain data be treated differently or does the common law protection affect all data and for all uses? What about aggregate data? Can some of the important outcomes data be stripped of patient identifiers and still be useful? What are the liability considerations when a physician is induced by a third party to disclose certain patient information?[33] These questions are particularly relevant in light of the previously raised issues of accommodating patient requests for confidentiality that may be grounded in state-based legal protections. Again, a decentralized system in which the data are not aggregated would pose less of a privacy risk. Moreover, an administrative system would arguably contain less protected health information and therefore be less risky in a privacy context.

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Generally, the federal privacy regulations under HIPAA (also referred to as the "Privacy Rule") regulates uses and disclosures of protected health information (PHI) by "covered entities" (health plans, health care clearinghouses, and certain health care providers).[34] Covered entities cannot use or disclose PHI except as permitted or required under the Privacy Rule. "Use" includes an examination of PHI while "disclosure" generally entails divulging or providing access to PHI.[35] The Privacy Rule applies to all

[33] *See Hammonds v. Aetna Casualty & Surety Co.*, 243 F. Supp. 793 (N.D. Ohio 1965) (holding one who induces doctor to divulge confidential information in violation of doctor's legal responsibility to patient may be held liable for damages).
[34] 45 C.F.R. §§ 160-164.
[35] 45 C.F.R. § 164.501.

PHI, regardless of the form in which it exists (i.e., written, oral and electronic PHI are all covered)

Under the Rule, covered entities are permitted to use or disclose PHI without specific individual authorization for treatment, payment and health care operations (TPO). Although the only required disclosures are to the individual who is the subject of the information, to the individual's personal representative, and to the Secretary of HHS to investigate or determine compliance with the privacy requirements, permitted disclosures pursuant to an authorization from an individual or if required by law are allowed.[36] A violation of the Privacy Rule by the covered entity can result in severe criminal and civil penalties.[37]

However, information that would otherwise be PHI is not considered PHI if the individualized health information in question is de-identified, and the federal HIPAA regulations allow for the use of PHI to create de-identified information.[38] De-identified health information is that which "does not identify an individual and with respect to which there is no reasonable basis to believe that information can be used to identify an individual . . . ."[39] The Rule includes certain "safe harbor" provisions listing particular identifiers that, if removed from PHI, renders the information de-identified.[40] Thus, covered entities are free to disclose and use de-identified health information without having to comply with the Privacy Rule. Moreover special rules govern the use of PHI for research.

Additionally, HIPAA established other requirements relating to the standards that must be used by covered entities to transmit PHI electronically in connection with a financial or administrative transaction.[41] And the HIPAA security rules are effective in April 2005 (2006 for small group health plans). In addition to federal regulation of privacy and confidentiality practices, states also have laws and regulations covering these topics. HIPAA specifically protects state laws that are "more stringent" than the federal rules. In other words, if the state laws are more protective of a patient's rights, they can be enforced and are not suspended merely because federal regulations exist covering the same subject matter.

Implications

The collection and sharing of health information by electronic health data systems described above (and detailed in Appendix A) involve both PHI and de-identified health information. Can most of the necessary data be used or disclosed as part of the "health care operations" function under HIPAA by covered entities? What would be needed to comply with HIPAA privacy rules if non-covered entities also had access to data

[36] *Id.*
[37] 42 U.S.C.S. § 1320d-6.
[38] 45 C.F.R. § 164.502(d)(1).
[39] 45 C.F.R. § 164.514(a).
[40] 45 C.F.R. § 164.514(b).
[41] 42 U.S.C.S. § 1320d-2(a).

collection systems containing PHI? To the extent that the data is collected for research purposes, what additional safeguards are necessary and to whom would they apply? Can any of these legal questions be answered by establishing firewalls? The designers of each of the existing models claim that their electronic health data systems are "HIPAA compliant". What does that mean? Compliant for privacy purposes? EDI (electronic data interchange) purposes? Security purposes?

Although the legal experts with whom we consulted believed that HIPAA poses some challenges to the establishment and use of electronic health data systems, the experts agreed that although the HIPAA issues needed to be addressed and carefully analyzed, rather than ignored, ultimately HIPAA was not likely to be a substantial legal barrier. There exists a general misunderstanding of what HIPAA actually requires that has created a misplaced fear regarding the difficulty of compliance. Lawyers for some health care providers and institutions may currently perceive HIPAA to be a greater obstacle to data collection and use than it really is. A clarification of what the law covers would assist in resolving this misunderstanding. On the other hand, less clear is the barrier that state laws might pose since these laws vary considerably and will have to be evaluated on a circumstance by circumstance basis to determine whether each provisions of state law is more stringent than the related HIPAA provision. Moreover, it is not always clear which state laws will need to be analyzed since, depending on the system design and users, more than one state law may be implicated.

Privacy Act of 1974

The Privacy Act of 1974 established a comprehensive data collection and management procedure for the federal government. Under the Act, federal agencies cannot disclose identifiable information about an individual derived from a "record" within a "system of records" without the specific individual's consent.[42] To fall within the protection of the Privacy Act, the record must be maintained by an agency and contain any personally identifiable information. The Act only applies to disclosures by the federal government or third party contractors maintaining government records,[43] and thus does not cover private parties even if the information held by the private parties matches the information held by the government.[44] Moreover, the Privacy Act does not apply to de-identified information.[45]

Implications

The federal government utilizes Model III (Appendix A) – a centralized system – which could potentially implicate the Privacy Act of 1974. Does CMS only gather data for quality improvement purposes and not disclose PHI? If the federal government decided to establish another type of data base along the lines of Model I (Appendix A)

[42] 5 U.S.C.S. § 552a(b) (1989 & Supp. 2004).
[43] 5 U.S.C.S. § 552a(m)(1) (1989 & Supp. 2004).
[44] *See Lohrenz v. Donnelly*, 187 F.R.D. 1 (D.D.C. 1999).
[45] 45 C.F.R. § 5b.1(h).

with its "virtual" (decentralized) data base approach, would the Privacy Act still apply, since there is not a single "record" within a single "system of records"?

Gramm-Leach-Bliley Financial Services Modernization Act of 1999

This Act contains comprehensive federal privacy protections for consumers/customers of financial institutions which, under the Act, include health insurers.[46] The privacy protections contain requirements applicable to nonpublic personal information obtained by a covered institution, even if the information is not financial in nature.[47] The central aim of this Act is to require financial institutions to notify consumers of their information disclosing policies and allow consumers to opt out of having their personal information shared with nonaffiliated third parties.

Implications

Does this law have any application to the collection and use of data collection systems used solely for health purposes by health care providers or institutions other than insurance companies? Would HIPAA preempt the less-stringent standards of GLB? If a health insurer participated in a health information sharing model with other non-insurance entities, would the opt-out rules for individuals apply, since these other entities are likely to be non-affiliated third parties? Would the participation of an insurance company covered under GLB taint the operation of the information system and cause everyone else to be forced to operate under the GLB rules?

State Legislation

A patchwork of state legislation regulating privacy implicates the models for the collection and sharing of health information. Regarding state collections of data, most states have passed laws that parallel the Federal Privacy Act discussed above.[48] Additionally, some states have enacted legislation that provides broad and comprehensive protections of health information collected, acquired, used, or disclosed within the state.[49] Certain states have passed disease-specific laws that include very strong security protections for certain types of health information, such as HIV status, sexually transmitted diseases, public health information, or genetics.[50]

[46] 15 U.S.C.S. §§ 6801-6810 (Supp. 2004).
[47] *Id.*
[48] *See e.g.* N.Y. Pub. Off. Law §§ 91-99 (McKinney 2004).
[49] *See e.g.* Cal. Civ. Code §§ 56-56.35 (West 1982 & Supp. 2004) (law intended to protect confidentiality of individually identifiable medical information obtained from patient by health care provider, while at same time setting forth limited circumstances in which release of such information to specified entities or individuals is permissible).
[50] *See* Gostin et al., *Balancing Communal Goods and Personal Privacy Under a National Health Informational Privacy Rule,* 46 St. Louis U. L.J. 5 (2002).

Implications

Which of the state laws would not be preempted by HIPAA (those state laws that are more stringent (i.e., more protective of individuals) are not preempted)? What special legal obstacles would have to be overcome if the data collection system's users were located in more than one state but through contract entered into a partnership? What if the individuals whose PHI was being collected and used were from differing states? How would the conflicting state privacy laws be reconciled? How would state implementation of stricter federal privacy provisions affect the ability of certain Federal programs such as Medicare or the VA Health System to participate in data consortia?

B. NON-PRIVACY-RELATED LEGAL ISSUES

Health Care Fraud and Abuse

(a) Federal False Claims Act

The federal government has been using its power through prosecutions under the False Claims Act (FCA)[51] to provide incentives for active efforts to both improve health quality and report the results. The FCA authorizes the federal government to investigate and sanction health care facilities for providing poor quality of care.[52] The Act does not require a specific intent to defraud. Liability under the FCA attaches to those who "knowingly" – defined as deliberate ignorance or reckless disregard – present or cause to be presented "a false or fraudulent claim for payment."[53] U.S. Attorneys are now applying the FCA to Medicare/Medicaid transactions involving care of very poor quality. The theory is facilities that provide care of substandard quality and then seek government reimbursement are making "false claims."

The OIG has stated that it will focus on quality of care in nursing homes through the use of the FCA.[54] Much of the litigation has been focused in the Philadelphia area, and in the vast majority of cases the DOJ forces a settlement because of the enormous costs of defending such an action.[55] For example, in September 2004, the DOJ reached a settlement with the Green Acres Nursing home after alleging inadequate services regarding nutrition, provision of medication to residents, falls, pressure ulcer care including the prevention and treatment of wounds, and incontinence care. The settlement provides for the following:

---

[51] 31 U.S.C. §§ 3729 et. seq. (2004).

[52] In addition, private "relators" can come forward under a separate "qui tam" authority to report false claims. If the government declines to prosecute, the relator can step into the shoes of the U.S. government and pursue the case and recover the money damages.

[53] 31 U.S.C. § 3729(a)(1) (2004).

[54] *See* "IG Rehnquist Sees Health Fraud Crackdown, Promises Additional Interagency Cooperation," BNA's HEALTH CARE DAILY REP. (May 17, 2002).

[55] *See* http://www.usdoj.gov/usao/pae/Documents/ElderAbuse.htm for a list of FCA actions and settlements in the Philadelphia area.

1. Payment of $143,000 to the government.

2. Creation of a Quality of Care/Quality of Life Fund in the amount of Twenty Five Thousand Dollars ($25,000) that will be used within a year to purchase services and/or equipment that would enhance the quality of life of the residents;

3. For at least a one year period, use of independent third-party consultants selected by the United States to assist in and assess Green Acres' compliance with the settlement agreement.

4. Greenacres Health Systems agrees to develop a Corporate Compliance Program that sets forth the structure for reporting and addressing all components relevant to the provision of adequate care. This compliance program will apply to all of the health systems long-term care facilities.

5. Conduct training at least semi-annually for staff on issues identified by the facility's Compliance and Quality Assurance Committees and/or the government.

This case marks the fourteenth nursing home failure of care case resolved in this district by means of the FCA within the last eight years.[56]

Implications

The potential use of any of the models for gathering data to assess the quality of care could implicate the FCA. To the best of our knowledge, this tool has been used in an institutional context only, but there is no reason why it could not be applied to individual professionals as well. Perhaps one of the most interesting aspects of this FCA strategy is the role of Health Care Corporate Compliance (item #4) in preventing FCA sanctions. The IG has emphasized that one critical means for addressing exposure to FCA is prophylactic activities on the part of institutions so that they can demonstrate that they have vigorous systems for nipping problems in the bud. For this to work in a FCA context, the institution presumably would have a rigorous quality improvement program which includes standard setting, oversight of staffing and the process of care, measurement of key outcomes, and collection and analysis of data. In other words, demonstrating an active effort to internally investigate and improve quality could help a facility defend against a false claims charge.

(b) Physician Self-Referral (Stark) Law

The Stark law protects against conflicts of interest that may arise between physicians and other health care entities. Physicians cannot refer patients to an entity for certain health services if the physician (or an immediate family member) has a financial relationship with that entity. The law also prohibits such entities from billing for any services resulting from such referrals unless an exception applies, however such exceptions are insufficient to cover all the potential arrangements in which physicians

[56] *Id.*

and health entities may wish to engage to promote heath information technology.[57] Because many physicians find health information technologies cost prohibitive, they often accept hardware, software, or other resources from a hospital or other provider. If the physician then refers a patient to an entity that has provided these technologies, the Stark law could be triggered. Violations can result in exclusion from federal health programs and civil penalties. The Medicare Prescription Drug, Improvement and Modernization Act of 2003 does call for HHS to establish exceptions to facilitate electronic prescribing, and CMS is currently revising a rule after receiving comments that creates a new exception to the Stark law for the building of "community-wide health information systems."[58]

Implications

Given the fact that many physicians do not currently have computer capacity in their offices, in some cases, physicians have been given incentives to assist in the development that capacity, including furnishing of free or low-cost computers, hardware, software, and computer instruction. In addition, physicians participating in any one of the models may, from time to time, accept various types of health information technologies from others for start-up purposes or upgrades. Do subsequent referrals to those organizations for health services violate the Stark law? There are statutory and regulatory exceptions to the self-referral laws. Do they sufficiently cover all potential arrangements in which the parties may wish to engage? Some experts claim these fraud and abuse laws will not be implicated when only private funds are used, but without confirmation that this is correct, some physicians may be reluctant to participate in these programs.

(c) Anti-Kickback Laws

Anti-kickback laws strictly prohibit individuals or entities from knowingly and willfully offering or accepting remuneration to induce a patient referral for or purchase of an item or service covered by any federal health care program.[59] Violations can result in exclusion from federal health programs, civil and criminal penalties. Some exceptions exist, but again, none are sufficient to cover all potential arrangements regarding health information technologies. HHS noted the difficulty in "crafting safe harbors that exclude abusive arrangements,"[60] and no parallel exception for "community-wide health information systems" exists under the anti-kickback laws.

Implications

[57] 42 U.S.C. § 1395nn (2000).
[58] Interim Final Rule on Medicare Program; Physicians' Referrals to Health Care Entities With Which They Have Financial Relationships (Phase II), 69 Fed. Reg. 16054-16146 (March 26, 2004).
[59] 42 U.S.C. § 1320a-7b(b) (2000).
[60] *HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption*, The United States Government Accountability Office, GAO-04-991R at p. 47 (August, 2004).

Much like the Stark law, anti-kickback laws could potentially be triggered if, after the acceptance of health information technology from a hospital or other provider, the physician then refers a patient to that hospital or provider for government services and the health information technology is subsequently viewed as remuneration. There are statutory and regulatory exceptions to the anti-kickback laws, but do they sufficiently cover all potential arrangements in which the parties may wish to engage? Again, some experts claim anti-kickback laws can be avoided if only private funds are used.

Antitrust

Antitrust laws exist to promote competition by avoiding monopolistic behaviors that knowingly and unreasonably limit competitors in a given field.[61] It is unclear what exactly constitutes a violation with respect to the impact of health information sharing arrangements among several providers and payers. The Department of Justice has issued opinions stating that to the extent the benefits of such arrangements outweigh any anticompetitive impact, they are unlikely to violate federal antitrust law.[62] However, as one expert meeting attendee noted, "today's collaboration is tomorrow's execution."

Implications

Contract agreements among various entities described in the models could implicate antitrust laws in a number of respects. If the use of one of these models becomes necessary to compete in the marketplace, does antitrust law get triggered if certain entities are excluded through the contract terms? If the models eventually serve to determine pay for performance quality assessments, must all types of models do so uniformly using the same set of criteria? Will a model be deemed an essential facility and thus require access for all providers and payers? Adoption of health information systems could be perceived as exclusionary or anticompetitive. Does several providers and payers working together to utilize a health information system constitute collusion? Are incentives offered to potential participants violative of antitrust law? Several experts noted the NEHEN system (Appendix A) avoids antitrust implications because it is a non-exclusive community-wide model that any entity can freely join or leave. NEHEN is, however, dues-based which could be deemed prohibitive for smaller entities.

Federal Tax Laws

(a) Private Inurement/Benefit

The possible participants in the various health information models could include physicians, hospitals, payers, pharmacies, pharmacy benefit managers, the entities created to run the systems themselves, such as NEHEN, and their subcontractors. The tax-exempt status of any one of these entities is dependent on several requirements. One such requirement prohibits tax-exempt organizations from providing financial or other

[61] 15 U.S.C. § 1 et. seq. (2000).
[62] GAO Report at 48, *supra* n. 60.

benefits to private individuals.[63] Put another way, the net earnings of a tax-exempt organization may not inure to the benefit of a private person (including a private entity). This prohibition against private inurement embodies the primary distinction between taxable and tax-exempt entities.[64] This rule is rigidly enforced; for example, a tax-exempt social club lost its exempt status because it served lunch and a snack to its members.[65]

Implications

The parties contracting or joining a care alliance to form the health information system may include one or more tax-exempt entities. The accounting practices of any tax-exempt entity will be heavily scrutinized to ensure that no private inurement occurs. If several taxable insurance companies, hospitals, and physician practices engage in a partnership for the electronic transmission of health data, and that system is run and managed by a tax-exempt partner, do the savings realized by the partners inure a private benefit?

Likewise, the provision of health information technologies and other resources by tax-exempt organizations to physicians could jeopardize the tax status of these organizations if the health IT resources are viewed as a benefit conferred to a private individual.

(b) Unrelated Business Income

Income generated by a tax-exempt organization from a business activity not substantially related to the role that created the tax-exempt status is taxable income.[66] For a business activity to generate unrelated business taxable income, the activity must be conducted regularly and not sporadically. For example, if a tax-exempt organization sells cars once a year at an exhibition, the income generated is not unrelated business income. Once classified as an unrelated trade or business, the organization must compute its unrelated business taxable income and pay tax thereon.[67]

Implications

Again, the organization of the partnership that includes a tax-exempt member – the entity running the system itself – must take into consideration unrelated business income. It is not at all clear how the flow of money (dues, savings, administration costs, etc) will be captured in tax law, and thus taxation of the tax-exempt entity in the partnership may occur if certain charges are deemed to be outside the purpose for which

[63] 26 U.S.C. § 501(c)(3) (2000).
[64] *See* Darryll K. Jones, *The Scintilla of Individual Profit: in Search of Private Inurement and Excess Benefit*, 19 Va. Tax Rev. 575, 577 (2000).
[65] *See Spokane Motorcycle Club v. United States*, 222 F. Supp. 151, 154 (E.D. Wash. 1963).
[66] 26 U.S.C. §§ 501(b), 513(a) (2000).
[67] *See* 44 Tax'n for Acct. 378, 1990 WL 361175 (W.G.&.L. 1990).

the tax exempt status was sought. Charges that tax-exempt hospitals impose on others for using health IT resources financed by the hospital may be taxable.

Civil Liability in a Health Quality Context

In certain key respects, the thorniest legal questions that arise perhaps may have to do with the implications that could flow from more data – and more access to data. Liability problems are popularly associated with the legal consequences of privacy and security failures that lead to unlawful data access and use. But as the volume of data reported by – and indeed, present within – information systems grows, the potential also grows for greater data access related to legal enforcement efforts undertaken by individuals and government agencies to enforce standards of quality and accountability.

(a) Professional Liability for Substandard Quality Care

State malpractice laws define the standard of care that must be followed in carrying out treatment activities. The systematized collection of health data and its analysis for quality assessment and improvement purposes should make it easier to identify and ultimately prevent medical errors. However, these collection and analyses activities may also make it easier to identify health care institutions and providers with below-average patient outcomes and those who may arguably be delivering substandard care. The availability of this information could also lead to referral liability if a physician refers a patient to another doctor with a poor quality rating.

Implications

It is possible that any system distinction could increase physicians' risk of malpractice claims. However a centralized model allowing for quality research imposes more potential liability than a decentralized model. Simply because the centralized model that warehouses all clinical data together could be researched using certain quality metrics, providers could be "graded" and a poor evaluation used as evidence in a malpractice suit. Depending on the extent to which outcomes and treatment data is publicly available or is not protected from discovery in liability litigation or other quality of care enforcement actions, physicians and other health care professionals and healthcare institutions and suppliers may be less willing to participate in data collection and exchange programs. Moreover, the increased availability of the health information itself could raise the standard of care by requiring physicians to evaluate all available health information on a given patient in making treatment decisions. If physicians have the ability to use these systems to identify quality measures, what then becomes the industry standard? Also, does a flawed design in the system itself that leads to medical errors carry liability?

Other medical malpractice concerns include treatment based on incorrect or incomplete information in the electronic data. Indeed, incorrect or incomplete information problems continue to plague the paper system in the form of the deficient or

missing charts, and the transformation to an electronically-based health information system will not automatically solve the liabilities stemming from acting upon an incomplete or erroneous medical record. An automated system could certainly be set up to catch and thus reduce these errors, however the errors that remain have increased their exposure exponentially. In fact, the electronic medium enables vastly more providers to treat based on potentially flawed information thereby broadening liability. For example, even the designers of the identification correlation process in the Santa Barbara model admit it is not perfect and could conceivably result in a misidentification of the proper patient receiving treatment. Even if no injury results, is there an obligation to correct the error? Also, certain sensitive health information is often filtered out of electronic transmissions which a treating physician may need to render adequate care. Can it be released for emergency care? The Santa Barbara and NEHEN models operate under a "user beware" contract term in which all participants agree that occasional errors in the electronic data are inevitable. But what then is the system of record? And what rights does a patient have if treatment is provided based on a provider's evaluation of the medical record of another patient?

Note that this is one of the areas in which the legal questions are not substantially different when the medical record system is a paper one. Such patient mix-ups are possible even without an electronic medical data system. However, one of the arguments in support of electronic systems is that the chances of such a mistake are reduced because there are many additional ways to screen out such mistakes in an electronic system.

Additional implications arise if the physician uses the data for purposes to which the patient did not consent. Is this a breach of the duty of confidentiality? Also, what is the medical liability if the patient accesses his or her own health information with the physician's aid and then, armed with this health information, acts in a way that injures the patient? And who is permitted to grant this access to patients? In fact, the issue of ownership of the medical record itself is critical, and the next phase of our research will attempt to resolve the record ownership question through a consensus of experts.

(b) Corporate Liability for Substandard Quality Care

In addition to medical malpractice, corporate liability in a health care context imposes civil liability on the various entities (hospitals, managed care organizations, physician groups) involved in the provision of care to patients if the structure of the health services themselves proximately causes injury. For example, an HMO that contracts with a physician not properly licensed can be held liable for sending patients to that individual for treatment. Entities participating in an electronic health information system that is structured to collect race and ethnicity data for quality measurement purposes (which is a lawful practice under current federal civil rights law) may fear the potential for civil corporate liability if the data reflects substandard care for specific groups of people. Additionally, simply amassing such data and then failing to address the problems the data highlight may also result in corporate liability.

Implications

The law is unclear regarding what, if any, corporate liability implications arise from the collection of race and ethnicity data for quality control purposes. If the data are collected, can a plaintiff use this information to support an allegation of poor quality care in the case of minority patients, quite apart from a claim of legal discrimination against minority patients under Title VI of the 1964 Civil Rights Act? Even where a defendant's actions cannot be challenged for their discriminatory effects, could a minority patient use evidence of suboptimal care for minority patients to bolster a quality claims? Would the absence of data suggesting disparities in care bolster a defense that the quality of treatment met legal standards? How far does the concept of privilege extend in litigation of this sort? If an entity has the capability to collect this type of data but chooses not to do so, does corporate liability attach?

(c) Defamation

The law of defamation embodies the notion that individuals and entities should be able to enjoy their reputations free of any false or misleading attacks.[68] A reputation that is defamed is one that has been subject to untrue derogatory statements which denigrates the opinion that others in the community hold of that individual.[69] One potential goal of the health information models is to identify quality gaps in the provision of health services both at the provider and hospital levels through systematic research of the clinical data in centralized systems. Inevitably certain practitioners will be at the bottom of the list after quality measures are evaluated.

Implications

The use of a centralized model to collect data for quality assessment purposes will eventually create a ranking. Although the current systems are not designed to measure quality, in the near future they will be and thus allow health care regulators and consumers to rate providers against one another. A lawsuit for defamation could be brought by the physician or the hospital if either believes the poor quality assessment is unjustified or unfairly determined, and that determination harmed its reputation. Because in such a case the only defense would be to prove the truth of the poor quality allegation, a messy piece of litigation could result attempting to determine whether the physician or hospital actually provided poor quality of care.

Contractual Breaches

Contracts will govern most of the activity that occurs within the various models. When participants contract with one another to create a partnership, those contracts will detail the rules of the game as to the use of the health information system. Providers and payers will use contracts to define the rights and liabilities for issues pertaining to personal property, intellectual property, confidentiality of the health data, the use of trade

[68] 50 Am. Jur. 2d Libel and Slander § 2 (Supp. 2004).
[69] *Id.*

names, system security, medical malpractice liability for errors in the data, and data standardization. It is important to note that in addition to intellectual property notions regarding ownership of the information system, certain personal property rights also exist in the data itself. Likewise, personal property rights to an individual's health record continue to remain in question and will be analyzed in future phases of this project.

Implications

Several experts noted that many thorny issues can be solved though the use of contracts. Nonetheless, reaching the point where the participants contractually agree on issues that are still unclear in the law becomes the real obstacle. Who actually owns the information traveling back and forth? Who incurs the liability when erroneous data contaminates the system? Who has the ownership rights in the intellectual property developed from standardizing the data? What about the very standards themselves? Copyright protections as they now exist may be inadequate to protect the interests of newly developed health information technologies.[70] Also, what is the fair market value of an electronic medical record? Can the rights to it be bought and sold?

Additionally, the concept of a "third-party beneficiary" may be implicated with respect to the contracts. When two parties contract for the benefit of a third party, that third-party beneficiary usually has the right to enforce the contract even though that third-party may not have been involved in the agreement itself.[71] This type of arrangement is most commonly seen in the use of trusts where a trustee and a settlor contract for the benefit of a third party. If the models are used under the auspices of improving the quality of care (presumably for the benefit of the patient), the patient could claim third-party beneficiary status and sue, possibly contending that the payer and provider are not providing the intended benefit to the patient.

State Licensing Matters

Physicians must be licensed in any state in which they practice medicine, and the licensing requirements vary from state to state.

Implications

If a health IT system enables a physician to provide advice across state lines, it is possible the physician may be viewed as practicing in a state without a license. Indeed, providers that practice telemedicine must be aware of the licensure requirements of the states *where the patients are located*. Most states maintain "full licensure" laws that require telemedicine practitioners to be fully licensed in the state where the patient resides, while a handful of other states offer "special purpose licenses" for out-of-state physicians that exempt certain licensure requirements for the practice of telemedicine.

[70] 17 U.S.C. § 106 (2000).
[71] *See* Howard O. Hunter, THE MODERN LAW OF CONTRACTS § 20:2 (2003).

Civil Rights

Title VI of the Civil Rights Act of 1964 prohibits recipients of federal assistance from discriminating on the basis of race, color or national origin. The Americans with Disabilities Act (ADA) prohibits discrimination against qualified persons with disabilities by places of public accommodation, which have been defined to include health care providers.[72] Although the ADA remains enforceable by individuals, the United States Supreme Court ruled in 2000 that private litigants could challenge only intentional, and not *de facto*, acts of discrimination by recipients of federal financial assistance under Title VI. [73] The Secretary of Health and Human Services retains full enforcement rights over all forms of discriminatory conduct under civil rights laws, but the enforceability of civil rights laws by private individuals is now significantly constrained.

There exists a common misperception that civil rights law prohibiting discrimination on the basis of race and ethnicity would somehow bar collection and analysis of racial and ethnic data as part of a project to reduce disparities and improve health care quality. Racial and ethnic data have been shown to be integral to analysis of health care quality for a patient population; as a result, while the use of such data to achieve discriminatory results would be barred, its collection would not be, and its use to improve health care quality would appear to be entirely consistent with the purpose and structure of anti-discrimination laws. Indeed, Title VI expressly grants authority to the federal government to mandate the collection of racial and ethnic data, and the Secretary has the authority to order collection for quality improvement purposes. Nothing in federal law would appear to prohibit a covered entity from collecting data for quality improvement.[74] State laws permit the collection of data for quality improvement purposes, although the terms used under state law vary. [75] Notably, the State Children's Health Insurance Program (SCHIP) provides for state collection and reporting of race and ethnicity data regarding health care services to the federal government in quarterly reports.[76]

Implications

Collecting and analyzing health data through the use of a centralized system by race, ethnicity and gender or by certain measures of health status and functioning may be useful in identifying and correcting racial and ethnic disparities across health care institutions and providers. However, concerns have been raised that the availability of this type of information could be used improperly for racial and ethnic profiling, the design of benefit plans which discriminate on the basis of health status or disability, and

---

[72] *See Bragdon v Abbott,* 524 U.S. 624 (1998).
[73] *See Alexander v. Sandoval*, 532 U.S. 275 (2001).
[74] 42 U.S.C.A. § 2000e et. seq. (2004).
[75] For example, Maryland, New Hampshire, California, and New Jersey implicitly allow data collection on race and ethnicity but explicitly prohibit heath insurers and managed care organizations from requiring this information on the application form. *See* National Health Law Program, *Assessment of State Laws, Regulations, and Practices Affecting the Collection and Reporting of Racial and Ethnic Data by Health Insurers and Managed Care Plans* (2001).
[76] 42 C.F.R. § 457.740 (a)(3)(ii)(2001).

discrimination based on genetic information. On the other hand, collection of this type of data could make it easier for health systems to understand how key populations gain access to and use health care, as well as understand their experiences in the health care system. Data also could be used to establish population-specific performance measurements and benchmarks as a means of incentivizing and measuring compliance with civil rights laws, and for adjustment in payment to reflect actual patient experiences. The real challenge lies in communication and outreach to educate the public, and specifically the participants in the health information system models, that the proper collection and dissemination of racial and ethnic data with regard to health disparities is permissible.

Intellectual Property/Personal Property Issues

Ownership of health information and the ownership of the system that electronically transmits the health information should be considered as distinct legal concepts. The data itself could implicate personal property rights, with the patient, insurance company, physician and other entities making cognizable claims to ownership. The rights to the system (i.e. how it was built, how it runs, security measures, etc.) involve intellectual property. Both types of property are quite valuable, and thus the modern health care enterprise has elevated issues of ownership because of the interest of business investors in owning their products – either personal property or intellectual property – and thus being able to charge a licensure or use fee. Federal and state laws deal with the protection of rights and income that arises from the proprietary interests that flow from the creation and operation of business organizations, hospitals, physician group practices and other related organizations. These protections take many forms, such as reservations of rights through copyright, trademark, licensing, franchising, trade secrets. Under these laws, uses of the protected intellectual property may, under certain circumstances, be authorized through structured programs of permitted uses, including the payment of fees in connection with the use of protected property.

Implications

Creation of interoperable electronic data systems, whatever the distinctions, in which data is exchanged among health care stakeholders, such as medical providers, hospitals, payers, and health plans raises substantial questions about the rights regarding the health data. Who owns the data? Who owns the rights to the system itself and its components? Are the methods through which data is shared and the processes used to format, encrypt, de-identify, and store data protected? If the data is standardized, who owns the right to that process and its product? These and other similar questions regarding ownership must be resolved at an extremely early stage of the process so that legal disputes are less likely to arise as the project progresses. Participants in data sharing arrangements will want to identify any potential system feature that has the potential to dilute property interests or to raise conflicts among competing property interests.

Governance of Data Sharing Arrangements

An issue closely related to the personal and intellectual property questions is how the data sharing arrangement will be governed. Although these questions are typically governed by formal or informal agreements or contracts, state and federal laws in many related areas must be considered.[77]

Implications

One of the threshold issues is whether a separate legal entity is necessary to accomplish the data sharing functions and if so, what corporate form should it take. Other issues might arise regarding the ability of corporations and other legal entities to enter into contracts, the ability of organizations of health professionals to participate in data sharing arrangements, and, to the extent that public funds might be involved in the establishment and operation of a data sharing arrangement, what constraints does that place on the system. Moreover, what is the organizational liability for acts or omissions of individuals and entities based on data sharing activities? Who decides what individuals and entities may participate in the electronic data sharing system and what are the criteria for participation? Who decides if the conditions for participation have been violated? What sanctions exist if agreed-upon protocols for use are violated? Resolution of governance issues can be very difficult, especially if the participants in a data sharing arrangement span more than one state.

V. IMPLICATIONS FOR HEALTH PRACTICE AND HEALTH INFORMATION

Payers increasingly expect that health care providers will furnish extensive information on their patient practices both for payment and quality measurement purposes. Even more fundamentally perhaps, future generations of health care providers can be expected to be judged in the quality of their care by the extent of their active participation in health information systems that are capable of measuring, and providing them with timely feedback information about, the quality of their care. If legal expectations about information in a payment and quality context are to be realistic, then legal barriers to the development, diffusion, active use of health information systems, and legal ownership of the health record also must be addressed.[78] Indeed, resolution of these legal questions to be addressed in the next phase of our research – as well as new questions that emerge in the future – would appear to be essential to spurring a social willingness to invest in health information improvement.

This analysis underscores the scope and range of laws which collectively comprise the legal environment for health information. Much of this environment relates to the health care system's accountability to patients, health care purchasers and health

[77] Questions of corporate law may arise in the structuring of the various systems, however the data sharing agreements would not be affected by corporate structure.

[78] While HIPAA clearly establishes an individual's right of access to one's health record, actual ownership of the information contained therein is still ambiguous.

care. This accountability comes in various forms: accountability for the integrity and privacy of personal health information; accountability to patients for health care quality, non-discrimination, and fairness in treatment of patients from disparate backgrounds; accountability to purchasers for health quality; and accountability to government over matters of public health protections, health care quality, and the integrity of health care transactions. Furthermore, this analysis suggests that this level of accountability is present regardless of whether information is paper or electronic, collected as a set of isolated information transactions or as part of a highly connected electronic information enterprise. In other words, at the level of the individual health professional, the arrival of an electronic information era probably adds little new to the law of health information. Nothing about the modern information age alters fundamental legal accountability for professional conduct.

That said, it would be naïve to assert that the modern health care information enterprise changes nothing. As far as the law is concerned, electronic systems have two types of effects. First, they provide the means to generate far more information about health care practice, and thus, the level of legal exposure under longstanding principles of legal accountability is elevated. Second, because providers' legal exposure may increase as large amounts of information about their health care practices become available, the advent of the modern health information system raises questions regarding the potential need for – and relative value of – added legal protections for health care providers who become active participants in the new enterprise.

Similar considerations come into play where formation of the electronic health information industry is concerned. Part of this pathway to formation inevitably must be clarification of existing laws in order to reconcile the legal environment with emerging business models. Our consultations with experts suggest that this need for coordinated and multi-agency intervention to ensure proper reconciliation is particularly true in the case of health care information privacy, business taxation, health care fraud, intellectual property, and antitrust law.

Whether additional protections are warranted entails a careful balancing of society's interest in generating a great deal of information about health care against society's equally great interest in avoiding so serious an exposure of health care providers to new levels of liability that they come to perceive the health care enterprise itself as generating too serious a legal exposure. An effort to carefully balance social interests is inherent to the adoption of legal standards; indeed, much of law is fundamentally a formal effort to reconcile competing social preferences and needs.

In some cases, the development of standards which allow the system to evolve without generating undue liability on the part of providers and businesses may be relatively simple and non-controversial (although we hesitate to add that nothing in law ever seems to be simple and without controversy). One example of a relatively simple and beneficial step would be the issuance of clarifications by federal and state civil rights agencies which are aimed at underscoring that the collection and analysis of data on the race and ethnicity of patients for purposes of quality improvement activities not only

poses no legal problem but would in fact be considered evidence of active compliance with civil rights standards. Moreover, federal legislation clarifying these misconceptions and promoting race and ethnicity data collection might be an important step forward.[79]

Another example – although one which undoubtedly is much less simple and more prone to the resolution of competing interests – would be the joint issuance of comprehensive standards across a series of federal agencies, which clarify the ways in which the emerging electronic information enterprise can proceed without running afoul of existing health privacy, tax, antitrust, and fraud laws. On numerous occasions in the past, federal government agencies have worked closely to jointly develop common standards covering a range of federal undertakings. Examples of coordinated federal activities to further health care activities can be found in uniform federal standards governing human subject research, health care information privacy, and civil rights compliance.

This analysis is intended to offer a first step towards trying to identify key legal issues and facilitate a consensus around the new conceptual legal framework on which the new health information system depends. The legal issues may vary somewhat as the purposes and uses of emerging systems change, and as decisions are made regarding which, if any, aspects of the system should be mandated in law. Our in-depth discussions with information and legal experts greatly assisted in identifying the shape of the legal environment and how its specific dimensions may need to be altered in the coming years.

In broad terms, we believe that the following steps will help create a legal climate which encourages innovation in health information:

(1) First, it is important to identify the legal issues for which sufficient expert consensus exists that a clarification of current law – rather than new law – will ease impediments to innovation.

(2) Second, this consensus should be translated into specific actions aimed at encouraging health information activities. Clarification of permissible conduct is key to the diffusion of technological advances such as the use of health information, as well as health information technology, to improve health care quality and reduce disparities.

[79] In the 108th Congress, several bills on this issue as it relates to health care were recently sponsored but never enacted into law. *See* Faircare Act, S. 2594 and H. 5338, 108th Cong. (2004) (requiring the collection of data on race, ethnicity, highest education level attained, and primary language in federal health care programs); Closing the Health Care Gap Act of 2004, S. 2091, 108th Cong. (2004) (promoting the accuracy of data collection on race and ethnicity in public and private health plans); Health Information for Quality Improvement Act, S. 2003, 108th Cong. (2003) (providing for demonstration projects for the collection of race and ethnicity data). However, race and ethnicity data collection is required at the federal level in other areas such as banking law which requires the collection of data on the "racial characteristics" of mortgagors and mortgage applicants. *See* Home Mortgage Disclosure Act, 12 U.S.C. §2803 (b)(4) (Supp. 1993). Likewise, a provision of the Fair Housing Act requires the collection of data on the "racial and ethnic characteristics" of persons eligible for assistance under the Act. *See* 42 U.S.C. §3608a (1988).

(3) Third, where consensus emerges that more far-reaching changes in law should be pursued, it will be important to pursue these changes within the context of a conceptual legal framework which promotes advances in information without compromising the fundamental trust relationship between health care providers and their patients and the integrity of the health system itself. The singular nature of health care and health information is such that all efforts to alter the system so as to gain large amounts of knowledge about who gets health care, for what purpose, and to what end must, in our view, proceed only with the fundamental relationship between health professionals and patients clearly in view.

The technology revolution that will ultimately transform physician practices from their current reliance on paper records to a new frontier of electronic data records and rapid data retrieval and interchange may appear to be diffusing slowly. At the same time, greater clarity in health policy, coupled with further changes in policy where they are needed and financial incentives to support a transformed health system will produce the desired effect, just as a combination of policy reforms and financial underwriting have aided the diffusion of other innovations in health care. Over time, a transformed health information environment is poised to emerge not only as a basic component of health care quality, but as a central feature of the business of health care.

Given the momentum and commitment of these emerging public-private partnerships to drive change, it is critically important to assure that the legal framework and environment for these activities is not an impediment to progress, but rather facilitates it in a way that supports the advancement of these activities to improve patient care and health outcomes, while preserving essential patient protections. This is a daunting task, but one that we believe is both necessary and achievable.

APPENDIX A

The following descriptions, developed with the assistance of several data experts,[80] are intended to illustrate the architecture of "decentralized" and "centralized" systems of electronic data exchange. These were developed for discussion at the October 26, 2004 meeting.

MODEL I: DECENTRALIZED ADMINSTRATIVE DATA EXCHANGE

Example: New England Health EDI Network ("NEHEN")

NEHEN is a data exchange system developed to reduce health care administrative costs. NEHEN consists of a consortium of 42 regional payers and providers (some of whom own shares in NEHEN) that have entered into agreements to exchange patient specific administrative data. The data are not stored in a permanent record, but exist "virtually" and solely for the use of the health care provider that requests the data. An authorized provider, for instance, may query NEHEN regarding a patient's insurance status for a particular service. NEHEN retrieves the requested information from the appropriate warehouse (i.e., the payer's warehouse in this instance) and displays it on the provider's computer screen.

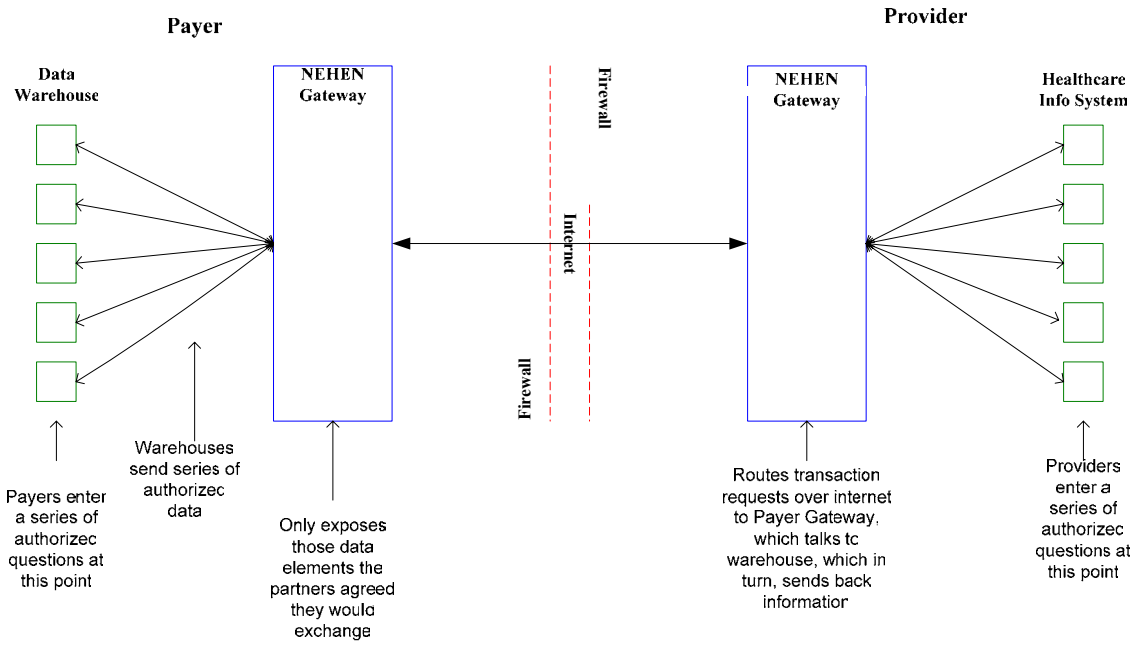
The requested data are transitory in nature, existing only for the moment in time when the query is made; once the provider exits the screen, the information is lost. The electronic data transactions that NEHEN supports comply with the HIPAA electronic data interchange (EDI) standards.[81] NEHEN's limited purpose is to support and process claims-related transactions between payers and providers. It serves solely as a system of administrative data sharing and information cannot be aggregated. This limited function makes it inadequate for quality improvement and research. The diagram set forth below summarizes the NEHEN system of data exchange.

---

[80] We are extremely grateful for the assistance provided by data and information system experts, including John Halamka, M.D., Chief Information Officer, CareGroup Health System and Harvard Medical School and Chairman of the New England Health Electronic Data Interchange Network (NEHEN); David Szabo, Nutter, McClennen & Fish, LLP, Boston, MA; Nicholas Augustinos, Vice President, Care Data Exchange Group, CareScience, San Francisco, CA; and Greg DeBor, Partner, Global Health Solutions, Computer Sciences Corporation, Boston, MA; and Lori Evans, Senior Advisor, Office of the National Coordinator for Health Information Technology (ONC), U.S. Department of Health and Human Services (HHS).

[81] These include the following standard transactions under HIPAA: benefits/eligibility (HIPAA standard transaction 270/271), referral/authorization (HIPAA standard transaction 278), claims payment (HIPAA standard transaction 837), remittance (HIPAA standard transaction 835) and claims status inquiry (HIPAA standard transaction 834).

Model I



Properties

- NEHEN includes 42 member systems representing payers and providers, some owning a share in the NEHEN system itself.
- Patients may not access data through NEHEN.
- NEHEN is a "heartless" system in that there is no central data repository, and thus, the system of data exchange is very similar to faxing information between 2 individuals. Individuals may store and provide the data, but the fax machine fails to store any data independently or deposit the data in a central location. This avoids computer "hacking."
- NEHEN is HIPAA compliant (e.g., currently compliant with the HIPAA privacy and EDI rules).
- The private software licensed out by NEHEN handles the routing and delivery of information and is available at every member site.
- NEHEN member systems are responsible for creating transactions according to the national standards.
- No self-insured employer-sponsored group health plans are members of NEHEN at present.

Data Transmission

- The specific information available to NEHEN members is determined by a set of authorized questions which the system is empowered to answer through data searches. These questions are predetermined by the members.

- Data travels through the NEHEN gateway in both directions. The members (providers and payers) never send data directly between one another. The gateways retrieve and send data among the member systems and are primarily responsible for translating all information into a universal format. There is no central storage. An audit trail of questions, however, may be generated by holders of data.
- The Payer's gateway translates the information into a standard data format called under HIPAA the "271" format.[82] The Provider's gateway receives data and distributes it to the appropriate provider.
- Each provider owns a data warehouse, which in the case of NEHEN, contains administrative data. A decentralized model could also be used for clinical data exchange.
- Member entities that participate in NEHEN include Partners Healthcare System, Inc., CareGroup, Inc., Lifespan, Harvard Pilgrim Health Care, Inc., and Tufts Associated Health Plans, Inc.
- NEHEN is capable of handling Medicaid and Medicare financial data.

Recognized Transactions

- HIPAA Transactions 270/271 (Benefits/Eligibility)
- HIPAA Transaction 278 (Referral/Authorization)
- HIPAA Transaction 837 (Claims)
- HIPAA Transaction 835 (Remittance)
- HIPAA Transaction 834 (Claims status inquiry)

Example of a Transaction

1. Physician requests information on his/her computer terminal.
2. The information passes over the internet through the Provider Gateway which, in turn, communicates with the Payer Gateway.
3. The Payer Gateway retrieves information from the warehouse and translates it into the standard HIPAA 271 transaction format.
4. The Payer Gateway sends back the requested information through the Provider Gateway, which routes it back to the requesting provider.

Other Issues Re: Model I

- Information transmitted in NEHEN cannot be aggregated, which makes the system inadequate for quality improvement and research.
- Data in the system includes addresses, co-payment and coinsurance information.
- There is no coordination of data regarding an individual's general eligibility for benefits and the specific benefits to which the individual

[82] This is the HIPAA standard transaction number for data transactions involving eligibility of individuals for benefits.

may be entitled under his/her health plan in the NEHEN system (in other words, a provider may not be able to ascertain whether a particular service is covered for his/her patient).

MODEL II. DECENTRALIZED CLINICAL DATA EXCHANGE

Example: Santa Barbara County Care Data Exchange ("SBCCDE")

Formed in 1998, the SBCCDE offers an excellent example of a decentralized clinical data exchange system. The goal of SBCCDE is to improve the quality, efficiency, and safety of health care by making available both inter and intra organizational patient specific information at the point of care.[83] The exchange is funded by a $10 million grant from the California HealthCare Foundation and connects ten health care organizations assembled in four Care Data Alliances.[84] The four Care Data Alliances consist of: (1) The Lompoc Valley Community HealthCare Organization, which includes a 75 bed acute-care hospital; (2) the Mid-Coast Medical Care IPA, an independent physicians' association of 24 primary-care physicians and 35 specialists managed by a third party administrator; (3) the Sansum Santa Barbara Health Foundation, a primary and multi-specialty practice of 16 facilities and 200 physicians; and (4) the Santa Barbara Regional Health Authority, a county organized health system administering several publicly funded programs, including Medi-Cal.[85] Each care alliance establishes unique data sharing goals based on their individual members' interests.[86] The LompacValley alliance, for example, shares laboratory, radiology, and pharmacy records; whereas the Santa Barbara Regional Health Authority shares data concerning eligibility verification, online referrals or authorizations, and HEDIS reporting.[87]

The SBCCDE focuses on an institution-to-consumer or institution-to-physician exchange of data.[88] An authorized physician or patient, via a web-based interface, may view clinical and administrative results (e.g., patient demographics, medical records, medical transcription, eligibility and referral information, and laboratory, radiology, and pharmacy data) from hospitals, payers, or labs that store information in a central warehouse.[89]

The SBCCDE shares many of NEHEN's qualities, with a few exceptions. For example, the SBCCDE utilizes a Master Patient Index ("MPI") which, similar to an Internet search engine, identifies the specific data warehouse storing the desired information.[90] Once the MPI identifies the proper data warehouse, the Clinical Information Architecture ("CIA") extracts the information and displays it on the users

---

[83] California HealthCare Foundation, *Santa Barbara County Care Data Exchange Fact Sheet* (2003) *available at* www.chcf.org/documents/ihealth/SantaBarbaraFSWeb.pdf.
[84] *Id*. at 1.
[85] *Id.* at 4.
[86] *Id*. at 2.
[87] *Id.*
[88] *See* Brailer, *supra* n. 9.
[89] *Id.*
[90] *Id.*

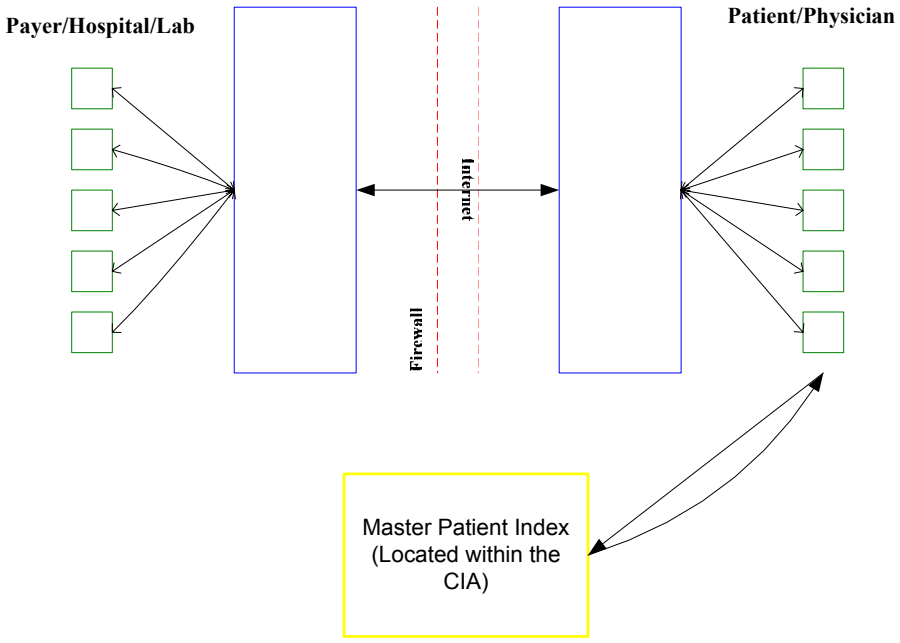
computer screen.[91] No permanent storage of this information occurs in the CIA, however, audit trails exist that track the various information requests occurring over time.

The CIA complies with both HIPAA as well as California's stricter Medicaid privacy regulations.[92] Other security measures include rules for authentication, informed consent, data holder overrides, and auditing options.[93] In addition, the SBCCDE's central governance reviews urgent requests for data and investigates complaints concerning improper data use.[94] Consumers serve a role in protecting privacy as well. A patient, for instance, may restrict access to personal information held by a particular institution or conduct audits to investigate any suspicious requests for data.[95]

The diagram and bullet points set forth below summarize a decentralized system of clinical data exchange, using the SBCCDE as an example.

Model II

Central Infrastructure Architecture (CIA)



[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*
[95] *Id.*

Properties

- There are 10 health care organizations assembled in 4 Care Data Alliances.
- Data is located via a MPI, which functions much like a "google" or "yahoo" search engine. Once the specific data warehouse is located containing the desired information, the system retrieves the information.
- Like Model I, all data is transitory in nature; no data is stored.

Data Transmission

- The system displays data following transit through the appropriate gateway. Data is never sent directly and providers never directly communicate with a warehouse.
- Gateways can retrieve and send data, but not store it.
- The Payer Gateway (located in the CIA) translates information from warehouse into common format.
- The Provider Gateway (located in the CIA) receives data and distributes to appropriate provider.
- Data is temporal, not permanent.
- Data can not be aggregated.
- This model uses a probabilistic method of data retrieval. For example, a patient is identified based on a series of characteristics (name, address, age, zip code), called unique patient identifiers. There is a 99.9% chance of identifying the correct patient.
- The system of data warehouses is similar to Model I, with the only difference being the MPI, which identifies the particular warehouse that contains the relevant information.

Example of a Transaction

1. Provider queries the MPI to locate relevant data.
2. MPI provides provider with the appropriate data warehouse containing the information.
3. The provider sends query to the warehouse(s) identified by the MPI.
4. The information is then sent through the gateway much like it does in the NEHEN model.

MODEL III: CENTRALIZED DATA EXCHANGE SYSTEM

Example: Medicare Health Care Quality Improvement Program ("MHCQIP")

Medicare's Quality Improvement Program is an example of a centralized data system of data exchange whose purpose is to aid in health care quality improvement efforts. To monitor and improve care delivered to Medicare beneficiaries in each state,

The Centers for Medicare and Medicaid Services (CMS) contract with not-for-profit organizations called Quality Improvement Organizations (QIOs).[96] QIOs evolved from Experimental Medical Care Review Organizations (EMCROs), which are charged with reviewing the quality of inpatient and ambulatory care services, and Peer Review Organizations (PROs), which are responsible for conducting utilization review, hospital admissions, and medical necessity determinations under Medicare.[97] The purpose of the QIO is to broaden data collection capabilities under federal insurance programs.

QIOs are responsible for collecting and processing electronic data from hospitals specific to four hospital based topics: acute myocardial infarction, heart failure, pneumonia, and surgical infection.[98] Participation in the program is voluntary; however, real time feedback reports, comparison data on statewide performance benchmarks, clinical and analytical tools, and information exchange all serve as incentives for hospitals to participate.[99] The Bush administration has expressed interest in expanding the QIO program beyond hospitals to include nursing homes, home health services, and physicians' offices.[100]

QIOs collect information via a CMS authorized website called QNet.[101] QNet is the only approved method for transferring data to a QIO.[102] Information may be transferred to a QIO through a vendor, disc, or hardcopy.[103] Once this transfer is complete, the QIO deposits the information into a central data warehouse, where it may be used for analysis by CMS or other health care providers.[104] Providers may access the data warehouse via CART, an application developed by CMS to provide data feedback reports aimed at improving quality.[105] An example of a data feedback report would be a chart comparing the timing of a hospital's antibiotic administration in the case of a patient with pneumonia against national, regional, state-level, and other institutional performance standards.[106]

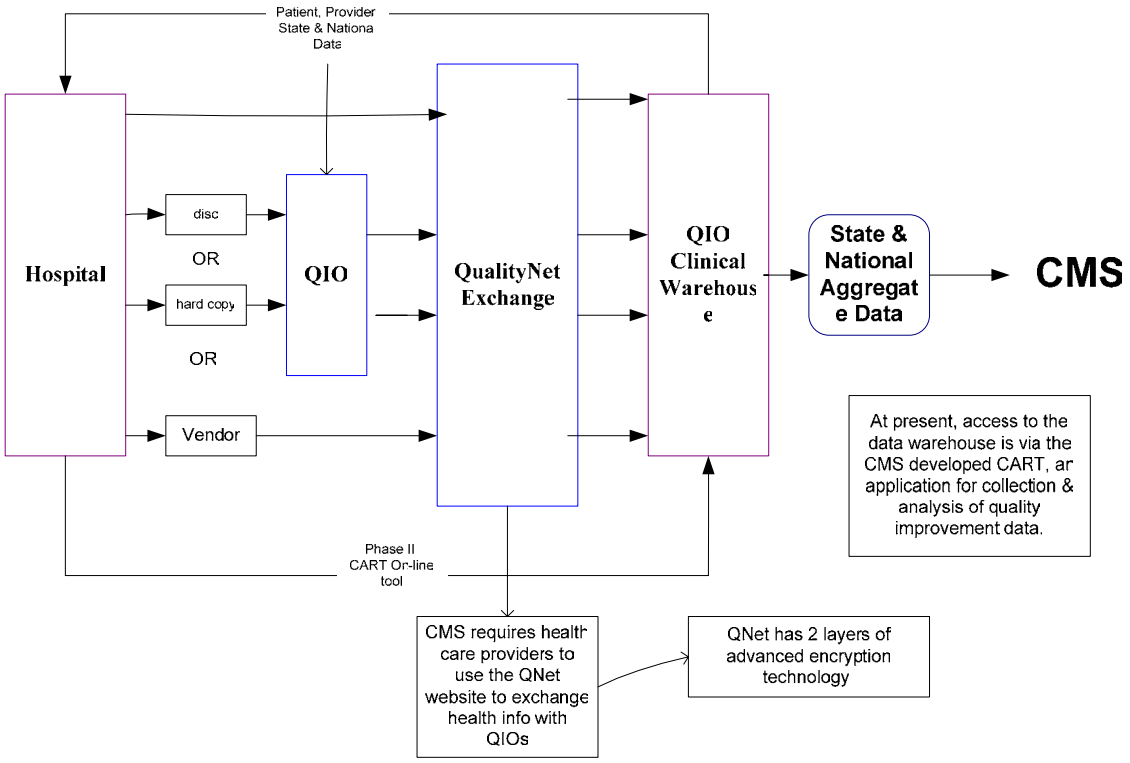
---

[96] *See* Lisa Sprague, "Contracting for Quality: Medicare's Quality Improvement Organizations" National Health Policy Forum, Issue Brief 774, at 2 (June 3, 2002) *available at* www.nhpf.org.
[97] *Id.* at 5.
[98] Quality Improvement Organization Manual, Chapter 14, *available at*: http://www.cms.hhs.gov/manuals/110_qio/qio110index.asp.
[99] *Id.*
[100] Sprague at 3, *supra* n. 96. Moreover, there has been increased interest in the use of claims data to improve quality through physician profiling. For instance, on Dec. 10, 2004, the staff of the Medicare Payment Advisory Commission (MedPAC) made public a draft recommendation that will be voted on by the Commission early next year that HHS should use Medicare claims data to measure the use of health care resources by individual physicians in the fee-for-service part of the program to compare the use of tests and procedures by individual doctors. Calling this type of provider profiling "resource use management", MedPAC also recommends that Congress direct HHS to carry out this type of measurement.
[101] Quality Net Exchange, Hospital Data Collection *available at*: http://www.qnetexchange.org/public/welcome/index.jsp?tabID=4&txt.
[102] *Id.*
[103] Quality Net Exchange, Data Exchange Process *available at:* http://www.qnetexchange.org/public/newcart/docs/pdf/data_exchange_process.pdf.
[104] *Id*.
[105] Chapter 14, *supra* n. 98.
[106] CMS Abstraction & Reporting Tool, Centers for Medicare and Medicaid Services *available at*: http://www.qnetexchange.org/public/newcart/index.jsp.

At the present time, QIOs are the only entities which measure and aggregate quality data on a hospital level.[107] The potential for QIOs to capture data necessary to measure large-scale changes in quality can be seen in a recent study which concluded that QIO data were able to demonstrate significant improvements in inpatient hospital care over a two-year time period.[108] Hospital-level data generally are not published under existing QIO agreements with hospitals;[109] however, CMS is currently conducting pilot studies of reporting systems which would provide for hospital-specific data reporting.[110] Other organizations conducting hospital quality improvement initiatives include the Agency for Healthcare Research and Quality (AHRQ) and the National Committee for Quality Assurance (NCQA).[111]

The following figure depicts the QIO system.

Model III[112]



[107] *See* David C. Hsia, "Medicare Quality Improvement – Bad Apples or Bad Systems" 289 (No. 3) JAMA 354 (Jan. 15, 2003) (*citing* Stephen F. Jencks, "Change in the Quality of Care Delivered to Medicare Beneficiaries" 1998-1999 to 2000-2001, 289 (No.3) JAMA 305 (Jan. 15, 2003)).
[108] *Id.*
[109] *Id.*
[110] Sprague at 10, *supra* n. 96.
[111] Hsia at 355, *supra* n. 107.
[112] Quality Net Exchange, Data Exchange Process *available at*: http://www.qnetexchange.org/public/newcart/docs/pdf/data_exchange_process.pdf.

Properties

- CMS requires providers that participate in Medicaid (primarily hospitals) to transmit quality related information to QIOs, which then deposit the information into a central repository.
- Information is transmitted to the QIO through a vendor, disc or hardcopy.
- Aggregate data in the central warehouse is permanent, allowing for research such as provider or patient profiling.
- Providers may access the central warehouse using a software application called CART, which provides data feedback reports for quality related purposes.
- Potential for research and capacity for permanent data storage makes this the most germane model for quality improvement purposes.

Data Transmission

- Providers (currently mainly hospitals) contract with QIOs and use the QNet website to transmit data to the QIO.
- QIOs translate the data into a common format and deposit it into the central warehouse.
- Providers use CART to retrieve information from the data warehouse in the form of data feed back reports. A typical report could be a chart comparing the timing of antibiotic administration for pneumonia on national, state, and institutional levels.
- Warehouse contains CMS-required health data collected from hospitals participating in Medicare.
- Warehouse may be accessed by CMS or provider and used for quality improvement.

Example of a Transaction

1. Either independently or through a vendor, providers transmit health information to the QIO via the QNet website.
2. QNet translates information into a common format and delivers it to the CMS central warehouse.
3. Providers use CART, a CMS authorized software, to retrieve information from the warehouse for quality analysis (e.g. data feedback reports).

ADDITIONAL EXAMPLES OF DECENTRALIZED AND CENTRALIZED MODELS

Our research and discussions uncovered numerous emerging examples of each of the three principal models:

Decentralized Models

1. Indiana Health Information Exchange Inc. (Regenstrief Medical Records System)

This system of data exchange links a community medical records system to numerous health care entities participating in the network. Participating entities include emergency rooms, HMOs, local and state health departments, pharmacies, and public school clinics. The system exchanges various types of data, including the number of ER visits, inpatient lab results, hospitalization discharge summaries, medication profiles, and radiology images. Data is held by the participants in individual databases, separate from all other databases. Each database utilizes a "global patient registry" and a "global doctor registry" to link patient data to an individual member. The system is used by both payers and providers and includes no patient access.

2. MA Share

This system is a regional collaborative operated by the Massachusetts Health Data Consortium. It is identical to the NEHEN model, except it shares clinical rather than administrative data.

3. Patient Safety Institute (PSI)

Users of this system include three hospitals in the Seattle area. The system focuses on allowing health care providers access to medical information at the point of clinical interaction. The patient authorizes data sharing and retains the option to provide supplemental information. Similar to Models I and II, PSI does not store clinical information, but gathers data from individual databases. Physicians access patient data, which is updated each time a patient visits a participating clinic or hospital. Both physicians and patients can view clinical information from any location.

4. Minnesota Center for HealthCare Electronic Commerce and the Minnesota Health Data Institute

Users of this system include major health systems, payers, and government entities in Minnesota. The system exchanges public data with state public health departments via e-mail and file transfers. The information that is exchanged includes lab reports, birth and death reports, reportable events, disease registries and trauma registries.

5. Health Bridge (Cincinnati Area)

Provides electronic access to 17 regional hospitals via a community wide messaging platform that enables physicians and their staff to use an electronic in-

box to view radiology, lab and transcription data regardless of where the data originated. The system serves only as a data exchange, with no centralized database.

6. California Information Exchange (CALINX)

CALINX exchanges patient eligibility, enrollment, member ID cards, encounters, clinical lab results, and pharmacy information. The goal is to link employers, health plans, and physician groups in the exchange of data.

Centralized Models

1. Community Wide Health Management Information System (CHMIS)

A CHMIS collects and stores data in a central depository for quality improvement purposes.[113] Its aim is to create not simply a system of information sharing, but also data repositories that could measure the cost and quality of competing providers in the community.[114] The initiative began in seven states: Minnesota, Iowa, Ohio, Vermont, Washington State, New York, and Tennessee.[115] Some initiatives were helped by state legislation mandating the maintenance of state wide databases.[116] CHMISes failed because competitors felt uneasy about sharing information and community wide data sharing proved too expensive when compared with less expensive inter-organizational systems of data exchange.[117]

2. North Carolina Healthcare Information and Communication Alliance (NCHICA)

NCHICA stores emergency department data in a centralized location. The central depository contains information concerning patients either treated in the emergency room or treated and then subsequently admitted into the hospital. Data is accepted in whatever format the provider finds easiest and then translated into the CDC's Data Elements for Emergency Department Systems standard. Information includes clinical data, information specific to emergency rooms, such as admitting diagnosis, patient ID data, and procedure and result data.

3. The Foundation for Health Care Quality and the Community Health Information Technology Alliance (CHITA) (Electrnic Laboratory Based Reporting System (ELBRS)

[113] *See* Paul Starr, "Smart Technology Stunted Policy Developing Health Information Network" 13 Health Affairs 91, 96-103 (May/June 1997).
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.*

The Foundation for Health Care Quality (FHCQ) is a Seattle based non-profit founded in 1988. It allows the Washington State Department of Health to electronically send lab test results, which include identifiable patient data, from private sector clinical labs to the state health agency. From the state health agency, the data is sent to the local health agency in the county the patient resides.

CHITA is a member-driven alliance of healthcare and public private technical organizations operated under the non-profit FHCQ and governed by a Board composed of representatives from member organizations. Its goal is to expand and enhance the use of electronic commerce in the healthcare industry. It is open to all organizations in healthcare and technology, with a focus on the Pacific Northwest.

APPENDIX B

Legal Environment for Emerging Information Systems and Implications for Access to Quality and Disparities Data

Meeting Participants (October 26, 2004)

David Abelman
Assistant Vice President/
Associate General Counsel
Tufts Health Plan

Nicholas Augustinos
Vice President of the Care Data Exchange Group

Bernadette Broccolo
Partner
McDermott Will & Emery LLP

Katherine Brown
Managing Director, Disclosure Project
National Partnership for Women and Families

Andrew Chang
Director
Center for Patient Safety Research
Joint Commission on Accreditation of Healthcare Organizations

Almeta E. Cooper
General Counsel
Ohio State Medical Association

Gregory J. DeBor
Partner, Global Health Solutions
Computer Sciences Corporation

Joyce Dubow
Associate Director
Public Policy Institute, AARP

Bruce Merlin Fried
Partner
Sonnenschein Nath & Rosenthal

Roosevelt Hairston, Jr.,
Office of General Counsel
Children's Hospital of Philadelphia

Steve Hitov
National Health Law Program

Bill Kramer
Deputy Chief Legal Officer
Aetna US Healthcare

Tom Perez
Assistant Professor of Law
University of Maryland School of Law

David Szabo
Partner
Nutter, McClennen & Fish, LLP
World Trade Center West

Linda Tiano
Senior Vice President & General Counsel
Wellchoice, Inc.

Diane E. Thompson
Senior Vice President, Programs
FasterCures
The Center for Accelerating Medical Solutions

Steve Wetzel (invited, but did not attend)
Executive Director
Consumer Purchaser Disclosure Project

Cindy Wisner
Assistant General Counsel
Trinity Health

Bruce Wolff
Manatt, Phelps & Phillips

The Robert Wood Johnson Foundation

Anne Weiss
RWJ Project Officer

The Department of Health and Human Services

Jodi Daniel
Office of the General Counsel

Centers for Medicare and Medicaid Services

Trent Haywood, MD
Acting Deputy Chief Medical Officer
Acting Director
Quality Measurement and Health Assessment Group

Agency for Healthcare Research and Quality

Carolyn Clancy
Director

Scott Young

Mike Fizmaurice

Larry T. Patton
Senior Advisor to the Director

Office of Civil Rights

Jeff Zelmanow
Privacy Analyst

Office of the National Coordinator for Health Information Technology (ONC)

Lori Evans
Senior Advisor

Office of the Assistant Secretary for Planning and Evaluation

Jennie Harvell
Senior Policy Analyst
Division of Disability, Aging & Long-Term Care Policy

Helga E. Rippen, MD, PhD
Deputy Senior Advisor
National Health Information Infrastructure

George Washington University Department of Health Policy

Sara Rosenbaum
Chair/ Hirsh Professor of Law and Health Policy

Phyllis Borzi
Research Professor

Bruce Siegel, MD
Director
Urgent Matters

Taylor Burke
Assistant Research Professor

Lee Repasch
Research Scientist

John F. Benevelli
JD/MPH Candidate

APPENDIX C

Review of Literature

I. INTRODUCTION

The Center for Health Research and Policy at the George Washington University received a twelve-month grant from the Robert Wood Johnson Foundation to examine (1) the legal landscape surrounding the use of health information used to improve health care quality and to narrow racial disparities in the delivery of health services, and (2) how this landscape may need to be re-conceptualized to support advances in health information, while concurrently protecting patients' privacy in an environment consisting of interoperable systems of electronic data exchange. In conjunction with the grant, this review of literature examines scholarship concerning two architectural models of health information systems, the recent Department of Health & Human Services ("HHS") initiative to create a National Health Information Infrastructure, and the legal issues surrounding the sharing and collecting of health information. The review also examines scholarship discussing racial and ethnic disparities in the delivery of health care.

Specifically, literature in sections II and III discuss de-centralized and centralized data exchange systems. These articles are found in peer review journals involving health policy and law, including Health Affairs, American Journal of Law and Medicine, Journal of the American Medical Association, and The Journal of the American Medical Informatics Association. These three sections also consider articles collected from the websites of the California Health Care Foundation, The Commonwealth Fund, Regenstrief Institute, CareScience, Health Privacy Project, The National Health Policy Forum, and the E-Health Initiative. Section IV discusses the recent report by the Department of Health and Human Services promoting a National Health Information Infrastructure, as well as scholarship influencing and commenting on the initiative. Section V examines law review articles discussing the legal issues surrounding the sharing and collecting of health data. Articles in Section VI discuss racial and ethnic disparities in the U.S. health care system, gathered from both WESTLAW and peer review journals. Finally, articles in section VII discuss various topics such as the use of health technology among physicians, the impact of data exchange on quality improvement, and the use of electronic medical records.

II. DE-CENTRALIZED DATA EXCHANGE

A de-centralized data exchange allows authorized health care providers and payers to exchange administrative and clinical health information. Data is not stored in a single location, but remains with individual data holders. Some de-centralized systems use a Master Patient Index to locate data. The literature in this section provides excellent descriptions of the technical design of de-centralized systems. One area that the literature does not appear to address is the financial sustainability of these various models of data exchange. The Santa Barbara County Data Exchange ("SBCDE"), for instance, is

currently funded by CareScience, and experts believe that it is not a sustainable business model. More scholarship is needed examining the different issues – both legal and financial – affecting sustainable versus non-sustainable models. Such research would inform incentives motivating investment in health IT and reflect critically on the legal barriers to implementing such systems, since legal issues may vary depending on the model in question.

More research also needs to be conducted concerning whether these de-centralized systems can be used to improve quality. Are decentralized systems inherently incapable of quality improvement since they lack a central data depository? Can de-centralized systems evolve to aggregate data? What are the financial incentives needed to expedite this evolution? What legal issues are implicated in a de-centralized system that aggregates data as opposed to one that does not? Answers to these questions are essential to a full examination of the issues surrounding the various architectural models of data exchange.

David Brailer's *Moving Toward Electronic Health Information Exchange: Interim Report on the Santa Barbara County Data Exchange* and The Regenstrief Institute's *Design and Implementation of the Indianapolis Network for Patient Care and Research* provide excellent descriptions of two de-centralized systems. This section also includes The California HealthCare Foundation's report concerning probabilistic patient data matching software, often required in systems utilizing a Master Patient Index.

The SBCDE makes available inter and intra organizational patient specific clinical information at the point of care. The exchange is funded by a $10 million grant and connects ten health care organizations assembled in four Care Data Alliances. David Brailer's report discuses the SBCDE's structure, specifically its organization and operation, as well as the technology behind data integration, security, user access, and identity correlation. The report also discusses initiatives undertaken by Santa Barbara to assess the financial and quality improvement benefits of the system. The report concludes with a chapter concerning the implications for public policy surrounding interoperability and health information exchange. For a brief overview of the SBCDE, refer to the SBCDE Fact Sheet or the slide presentation authored by Ronald A. Paulus, President of CareScience.

The Regenstrief Institute's article focuses on the Indianapolis Network for Patient Care and Research ("INPCR") – a health care information network developed in Indianapolis that connects a community medical record system to three emergency departments, fifty community pharmacies, ten clinics, four HMOs, and twelve homeless care sites. The INPCR tests the feasibility of connecting providers across organizational boundaries and measures the benefits of the network. Co-authored by Clement J. McDonald, the Regenstrief article examines the design of the network, as well as the barriers and challenges of implementation. Specifically, in the barriers and challenges section, the article discusses privacy and security related to system access, patient identifiers, and the codes the network utilizes to represent diagnoses and prescription drugs.

De-centralized systems of data exchange often use probabilistic methods of patient identifying that match data from multiple data warehouses to patient records held by providers. A comprehensive patient profile is a pre-requisite to accurate matching. The California HealthCare Foundation published a report discussing patient matching entitled, *Patient Data Matching Software: A Buyer's Guide for the Budget Conscious*. The report limits itself to addressing the needs of ambulatory provider organizations that intend to create clinical data repositories to measure and improve quality, specifically discussing the benefits of using certain patient matching software over others.

III. CENTRALIZED DATA EXCHANGE

A centralized data exchange collects and aggregates data in a central location. Quality improvement and aggregation of data are best served by centralized systems of data exchange. The literature in this section focuses on Quality Improvement Organizations ("QIOs") and the CHIN/CHMIS movement of the 1990s. The QIO initiative, according to some scholars, stands as the nations premiere system for quality improvement. In conducting this literature review, we found a need for more scholarship discussing incentives promoting centralized systems in the private sector. More scholarship examining why CHMISes failed in the 1990s would be helpful in this regard. Such research should consider whether or not the present environment would be more amicable to centralized data systems then the environment of the 1990s.

Quality Improvement Organizations ("QIOs")

QIOs are not-for-profit organizations tasked with improving and measuring quality in the Medicare system. The Centers for Medicare and Medicaid Services ("CMS") require QIOs to collect and process electronic data from hospitals participating in Medicare. Through a CMS authorized website, QIOs deposit this data into a central warehouse to be used later for quality measurement and analyses.

Three articles listed below discuss the QIO program and its affect on quality. First, Lisa Sprague's *Contracting for Quality: Medicare's Quality Improvement Organizations*, examines the role of QIOs in quality improvement. The article explores the historical background of QIOs, the evolution of QIOs, and some current projects of QIOs. Second, David C. Hsia's *Medicare Quality Improvement – Bad Apples or Bad Systems?* posits that QIOs serve as the nation's primary system for quality improvement. Hsia identifies other initiatives aimed at improving quality as well, specifically those spearheaded by the National Committee for Quality Assurance and the Agency for Healthcare Research and Quality. Hsia also discusses several ways to build on the successes of the QIO program. Third, Stephen Jencks's *Change in the Quality of Care Delivered to Medicare Beneficiaries* illustrates the success of QIOs by providing data that tracks national and state level performance changes spurred by the QIO initiative. Finally, the CMS website provides a good technical overview of the QIO program.

CHINs & CHMISes

Paul Starr's *Smart Technology, Stunted Policy: Developing Health Information Networks* presents an excellent analysis of the rise and fall of CHINs and CHMISes. Conceived in the early 1990s, CHMISes and CHINs stand as two early models that exchanged health information between health care organizations under different ownership. A CHMIS (Community Health Management Information System) collects and stores data in a central depository for quality improvement purposes. The CHIN (Community Health Information Network) still exists today in a variety of incarnations, but may lack the commitment for quality improvement inherent in a CHMIS. Some CHINs, for example, do not store information in a central data depository, but exist solely as an information sharing system. CHINs and CHMISes were experimented with in the 1990s, but failed in their endeavor for a variety of reasons. Some of these reasons, according to Starr, include the fact that competitors felt uneasy about sharing information and community wide information sharing proved expensive and unnecessary when compared with less expensive inter-organizational systems of data exchange.

IV. THE DEPARTMENT OF HEALTH & HUMAN SERVICES – NATIONAL HEALTH INFORMATION INFRASTRUCTURE

The Department of Health and Human Services (HHS) recently issued *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care*, outlining a plan that guides the implementation of health IT in both the public and private sectors. The goal of the initiative is to improve the quality of health care, by reducing the amount of medical errors, preventing unnecessary treatments, and decreasing the amount of variations in care. Two precursors to the HHS report are also included in this section, *Achieving Electronic Connectivity in Healthcare, A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders* by the Markle Foundation and *Information for Health: A Strategy for Building the National Health Information Infrastructure*, issued by the HHS in 2001.

A recent Markle Foundation study – conducted on request from David Brailer, the National Health Technology Coordinator – identifies necessary steps towards implementing a fully integrated health information network. The January 2005 report specifically focuses on the possible cost savings of an interoperable data exchange system. The report was published in conjunction with an article in Health Affairs, also included in this section.

The most recent HHS report identifies four main goals: (1) Inform Clinical Practice: This goal endeavors to bring electronic health records directly into clinical practice by incentivizing the adoption of health IT by reducing financial risk, especially in rural or underserved populations. (2) Interconnect Clinicians: This goal focuses on enabling physicians to access information at the point of care by coordinating federal health information systems, developing local oversight over health data exchange, and developing a national health information network. (3) Personalize Care: This goal seeks to develop consumer-centric information to help individuals manage their own health decisions. (4) Improve Population Health: This goal furthers the reporting of important

information to public health officials. The report does not, however, set forth the legal barriers to accomplishing these objectives. For a discussion of the legal barriers from the government's perspective, see the GAO report referenced in the Legal Issues section of this review.

To promote the National Health Information Infrastructure, the Agency for Healthcare Research and Quality (AHRQ) recently awarded $139 million in contracts and grants to promote the use of health IT. Specifically, AHRQ awarded $25 million in contracts to five states to facilitate information sharing and $96 million in grants to 38 states and communities to support health IT infrastructures and promote data sharing. The research resulting from AHRQ funding will no doubt provide valuable information informing the creation of a national health information infrastructure. For a detailed explanation of the AHRQ project, see the AHRQ Fact Sheet listed below.

V. LEGAL ISSUES IMPLICATED IN SHARING & COLLECTING HEALTH INFORMATION

The literature in this section analyzes federal and state laws relevant to the sharing and collecting of health information. Many of these laws specifically address health information privacy, such as HIPAA or the variety of state privacy protection statutes. Other laws are not crafted specifically to protect privacy, but nonetheless still affect the exchange of health data. In conducting our research, we found a need for more scholarship analyzing these non-privacy related laws. For instance, as electronic medical records (EMRs) and health data exchange systems become more common, a new standard of care may emerge in medical malpractice cases. Additionally, issues of ownership and culpability arise when a data system is funded by a larger entity, or when data systems aggregate data rather than store it in various data warehouses. Legal scholars must endeavor to keep track of these evolving legal issues as technology quickly marches forward.

Privacy Laws

State Law

The articles below agree that a patchwork of privacy protections currently exist in the states. States vary greatly in the level of privacy protections because states are free to enact more restrictive protections over and above federal regulation. For example, the Health Privacy Project's report *The State of Health Privacy* writes that Florida alone contains more than 60 privacy laws, and it is by no means unique. According to James G. Hodge's *Health Information Privacy and the Public Health*, most states have enacted laws similar to the federal Privacy Act, and a few (e.g., CA, RI, MD, MT, and WA) have passed additional privacy protections. State privacy laws regulate specific data recipients, specific conditions and diseases, or particular data sources. State public health laws, insurance regulations, and licensure requirements also implicate health privacy. Other articles addressing state health privacy laws include *Privacy Concerns in the Health Care Industry*, by Lisa Sottto, *National Health Information Privacy and the New*

Federalism, by James G. Hodge, *Health Information Privacy: Can Congress Protect Confidential Medical Inforamtion in the "Information Age"?*, by Patricia I. Carter. *Synopsis of State Case & Statutory Law (Relevant Access & Disclosure to Medical Records* by the Editorial Staff of the Yale Journal of Health & Policy, and *The Privacy Paradox*, by Eric Jorstad.

Federal Law

Enacted in December 2000, HIPAA provides comprehensive protection of personal health information. HIPAA protects most individually identifiable health information created or received by covered entities. The Health Privacy Project provides an excellent summary of HIPAA, entitled *Summary of the HIPAA Privacy Rule*. James G. Hodge's *Health Information Privacy and the Public Health* also discusses HIPAA and its relation to public health. The Gramm-Leach-Bliley Act implicates health privacy as well, prohibiting financial institutions – including insurers – from disclosing non-public personal information unless the institution gives prior notice. Lisa J. Sotto's *Privacy Concerns in the Health Care Industry* briefly discusses the Gramm-Leach-Bliley Act and its effect on health information privacy.

Other federal laws implicating health privacy include the Freedom of Information Act, The Privacy Act of 1974, the E-Government Act, and the Public Health Service Act. These laws protect information held by the federal government and complying with HIPAA, in some instances, also satisfy their requirements. In *Whalen v. Roe*, the Supreme Court addressed the issue of whether constitutional protections under the 14th Amendment extend to the collection, storage, and dissemination of health information. Articles discussing *Whalen* include, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, by Patricia I. Carter, *The Nationalization of Health Information Privacy Protections*, by Lawrence Gostin, *Protecting Health Information Privacy: The Case for Self –Regulation of Electronically Held Medical Records*, by Catherine Louisa Glenn, and *Access and Aggregation, Public Records, Privacy, and the Constitution* by Daniel J. Solove.

Non-Privacy Laws

Collecting and sharing health information implicate a number of laws and legal issues not specifically intended to protect health information. The GAO's recently published report *HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption* identifies legal barriers resulting from laws related to fraud and abuse, antitrust, federal income tax, intellectual property, liability/malpractice, and state licensing. The Stark Law, for instance, may impede physicians from receiving resources from providers to implement health IT, since referrals subsequently made to that provider may violate the law. Anti-kickback laws may also be implicated in a similar manner. Regards to intellectual property, hospitals and other entities may be reluctant to invest in health IT in the absence of adequate copyright protection in fear they will be unable to recoup their investments. Pamela Samuelson's *Privacy as Intellectual Property?* and

Richard S. Murphy's *Property Rights in Personal Information: An Economic Defense of Privacy*, further address the issue of intellectual property and health information.

VI. RACIAL & ETHNIC DISPARITIES IN THE DELIVERY OF HEALTH CARE

The literature in this section agrees racial and ethnic disparities abound in the delivery of health care. The 2002 Institute of Medicine report, *Unequal Treatment*, documents serious and pervasive disparities in the provision of health care to racial and ethnic minorities. Marsha Lillie-Blanton's article *Site of Medical Care: Do Racial and Ethinic Differences Persist*, states that although these disparities are well documented, the underlying causes behind them are not well understood. Common explanations, according to Lillie-Blanton, include characteristics of the patient or provider, the variations in the primary sources of care used by whites and minorities, and structural and institutional factors, such as patient-provider relationships, referral networks, and the availability of resources.

General agreement exists that data collection efforts are key to solving racial and ethnic disparities. The Commonwealth Fund published an excellent report entitled *Racial, Ethnic, and Primary Language Data Collection in the Health Care System: An Assessment of Federal Policies and Practices*, addressing racial and ethnic data collection implemented on the federal level. Four major findings emerge from the report. First, collection and reporting of racial and ethnic data is legal under Title VI of the Civil Rights Act of 1964. Second, federal policies are increasingly encouraging the collection of racial and ethnic data. Third, racial and ethnic data are important to providing quality of care for all Americans. And finally, data requirements and methods of collection vary across federal agencies. The report also sets forth recommendations for improving racial and ethnic data collection on the federal level, discusses the legal basis for the collection of racial and ethnic data, lists the federal policies guiding the collection of racial and ethnic data, and provides arguments supporting the collection of racial and ethnic data.

Kevin Fiscella's article *Within Our Reach: Equality in Health Care Quality* discusses a number of public and private quality improvement initiatives focused on racial and ethnic disparities. The Commonwealth Fund and the Health Resources and Services Administration (HRSA) is developing a "report card" to rate the quality of care afforded to racial and ethnic minorities on the health plan level. An article by David R. Nerenz cited below discusses this joint initiative. The National Committee on Quality Assurance ("NCQA") recently assembled a Cultural Expert Panel On Culturally and Linguistically Appropriate Services to address racial disparities in health care. In the private sector, Aetna recently began collecting race and ethnic data to analyze how race and ethnicity affects quality of care. As mentioned above, the federal government has also begun work in this area, primarily targeting the six conditions identified in the HHS Initiative to Eliminate Racial and Ethnic Disparities in Health. In Congress, Senators Frist and Kennedy have introduced bills requiring organizations to collect patient race and ethnic data before receiving HHS funds.

There are a number of areas in need of more research and scholarship informing racial and ethnic disparities and data collection. When racial and ethnic data is collected by a private entity, for example, legal issues differ compared to when the federal or state government collects similar data. Issues involving the standardization of racial and ethnic data also exist. How can inconsistency in the categorization of race and ethnicity be avoided? What standard would improve comparability without inappropriately forcing certain racial groups to be aggregated into others? How can we make sure racial and ethnic data is not used to limit certain minorities' access to health care? Scholars should strive to answer these questions and further the cause of eliminating racial and ethnic disparities from our health care system.

VII. GENERAL

The literature in this section considers a range of issues, including the impact of health data exchange on quality improvement, electronic medical records (EMR), the financial effects and incentives behind implementing health IT, and the use of health IT among physicians.

A recent report by The Health Strategies Consultancy entitled, *Financial Incentives: Innovative Payment for Health Information Technology,* discusses misaligned incentives, noting that parties who pay for health IT are often not the ones who benefit from the technology, and further discusses health IT models that address these misaligned incentives. The cost benefit of implementing electronic medical records is also addressed in the Wang article.

The Commonwealth Fund report, *Information Technologies: When Will They Make it Into Physicians' Black Bags?*, discusses the use of health IT among physicians and barriers to its adoption. The report shows a modest embrace of health IT among physicians. A slight majority of physicians interviewed for the report claim they do use health IT for billing and payment purposes; however the use of health IT diminishes for purposes involving electronic medical records, electronic testing, and the ordering of prescription drugs.

VIII. CONCLUSION

The literature included in this review provides excellent technical descriptions of various data exchange models. With respect to legal issues, substantial literature exists addressing both federal and state privacy protections relevant in health data exchange and sharing. Racial and ethnic disparities in the delivery of health care are also well documented. Although the literature provides a foundation to informing the discussion concerning health information exchange, more work needs to be accomplished. Scholars must continue to identify legal issues apart from federal and state privacy protections. Further, existing legal principles may still endure, but they may need to be recast to fit advances in health information technology. Numerous other questions must also be answered, including: How does emerging technology re-define traditional legal doctrines or create new legal standards? How do legal issues differ dependent on the particular

architectural data exchange model in question? How can data exchange inform the debate concerning the elimination of racial and ethnic disparities? These questions and issues call out for more research and scholarship.

IX. BIBLIOGRAPHY

De-Centralized Health Information Systems

David Brailer, *Moving Toward Electronic Health Information Exchange, Interim Report on the Santa Barbara County Data Exchange* (July 2003) *available at* www.chcf.org/documents/ihealth/SBCCDEInterimReport.pdf.

California HealthCare Foundation, *Santa Barbara County Care Data Exchange Fact Sheet* (2003) *available at* www.chcf.org/documents/ihealth/SantaBarbaraFSWeb.pdf.

Care Data Exchange, Product Brochure, *The Solution to a Patient Centric Real Time Clinical Information within your Enterprise and Across your Community available at* www.carescience.com/healthcare_providers/cde/care_data_exchange.shtml#.

Catherine Frey, *Wisconsin Patient Safety Institute: Striving for Positive Outcomes*, 100 (No. 6) Wis. Med. J. 14 (2001) *available at* http://www.wisconsinmedicalsociety.org/uploads/wmj/100-6-FA-Frey.pdf.

DS Hopkins, *CALINX: A Multi-Stakeholder Statewide Initiative to Improve Healthcare Information Flows*, 14 J. of Healthcare Info. Management 41 (Winter 2000).

LeRoy Jones, Sujansky & Associates, *Patient Data Matching: A Buyers Guide for the Budget Conscious* (Aug. 2004) *available at* www.chcf.org/documents/ihealth/PatientDataMatchingBuyersGuide.pdf.

KS Lassila, *Assessing the Impact of Community Health Information Networks: A Multisite Field Study of the Wisconsin Health Information Network*, 18 Topics in Health Information Management 64 (Nov. 1997).

Thomas Lee, California Health Foundation, Slides, *Santa Barbara County Care Data Exchange* (Nov. 14, 2003) *available at* www.cmwf.org/programs/quality/lee_santabarbaraco_cde.ppt.

Clement McDonald, *The Barriers to a Electronic Medical Records System and How to Overcome Them*, 4 (No.3) J. of the Am. Med. Informatics Ass'n. 213 (May/June 1997) *available at* http://www.pubmedcentral.nih.gov/picrender.fcgi?artid=61236&action=stream&blobtype=pdf.

J. Marc Overhage, Regenstrief Institute for Health Care, Slides, *Indiana Network for Patient Care Overview* (Mar. 2003) *available at* www.connectingcommunitiesprogram.org/profiles/documents.aspx?Section=123&Category=124&Document=214&Page=117.

J. Marc Overhage, Regenstrief Institute for Health Care, *Design and Implementation of the Indianapolis Network for Patient Care and Research*, 83 (No.1) Bull. Med. Libr. Ass'n 213 (Jan. 1995) *available at* www.pubmedcentral.nih.gov/picrender.fcgi?artid=225997&action=stream&blobtype=pdf

Ronald Paulus, Care Science, Slides, *The Santa Barbara County Data Exchange available at* www.ehcca.com/presentations/HIPAA5/paulus.pdf.

EM Stone, *Comprehensive Health Data Systems Spanning the Public Private Divide: The Massachusetts Experience*, 14 (3 Suppl.) Amer. J. of Preventive Med. 40 (Apr. 1998).

Centralized Health Information Systems

Quality Improvement Organizations

Centers for Medicare & Medicaid Services, *Quality Improvement Organizations statement of work available at* http://www.cms.hhs.gov/qio/2.asp.

David C. Hsia, *Medicare Quality Improvement – Bad Apples or Bad Systems*, 289 (No. 3) JAMA 354 (Jan. 15, 2003).

Stephen F. Jencks, *Change in the Quality of Care Delivered to Medicare Beneficiaries, 1998-1999 to 2000-2001*, 289 (No.3) JAMA 305 (Jan. 15, 2003).

Lisa Sprague, National Health Policy Forum, Issue Brief 774, *Contracting for Quality: Medicare's Quality Improvement Organizations* (June 3, 2002) *available at* www.nhpf.org.

CHINs & CHMISes

C. Appleby, *The Trouble with CHINs*, 69 Hospital & Health Networks 42 (May 5, 1995).

RL Davenport, *Technological Considerations in the CHIN Design Process*, 9 Healthcare Information Management 29 (Spring 1995).

E-Health Symposium, Panel Presentation E-Health Symposium, Slides, *Community Health Information Network (CHIN)*, (Apr. 23, 2004).

R. Kennedy, *Building the CHIN Organization*, 9 Healthcare Information Management 21 (Spring 1995).

R. Korpman, *Which CHIN Ownership Model Holds the Promise for Long-Term Success?*, 26 Infocare (Apr. 1994).

Kelly Kwiatkowski, *Linking Personal & Public Health Information: A Vision for Community-Centered Health Information Systems*, MEDINFO (2001).

J. Morrissey, *CHIN Makes Vendors Work Together*, 24 Modern Healthcare 46 (Sept. 5 , 1994).

Fay Cobb Payton & Patricia Flatley Brennan, *How a Community Health Information Network is Really Used*, 42 (No. 12) Communications of the ACM 85 (Dec. 1999) *available at* www.cse.ohio-state.edu/~panda/788_sp00/papers/7b_payton_cacm99.pdf.

JM Petry, *Assessing Your CHIN*, 9 Healthcare Information Management 15 (Spring 1995).

Dr. H. U. Prokosch, World Congress of High Tech Medicine, Slides, *Community Wide Information Networks Steps Toward an Electronic Patient Record* (Jan. 12, 2000) *available at* www.imi.med.uni-erlangen.de/team/download/St_Gallen.pdf.

R. Rubin, *CHIN Overview: When You've Seen One, You've Seen One*, Infocare 22 (Fall 1995).

MJ Stark, *The Iowa CHMIS: Work in Progress*, 19 J. of Ambulatory Care Management 98 (Jan. 1996).

Paul Starr, *Smart Technology, Stunted Policy: Developing Health Information Networks*, 16 (No. 3) Health Affairs 91 (May/June 1997) *available at* http://content.healthaffairs.org/cgi/reprint/16/3/91.pdf.

M. Howard Williams, *Developing a Regional Healthcare Information Network*, 5 (No. 2) IEEE Transactions Info. Tech. in Biomedicine 177 (June 2001) *available at* http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=20003&puNumber=4233.

TK Zinn, *Information Networks – A CHIN Primer*, 15 Health Management Tech. 28 (Feb. 1994).

The Department of Health & Human Services – National Health Information Infrastructure

The Agency for Healthcare Research & Quality, *Health Information Technology Programs Fact Sheet* (Oct. 2004) *available at* http://www.ahrq.gov/research/hitfact.htm.

General Accounting Office, *Health Care: National Strategy Needed to Accelerate the Implementation of Information Technology* (July 14, 2004) *available at* www.gao.gov/new.items/d04947t.pdf.

Connecting for Health, Markle Foundation, *ONCHIT Request for Information – The Collaborative Response* (Jan. 18, 2005), *available at* www.connectingforhealth.org/resources/collaborative_response/collaborative_response.pdf.

Connecting for Health, Markle Foundation, *Achieving Electronic Connectivity in Healthcare, A Preliminary Roadmap from the Nation's Public and Private-Sector Healthcare Leaders* (July 2004) *available at* www.connectingforhealth.org/resources/white_roadmap_072004.pdf.

Tommy G. Thompson and David J. Brailer, *The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care* (July 21, 2004) *available at* www.hhs.gov/onchit/framework/.

U.S. Department of Health and Human Services, *Information for Health: A Strategy for Building the National Health Information Infrastructure* (Nov. 15, 2001) *available at* www.ncvhs.hhs.gov/nhiilayo.pdf.

Jan Walker, *The Value of Health Information Exchange and Interoperability*, Health Affairs Web Exclusive (Jan. 2005), *available at* http://content.healthaffairs.org/cgi/reprint/hlthaff.w5.10v1.

Legal Issues

Barbara Bennett, *Emerging Issues in Electronic Health*, 1245 PLI/Corp 173 (2001).

Patricia Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 Wm. Mitchell L. Rev. 223 (1999).

Angela Choy, Health Privacy Project, *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users* (Nov. 2001) *available at* www.healthprivacy.org/usr_doc/PIP_HPP_HealthPriv_report.pdf.

John R. Christiansen, *When Networks Collide: Managing the Risks Arising From the Interaction of HealthCare and Information Systems*, 11 No. Health Law 10 (1998).

Lisa L. Dahm, *Using DNA Profile as the Unique Patient Identifier in the Community Health Information Network: Legal Implications*, 15 J. Marshall J. Computer & Info. L. 227 (Winter 1997).

Yaron F. Dunkel, *Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United States in Light of the Source Informatics Cases*, 23 Loy. L.A. Int'l & Comp. L. Rev. 41 (Feb. 2001).

Editorial Staff of the Yale J. Health & Policy, *Synopsis of State Case & Statutory Law (Relevant Access & Disclosure to Medical Records)*, 2 Yale J. Health Pol'y L. & Ethics (2002).

Sharon Erwin, *Drafting & Reviewing Privacy Policies of Health-Related Web Sites: Some General Guidelines*, 13 No. 2 Health Law 10 (2000).

General Accountability Office, *Health Information First Year Experiences Under the Federal Privacy Rule*, Report to the Chairman, Committee on Health, Education, Labor, and Pensions, U.S. Senate (Sept. 2004).

General Accountability Office, *HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption, Briefing for Congressional Staff, Senate Committee on Health, Education, Labor, and Pensions* (Aug. 2004) *available at* www.gao.gov/new.items/d04991r.pdf.

Catherine Louisa Glenn, *Protecting Health Information Privacy: The Case for Self-Regulation of Electronically Held Medical Records*, 53 Vand. L. Rev. 1605 (2000).

Janlori Goldman, *Virtually Exposed: Privacy and E-Health*, 19 (No.6) Health Affairs 140 (Nov./Dec.2000) *available at* www.chcf.org/documents/ihealth/haGoldman.pdf.

Janlori Goldman, Sponsored by the California HealthCare Foundation, *Privacy: Report on the Privacy Policies and Practices of Health Web Sites* (Jan. 2000) *available at* www.chcf.org/topics/view.cfm?itemID=12497.

Janlori Goldman, *Protecting Privacy To Improve Health Care*, 17 (No. 6) Health Affairs 47 (Nov./Dec.1998) *available at* www.healthaffairs.org.

Lawrence Gostin, *Balancing Communal Goods and Personal Privacy Under a National Health Information Privacy Rule*, 46 St. Louis U. L. J. 5 (2002).

Lawrence Gostin, *The Nationalization of Health Information Privacy Protections*, 8 Conn. Ins. L. J. 283 (2001-2002).

Lawrence Gostin, James G. Hodge, *Informational Privacy and the Public Health*, 91 (No. 9) Am. J. of Pub. Health 1466 (Sept. 2000).

Lawrence Gostin, *Personal Privacy in the Health Care System*, Kennedy Inst. of Ethics J. 7.4 361-76 (1997), *available at* http://muse.jhu.edu/journals/kennedy_institute_of_ethics_journal/v007/7.4gostin.html.

Lawrence Gostin, *The Public Health Information Infrastructure: A National Review of the Law on Health Information Privacy*, 275 (No. 24) JAMA 1921 (June 1996).
Lawrence Gostin, *Health Information Privacy*, 80 Cornell L. Rev. 451 (March 1995).

Lawrence Gostin, *Privacy and Security of Health Information in the Emerging Health Care System*, 5 Health Matrix 1 (1995).

Mark Greenwood, *The Physician Profile Database*, 21 J. Legal Med. 477 (2000).

Patrick Gunn, *Health Insurance Portability and Accountability Act, A Practical Guide for Researchers*, 42 (No. 4) Med. Care 321 (Apr. 2004).

Health Privacy Project, *Summary of the HIPAA Privacy Rule* (Sept. 13, 2002).

Health Privacy Working Group, *Best Principles for Health Privacy* (July 1999) *available at* www.healthprivacy.org/usr_doc/33807.pdf.

James G. Hodge, *Health Information Privacy & Public Health*, 31 J.L. Med. & Ethics (2003).

James G. Hodge, *National Health Information Privacy and New Federalism*, 14 Notre Dame J.L. Ethics & Pub. Pol'y 791 (2000).

James G. Hodge, *Legal Issues Concerning Electronic Health Information: Privacy, Quality, and Liability*, 282 (No. 15) JAMA 1466 (Oct. 1999).

Joanne Hustead, *Genetics and Privacy: A Patchwork of Protections* (May 2002) *available at* www.chcf.org/documents/ihealth/GeneticsAndPrivacy.pdf.

John V. Jacobi, *Patients at a Loss: Protecting Health Care Consumers Through Data Driven Quality Assurance*, 45 Kan. L. Rev. 705 (May 1997).

May Beth Johnson, *HIPAA Becomes Reality: Compliance with New Privacy, Security and Electronic Transmission Standards*, 103 W. Va. L. Rev. 541 (Summer 2001).

Eric Jorstad, *The Privacy Paradox*, 27 Wm. Mitchell L. Rev. 1503 (2001).

Scott Killingsworth, *Website Privacy Policies in Principle and In Practice*, 618 PLI/Pat 663 (Sept. 2000).

Paul T. Kostyack, *The Emergence of the Healthcare Information Trust*, 12 Health Matrix 393 (Summer 2002).

John Lumpkin, *E-Health, HIPAA and Beyond*, 19 (No.6) Health Affairs 149, (Nov./Dec. 2000) *available at* www.chcf.org/documents/ihealth/haLumpkin.pdf.

Markle Foundation, Financial, Legal and Organizational Approaches To Achieving Electronic Connectivity In Healthcare (October 2004) *available at* www.markle.org/downloadable_assets/flo_sustain_healtcare_rpt.pdf.

Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Geo. L. J. 2381 (July 1996).

Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 Yale J. of Health Policy, Law, and Ethics 325 (Spring 2002).

Joy L. Pritts, Health Privacy Project, *The State of Health Privacy: An Uneven Terrain (A Comprehensive Survey of State Health Privacy Statutes)* (Aug. 1999).

William M. Sage, *Regulating Through Information: Disclosure Laws and American Health Care*, 99 Colum. L. Rev. 1701 (Nov. 1999).

Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan. L. Rev. 1125 (May 2000).

Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv. L. Rev. 2055 (May 2004).

Paul M. Schwartz, *Privacy and the Economics of Personal Health Information*, 76 Texas Law Review 1 (1997).

Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 Vand. L. Rev. 295 (Mar. 1995).

Daniel J. Solove, *Origins and Growth of Information Privacy Law*, 748 PLI/PAT 29 (June 2003).

Daniel J. Solove, *Access and Aggregation, Public Records, Privacy, and the Constitution*, 86 Minn. L. Rev. 1137 (2002).

Lisa Sotto, *Privacy Concerns in the Health Care Industry*, 748 PLI/Pat 831 (2003).

Paul C. Tang, *An AMIA Perspective on Proposed Regulation of Privacy of Health Information*, The J. of the Am. Med. Informatics Ass'n (Mar. 2000).

Samuel J. Wang, *A Cost Benefit Analysis of Electronic Medical Records in Primary Care*, 114 The Am. J. of Med. 397 (Apr. 1, 2003) *available at* http://www.cba.hawaii.edu/chismar/wang-cost-03.pdf.

Racial & Ethnic Disparities in the Delivery of Health Care

Marsha Lillie-Blanton, *Site of Medical Care: Do Racial and Ethnic Differences Persist?,* 1 Yale J. Health Pol'y L. & Ethics 15 (Spring 2001).

Kevin Fiscella, The Civil Rights Project at Harvard University, *Within Our Reach: Equality in Health Care Quality* (2004).

Scarlett Lin Gomez, *Hospital Policy and Practice Regarding the Collection of Data on Race, Ethnicity, and Birthplace*, 93 (No 10) The Am. J. of Pub. Health 1685 (Oct. 2003).

May-Jo DelVecchio Good, Russell Sage Foundation, Working Paper #199, *The Culture of Medicine and Racial, Ethnic, and Class Disparities in Healthcare* (Dec. 2002) *available at* http://www.russellsage.org/working_papers/199good.pdf.

Institute of Medicine, *Unequal Treatment: Confronting Racial and Ethnic Disparities in Health Care* (2003).

Nancy R. Kressin, *Agreement Between Administrative Data and Patients' Self-Reports of Race/Ethnicity*, 93 (No. 10) The Am. J. of Pub. Health 1734 (Oct. 2003).

M. Barton Laws, *Racial and Ethnic Identification Practices in Public Health Data Systems in New England*, 117 Pub. Health Reps. 50 (Jan./Feb. 2002) *available at* http://download.journals.elsevierhealth.com/pdfs/journals/0033-3549/PIIS0033354904501085.pdf.

John E. McDonough, The Commonwealth Fund, *A State Policy Agenda to Eliminate Racial and Ethnic Health Disparities* (June 2004) *available at* www.cmwf.org/programs/minority/mcdonough_statepolicyagenda_746.pdf.

National Research Council of the National Academies, *Eliminating Health Disparities: Measurement and Data Needs* (2004) *available at* www.nap.edu/books/0309092310/html/.

David R. Nerenz, *Eliminating Racial/Ethnic Disparities In Health Care: Can Health Plans Generate Reports?,* 21 (No. 3) Health Affairs 259 (May/June 2002).

Ruth T. Perot, The Commonwealth Fund, *Racial, Ethnic, and the Primary Language Data Collection in the Health Care System: An Assessment of Federal Policies and Practices* (Sept. 2001) *available at* http://www.cmwf.org/usr_doc/perot_racialethnic_492.pdf.

Vernellia R. Randall, *Racial Discrimination in Health Care in the United States As a Violation of the International Convention on the Elimination of All Forms of Racial Discrimination*, 14 U. Fla. J.L. & Pub. Pol'y 45 (Fall 2002).

Edward J. Sondik, *Race/Ethnicity and the 2000 Census: Implications for Public Health*, 90 (No. 11) The Am. J. of Pub. Health 1709 (Nov. 2000) *available at* http://www.hsph.harvard.edu/society/images/1709-Sondik-1100.pdf.

Audra T. Wenzlow, Institute for Research on Poverty, Discussion Paper No. 1283-04, *Understanding Racial Disparities in Health: The Income-Wealth Paradox*, (July 2004) *available at* http://www.ssc.wisc.edu/irp/pubs/dp128304.pdf.

Romana Hasnain-Wynia, The Commonwealth Fund, *Who, When, and How: The Current State of Race, Ethnicity, and Primary Language Data Collection in Hospitals* (May 2004) *available at* http://www.cmwf.org/usr_doc/hasnain-wynia_whowhenhow_726.pdf.

General

David Bates, *The Impact of the Internet on Quality Measurement*, 19 (No. 6) Health Affairs 104 (Nov./Dec. 2000) *available at* www.chcf.org/documents/ihealth/haBates.pdf.

The Commonwealth Fund, *Information Technologies: When Will They Make it Into Physicians' Black Bags?*, *available at* http://www.cmwf.org/publications/publications_show.htm?doc_id=251984 (accessed Dec. 12, 2004).

Bruce Fried, *E-Health: Technological Revolution Meets Regulatory Restraint*, 19 (No. 6) Health Affairs 124 (Nov./Dec. 2000) *available at* www.chcf.org/documents/ihealth/haFried.pdf.

Health Strategies Consultancy, *Financial Incentives: Innovative Payment for Health Information Technology* (Mar. 2004) *available at* http://ccbh.ehealthinitiative.org/highlights.aspx?Document=261.

Betsey L. Humphreys, *Electronic Health Record Meets Digital Library: A New Environment for Achieving an Old Goal*, 7 (No.5) J. of the Am. Med. Informatics Ass'n 444 (Mar. 2000).

Kohn, L., Institute of Medicine, *To Err is Human: Building a Safer Health System* (2000).

Institute of Medicine, *Crossing the Quality Chasm: A New Health System for the 21st Century* (2001).

Peter Kilbridge, *Crossing the Chasm with Information Technology: Bridging the Quality Gap in HealthCare* (July 2002) *available at* www.chcf.org/documents/ihealth/CrossingChasmIT.pdf.

Samuel J. Wang, *A Cost Benefit Analysis of Electronic Medical Records in Primary Care*, 114 The Am. J. of Med. 3