July 2005

MEMBER BRIEFING

INTEROPERABLE ELECTRONIC HEALTH RECORDS TASK FORCE

THE QUEST FOR INTEROPERABLE ELECTRONIC HEALTH RECORDS: A Guide to Legal Issues in Establishing Health Information Networks

Editors:*
Kristen Rosati, Esquire
Coppersmith Gordon Schermer Owens & Nelson PLC
Marilyn Lamar,Esquire
McDermott Will & Emery LLP

I. INTRODUCTION

The purpose of this Briefing is to provide an overview of the myriad legal issues that may arise in planning, implementing, and operating interoperable electronic health records (EHRs) in Health Information Networks (HINs).[1] The editors hope that by identifying these legal issues, healthcare attorneys, industry leaders and the government can formulate solutions to reduce the legal risks that would otherwise present significant barriers to further adoption of EHRs and HINs.

A. Background

The increased use of information technology (IT) has been expected to reduce healthcare costs and improve the quality of patient care for more than a decade. For example, anticipated cost savings from information technology was a factor in federal efforts to impose uniformity in electronic transactions through the "administrative simplification" provisions of the Health Insurance Portability and Accountability Act of

---

* The editors would like to thank the many AHLA members that contributed to this Briefing. The contributors and their roles are listed in the Introduction.

[1] Health Information Networks (HINs) may be called by a variety of other terms, such as Regional Health Information Organizations (RHIOs) or Community Health Information Networks (CHINs). In this Briefing, we use the broader and more inclusive term HIN.

1996 (HIPAA). Similarly, many people expect that the use of IT in patient care—particularly by making electronic health records easily available to all healthcare providers—also will reduce healthcare costs and improve the quality of care. Indeed, a few community-based HINs now serve as positive examples of how IT can be used to realize these benefits.

Unfortunately, many segments of the healthcare industry directly involved with patient care lag far behind other industries in the use of IT. Some healthcare providers still use paper-based medical record storage and retrieval, communicate with labs and pharmacies by telephone or fax rather than e-mail, and do not use electronic systems to assist in clinical decision making. The lower level of IT being utilized in patient care adversely affects costs and the quality of care.

Limited adoption of IT by providers may be due to aspects of healthcare that present unique challenges to the use of IT, including:

- the large number of physicians in solo or small group practices with very limited administrative support for IT and related practice changes;
- the lack of uniformity and interoperability of IT systems from different vendors;
- regulatory limitations on hospital funding of IT for physicians;
- antitrust and other legal concerns with respect to joint IT solutions; and
- privacy and security concerns.

However, momentum appears to be building now for increased use of IT in healthcare with renewed focus from the federal government on the potential benefits and a growing number of community-based initiatives.

B. Recent Federal Government Initiatives

In April 2004, President Bush called for the widespread adoption of electronic medical records for most Americans within the next ten years Dr. David Brailer, MD, PhD, was then appointed to serve as the National Coordinator for Health Information Technology, a new position within the Department of Health and Human Services (DHHS).

Dr. Brailer's office issued its Framework for Strategic Action in July 2004 (the Framework), which outlined four major goals:

(1) to inform clinical practice with the use of EHRs;

(2) to interconnect clinicians so that they can exchange health information using advanced and secure electronic communications;
(3) to personalize care with consumer-based health records and better information for consumers; and
(4) to improve public health through advanced biosurveillance methods and streamlined collection of data for quality measurement and research.

As a next step in this process, the Office of the National Coordinator for Health Information Technology (ONC or ONCHIT) issued a Request for Information (RFI) in November 2004 seeking information regarding the definition and structure of a National Health Information Network (NHIN), a proposed organization and business framework, the management and operation, standards and policies for interoperability, and financial, regulatory, and legal considerations. ONC reportedly received over 500 responses to the RFI, some of which have been published by the respondents. A summary published in June 2005 noted that the following concepts emerged from the majority of RFI respondents:

- A NHIN should be a decentralized architecture built using the Internet linked by uniform communications and a software framework of open standards and policies.
- A NHIN should reflect the interests of all stakeholders and be a joint public/private effort.
- A governance entity composed of public and private stakeholders should oversee the determination of standards and policies.
- A NHIN should be patient-centric with sufficient safeguards to protect the privacy of personal health information.
- Incentives will be needed to accelerate deployment and adoption of a NHIN.
- Existing technologies, federal leadership, prototype regional exchange efforts, and certification of EHRs will be the critical enablers of NHIN.
- Key challenges will be the need for additional and better-refined standards; addressing privacy concerns; paying for the development and operation of, and access to the NHIN; accurately matching patients; and addressing discordant state laws regarding health information exchange.

The Framework also called for a Health Information Technology Leadership Panel to be convened to examine the importance of investing in health information technology (HIT) and the roles of government and the private sector in its widespread implementation. The report issued by the HIT Leadership Panel on May 11, 2005 identified three key imperatives for HIT:

(1) Widespread adoption of interoperable HIT as a top priority;
(2) The federal government using its leverage as the nation's largest healthcare provider and payer to drive adoption of HIT; and
(3) Collaboration by private sector purchasers and healthcare organizations with the federal government to drive adoption of HIT.

Additional conclusions of the HIT Leadership Panel focused on a positive cost-benefit expectation regarding adoption, the need for a broad vision with a practical adoption strategy, and alignment of stakeholder incentives. Unlike some studies that have focused on physician adoption as a critical element, the HIT Leadership Panel concluded that consumers will be the key to adoption. It also noted that the federal government should provide leadership and that industry would follow.

Fostering the wider adoption of HIT continues to attract a bipartisan following in Congress, with Representative Patrick Kennedy (D-R.I.) and Representative Tim Murphy (R-Pa.) sponsoring H.R. 2234, the 21st Century Health Information Act. Senator Hillary Rodham Clinton (D-N.Y.) and Senate majority leader Dr. Bill Frist (R-Tenn.) have also introduced HIT legislation in the Senate known as the Health Technology to Enhance Quality Act of 2005 (or the "Health TEQ Act," S. 1262).

C. Alternative Structures for Health Information Networks

HINs have been identified by ONC as a favored approach to the initial goal of EHRs that would operate across a community or region. For purposes of this briefing, we will focus on three current approaches for a HIN:

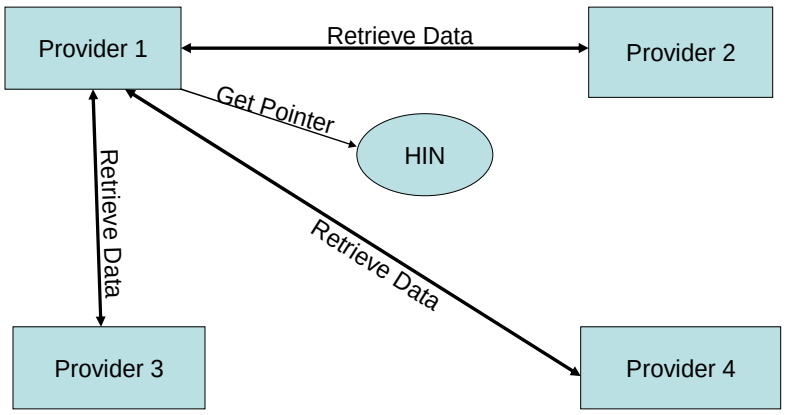
- "Pointer System" in which the HIN identifies where a patient's information is located and makes it available to an authorized user. All participants in a HIN (hereinafter referred to as Participants) interact with each other to exchange information, although an intermediary may do some of the processing.

- “Data Warehouse-Silo System” in which the HIN holds each participant’s information in separate silos, but pulls information from applicable silos when information about a particular patient is requested. This is also referred to as a “hub and spokes” arrangement.
- “Community Health Record System” where the HIN combines information from different providers in a single record.

These three approaches are represented graphically as follows:

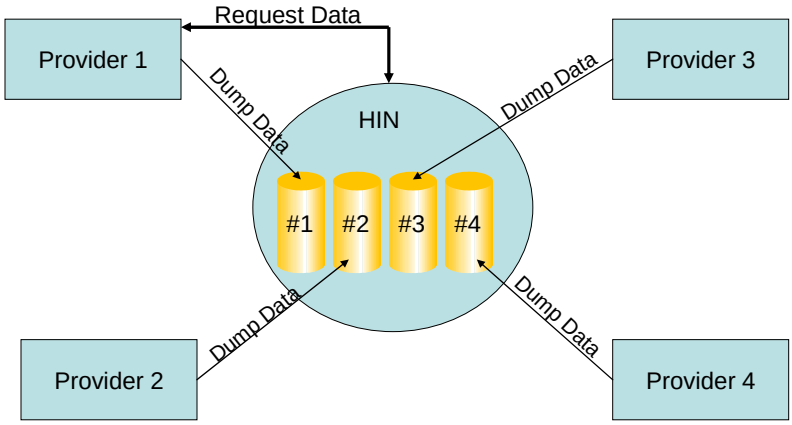
Pointer System

Diagram courtesy of Jeffrey Short, Hall, Render, Killian, Heath & Lyman, P.S.C



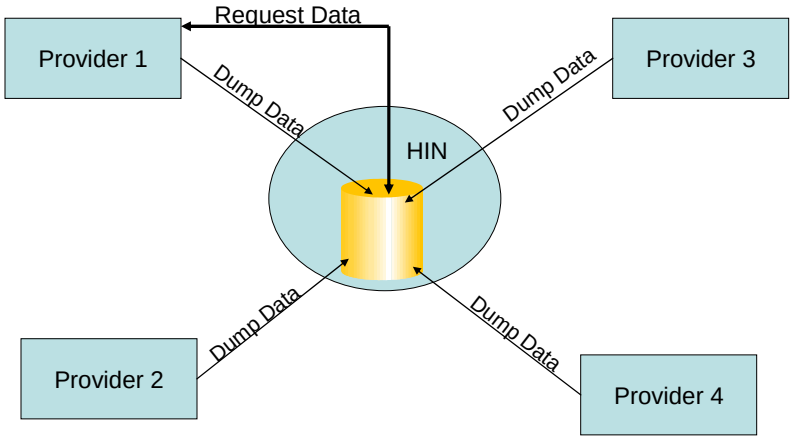
Data Warehouse-Silo System

Diagram courtesy of Jeffrey Short, Hall, Render, Killian, Heath & Lyman, P.S.C



Community Health Record System

Diagram courtesy of Jeffrey Short, Hall, Render, Killian, Heath & Lyman, P.S.C



In evaluating and structuring a HIN it may be helpful to analyze a client's needs in terms of these three forms of HINs, but variations on these models and entirely new approaches are likely to evolve over time. An ultimate goal of this process will be to link

the HINs on a nationwide basis, but this effort appears likely to occur only at a later stage of the overall initiative.

Another significant aspect of structuring a HIN is the decision of whether to form a new legal entity to serve as the HIN or whether one or more of the entities that participate in a HIN would serve those functions. For example, each of the HIN arrangements described above could be comprised of local hospitals, physicians, and clinical laboratories that assign the HIN functions to one of the hospital participants pursuant to a contract. Alternatively, the parties could form a new legal entity (Newco) that would conduct the HIN functions pursuant to a contract between the Newco and the participants. Use of a Newco obviously will present additional issues regarding ownership, tax status, and regulatory compliance for the HIN and its participants but should not present insurmountable barriers if the participants select this approach.

D. Overview of Legal Issues

Numerous legal issues will need to be considered and addressed in structuring, implementing, and operating a HIN or other systems of interoperable EHRs. Issues arising in each of the following areas are discussed in more detail in the separate Chapters that follow:

- **Privacy (Chapter 1)**
- **Security (Chapter 2)**
- **Stark and Anti-Kickback (Chapter 3)**
- **Non-Profit Tax (Chapter 4)**
- **Antitrust (Chapter 5)**
- **Intellectual Property (Chapter 6)**
- **Medical Malpractice and Other Potential Liability (Chapter 7)**
- **State Law Issues (Chapter 8)**

Although HINs and EHR arrangements will entail numerous agreements to delineate the scope of activities and satisfy HIPAA and other legal requirements, this Briefing does not propose model forms of these agreements because the overall arrangements are rapidly evolving and must meet the unique needs of the various communities they serve. This Briefing is not intended as a substitute for legal advice in

light of specific circumstances and after a review of the latest developments in each of these areas.

E. Acknowledgments

The editors would like to thank the numerous American Health Lawyers Association members who contributed to this Briefing. It is only with the assistance of dozens of members that AHLA is able to provide this Briefing to assist in analyzing and implementing new technologies that should be of great benefit to the healthcare system and to each of us as potential patients. Contributors to this Briefing include:

Chapter 1: Privacy

Alice J. Becker, PeaceHealth (Co-chair); *Rebecca L. Williams*, JD, RN, Davis Wright Tremaine LLP (Co-chair); *Jana H. Aagaard*, Law Office of Jana H. Aagaard; *Sheryl Tater Dacso*, JD, DrPH, Law Officers of Sheryl Tatar Dacso PLLC; *William P. Dillon*, McMorrow & Dillon PA; *Alexander D. Eremia*, MedStar Health; *Cecelia A. Gassner*, dba Lifetech Law Group; *Kimberly S. Gray*, Highmark Inc.; *Kate Hickner-Cruz*, Raymond & Prokop PC; *Michael W. Hubbard*, Smith Anderson Blout Dorsett Mitchell & Jernigan LLP; *Keith A. Kelly*, Ray Quinney & Nebeker PC; *Sallie Hunt*, West Virginia Health Care Authority; *Kimiko L. Orosz*, Bass Berry & Sims PLC; *Abbie P. Maliniak*, Fulbright & Jaworski LLP; *Gail Ruffin-Cruz Jones*, CIGNA HealthCare; *Jim C. Pyles*, Powers Pyles Sutter & Verville PC; *Kristen B. Rosati*, Coppersmith Gordon Schermer Owens & Nelson PLC; *Cynthia Marcotte Stamer*, Epstein Becker & Green PC; *Beth L. Rubin*, Dechert LLP; *Claire Turcotte*, Rosenn Jenkins & Greenwald LLP; *Robert H. Schwartz*, Raymond & Prokop PC; and *Brian M. Wyatt*, Hospital for Special Surgery.

Chapter 2: Security

Margaret Marchak, Raymond & Prokop PC (Chair); *Jana Harder Aagaard*, Law Office of Jana H. Aagaard; *William P. Dillon*, McMorrow & Dillon PA; *Claudia Egan*, von Briesen & Roper SC; *Alexander D. Eremia*, MedStar Health; *Randy Gainer*, Davis Wright Tremaine LLP; *Cecelia A. Gassner*, Lifetech Law Group; *Pat King*, Law Practice of Patricia D. King; *Marilyn Lamar*, McDermott, Will & Emery LLP; *Beth L. Rubin*, Dechert LLP; *Claire Turcotte*, Rosenn, Jenkins & Greenwald LLP; *Cindy Wisner*, Trinity Health; and *Brian M. Wyatt*, Hospital for Special Surgery.

Chapter 3: Stark and Anti-Kickback

Robert G. Homchick, Davis Wright Tremaine LLP (Chair), *Laird A. Pisto*, MultiCare Health System; *Dan Brown*, Greenberg Traurig LLP; *Claudia Egan*, von Briesen & Roper SC; *Rob Falk*, Powell Goldstein LLP; *Beth Schermer*, Coppersmith Gordon Schermer Owens & Nelson PLC; *Jordana G. Schwartz*, Sonnenschein Nath & Rosenthal LLP; and *Claire Turcotte*, Rosenn, Jenkins & Greenwald, LLP.

Chapter 4: Non-Profit Taxation

Bernadette Broccolo, McDermott Will & Emery LLP (Chair); *Gordon Apple*, Law Offices of Gordon J. Apple PC; *Charles M. Key*, The Bogatin Law Firm PLC; *Robert Q. Wilson*, The Bogatin Law Firm PLC.

Chapter 5: Antitrust

Christine White, McDermott Will & Emery LLP (Chair).

Chapter 6: Intellectual Property

Virginia Holden, McDermott Will & Emery LLP (Chair); *Jason A. Bernstein*, Powell Goldstein LLP; *Benjamin T. Butler*, Crowell & Moring LLP; *Heidi Echols*, McDermott Will & Emery LLP; *Donna Z. Eden*; Cecelia A. Gassner, Lifetech Law Group; *Marilyn Lamar*, McDermott Will & Emery LLP; *Patrick Richards*, McDermott Will & Emery LLP; and *Cynthia Wisner*, Trinity Health.

Chapter 7: Medical Malpractice and Other Potential Liability

Edward Shay, Post & Schell PC (Chair); *Jana Harder Aagaard*, Law Office of Jana H. Aagaard; *Kenneth C. Bartholomew*, Rath Young & Pignatelli PA; *Sarah E. Coyne*, Quarles & Brady LLP; *Sheryl Tater Dacso*, Law Offices of Sheryl Tatar Dacso PLLC; *John Humber*, Radiology Clinic LLC; *Charles Key*, The Bogatin Law Firm PLC; *Libby Lincoln*, The MMIC Group; and *Robert Q. Wilson*, The Bogatin Law Firm PLC.

Chapter 8: State Law

Brian D. Gradle, Hogan & Hartson LLP (Chair); *Nancy P. Gillette*, Ohio State Medical Association; *Rachel Glitz*, Davis Wright Tremaine LLP; *Barry S. Herrin*, Smith Moore LLP*; Pat King*, Law Practice of Patricia D. King; and *Kristen B. Rosati*, Coppersmith Gordon Schermer Owens & Nelson PLC.

CHAPTER 1:
PRIVACY

Because an EHR system likely will not be successful if patients do not trust that their information will be held confidentially, adequate protection for the privacy of health information included in the system is an essential step in the development of HINs. As the Department of Health and Human Service (DHHS) concluded, "the entire health delivery system is built upon the willingness of individuals to share the most intimate details of their lives with their health providers."[2] In enacting the Health Insurance Portability and Accountability Act (HIPAA),[3] Congress recognized that adequate protection of the privacy and security of health information is a "*sine qua non* of the increased efficiency . . . brought about by the electronic revolution."[4] The protection of medical privacy is essential for access to "effective, high quality healthcare."[5] The public perceives the "increasing use of interconnected electronic information systems as one of the greatest threats to medical privacy."[6] Thus, rigorous privacy protection for the health information stored in an EHR system is essential to the long term success of this mission.

In this Chapter, we describe legal issues relating to privacy, which we define as the right of patients to not have their information disclosed to unauthorized parties. These legal issues arise from a myriad of legal sources, including the HIPAA Privacy Rule, other federal privacy laws such as the federal Privacy Act[7] and the federal substance abuse treatment confidentiality regulations,[8] state laws for special classes of information (such as AIDS, mental health, substance abuse, genetic information, and developmental disabilities),[9] federal and state constitutional rights to privacy,[10] federal

---

[2] 65 Fed. Reg. 82,467 (Dec. 28, 2000).
[3] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191 (Aug. 21, 1996), 42 U.S.C. § 201, *et seq.; see also* HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subpart E.
[4] 65 Fed. Reg. 82,474.
[5] 65 Fed. Reg. 82,467; *see also Jaffee v. Redmond*, 116 S. Ct. 1923, 1928 (1996).
[6] 65 Fed. Reg. 82,465.
[7] Privacy Act of 1974, Pub. L. No. 93-579 (1974), 5 U.S.C. § 552a.
[8] 42 C.F.R. Part 2.
[9] *See, e.g.,* Arizona Revised Statutes § 36-501 *et seq.* (protecting mental health information).
[10] *See, e.g.*, *Lawrence v. Texas*, 539 U.S. 558, 123 S. Ct. 2472, 2478 (2003) (holding that, while the Constitution only protects citizens against violations of their rights by the government, encroachments by

Medicare Conditions of Participation,[11] state provider licensure requirements,[12] and Joint Commission on Accreditation of Healthcare Organizations accreditation standards.[13] Counsel involved in establishing HINs should be familiar with this wide variety of privacy laws and how they affect health information, but due to space constraints this Chapter discusses only the application of the HIPAA Privacy Rule because all health plans and most healthcare providers in the United States must comply with this regulation.

The particular legal issues relating to privacy protection will of course vary depending on how the interoperable EHR is organized. As explored in the Introduction, the legal structure for HINs can take a number of forms—the Pointer/Locator System, Data Warehouse/Silo System, or Community Health Record System. Moreover, whether the HIN is formed by a "web" of contracts between the HIN Participants, or whether a separate legal entity is created to own and operate the HIN, will affect greatly how the HIPAA issues are addressed. Counsel thus must closely examine the HIN's structure and operations, its purposes, and the identity of the participants in the HIN (such as providers, plans, payors, government agencies, and patients).

1-1. HIPAA Organizational Issues

1-1(a). HIN as a Covered Entity

HIPAA applies only to "covered entities," which are defined as: (i) health plans; (ii) healthcare providers that electronically conduct certain financial and administrative transactions for which standards have been adopted by the Secretary of DHHS under HIPAA; and (iii) healthcare clearinghouses.[14] Therefore, one of the key questions with

---

private entities exercising governmentally-granted authority can be determined a violation of constitutional rights if that is the practical effect, purpose, or intent of a law); *Ferguson v. City of Charleston*, 532 U.S. 67, 78, 121 S. Ct. 1281, 1288 (2001) (holding that disclosures of patient health information for law enforcement purposes without a warrant or patient notice and consent violates the Fourth Amendment); *Whalen v. Roe*, 429 U.S. 589, 599, 97 S. Ct. 869, 876 (1977); *Santa Fe Indep. School Dist.,* 530 U.S. 290, 309, 120 S. Ct. 2266, 2278 (2000); *Gilmore v. City of Montgomery,* 417 U.S. 556, 565, 94 S. Ct. 2416, 2422 (1974); *Reitman v. Mulkey,* 387 U.S. 369, 371, 87 S. Ct. 1627, 1629 (1967).

[11] *See, e.g.,* 42 C.F.R. § 482.24 (medical records requirements for hospitals).

[12] *See, e.g.,* Pa. Stat. 422.41(8).

[13] *See, e.g.,* Management of Information (IM) Standards, 2005 Hospital Accreditation Standards.

[14] 45 C.F.R. § 160.103.

respect to HIPAA compliance is whether the HIN itself is a covered entity, assuming it is a separate legal entity.

We first note that under all three models discussed in this Briefing, a HIN could function entirely pursuant to contractual provisions among the participating organizations. Under this scenario, an additional legal entity would not exist that could be characterized as a covered entity for purposes of HIPAA. Instead, the analysis would focus on the obligations of the participating entities (the HIN Participants) to enter into agreements with the party that performs the HIN services as a business associate of the participating covered entities.

Alternatively, if a separate legal entity performs the HIN functions under any of the approaches described in the Introduction, HIPAA compliance will require a review of whether the functions that the HIN entity performs would make it a covered entity for purposes of HIPAA.[15] In most cases the HIN functions would not, standing alone, satisfy two of the three HIPAA definitions of a covered entity. Specifically, such functions would not make the HIN entity a health plan (defined as an individual or group health plan that pays the cost of medical care) or a healthcare provider (defined as furnishing, billing, or being paid for health or medical services in the normal course of business).[16]

However, an entity performing the HIN functions would be a covered entity with respect to those functions if it satisfied the following definition of a healthcare clearinghouse:

> a public or private entity, including a billing service, repricing company, *community health management information system or community health information system,* and "value-added" networks and switches, that does either of the following functions:
>
> (1) *Processes or facilitates* the processing of health information received from another entity in a nonstandard

[15] CMS has provided a decision tool to assist in the analysis as to whether an entity is a covered entity for HIPAA purposes at http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp

[16] 45 C.F.R. § 160.103.

> format or containing nonstandard data content into standard data elements or a standard transaction.
>
> (2) Receives a standard transaction from another entity and *processes or facilitates* the processing of health information [in the standard transaction] into nonstandard format or nonstandard data content for the receiving entity.[17] (Emphasis supplied.)

For example, an entity providing HIN services in the Community Health Record System model might be taking information from providers and other sources and reformatting it in a manner that would involve the processing of nonstandard data into a standard format (or vice versa). Further, DHHS's inclusion of "community health management information system" and "community health information system" as examples in the definition could lend weight to the conclusion that a person or entity performing HIN functions in the Community Health Record System model might be considered a healthcare clearinghouse if the functions described above were performed or facilitated.[18]

1-1(b). HIN as a Business Associate

As discussed above, an entity performing HIN services is unlikely to be a covered entity under HIPAA unless it functions as a healthcare clearinghouse. However, the HIN may be a business associate (BA) of the HIN Participants that are covered entities.[19] If the HIN is an independent legal entity that operates the EHR system, the HIN itself will be a HIPAA business associate of the HIN Participants who are covered entities. If the HIN is a contractual "web," on the other hand, the HIN Participants should evaluate whether any of the Participants are providing a service to the others (such as housing the EHR or performing administrative services for the HIN

---

[17] *Id.*

[18] Although these terms were part of the original definition of healthcare clearinghouse in the November 3, 1999 Notice of Proposed Rulemaking for the Privacy Rule, DHHS has not explained their meaning in depth. *See* 64 Fed. Reg. at 59,227 and 59,930 (Nov. 3, 1999); 65 Fed. Reg. at 82,477 and 82,572 (Dec. 28, 2000).

[19] 45 C.F.R. § 164.308(b)(1). Note the exceptions included in § 164.308(b)(2) for transmissions of EPHI by a covered entity to a provider concerning treatment of an individual and by certain health plans and insurers to a plan sponsor if certain requirements are met.

in which the entity has access to the other Participant's patient or member health information), and thus will meet the definition of a business associate of the other HIN Participants.

Of course, the HIPAA Privacy Rule requires the covered entities each to have a contract in place with the business associate.[20] The HIPAA-required provisions for a business associate contract likely would best belong in the contract governing how the HIN will be operated, or that outlines the services to be provided by the HIN Participant/business associate. Because we assume the reader is familiar with the HIPAA-required provisions in a BA contract, we do not discuss them here. As a practical matter, one common contract should be used between the HIN and the HIN Participants, so that inconsistent obligations are not created between Participants.

The contracts should address how the system will deal with BA violations of the HIPAA rules. If a covered entity knows of a pattern of activity or practice of the BA that constituted a material breach of the BA's contractual obligations, the covered entity must take steps to cure the breach or end the violation. If such steps are unsuccessful, the covered entity must terminate the contract or report the problem to the Secretary of DHHS. This possibility should be anticipated in advance to protect the HIN Participants from liability under HIPAA.[21]

1-1(c). Organized Healthcare Arrangements

The HIN Participants should consider whether the HIN meets the requirements of an Organized Healthcare Arrangement (OHCA) under the HIPAA Privacy Rule. The Privacy Rule defines five different types of OHCAs. The OHCA definitions most likely to apply to a HIN include: (a) a "clinically integrated care setting in which individuals typically receive care from more than one healthcare provider," or (b) an "organized system of healthcare . . . in which the participating covered entities . . . hold themselves

---

[20] 45 C.F.R. § 164.502(e); § 164.504(E).

[21] 45 C.F.R. § 160.402 (a covered entity is liable under the federal common law of agency for the acts of a business associate, unless the covered entity complies with §§ 164.308(b), 164.314(a)(1)(ii), 164.502(e), and 164.504(e)(1)(ii).

out to the public as participating in a joint arrangement and participate in joint activities" involving utilization review, quality assessment, or payment activities.[22]

Unfortunately, there is little guidance regarding whether a HIN could qualify as an OHCA, such as whether the HIN Participants could be considered a "clinically integrated care setting," or how much joint activity is needed to qualify as a joint-arrangement OHCA. This may depend on the degree to which OHCA participants share a common patient population or provide services along a continuum of care to the community at large. It is noteworthy that DHHS has indicated that OHCAs "may take different legal structures."[23] This suggests at least the possibility of some flexibility in legal structure for OHCAs. Nevertheless, this uncertainty and lack of clear guidance may present an obstacle to pursuing an OHCA-model HIN and cause HINs to pursue other models for compliance, such as having business associate agreements in place between the HIN and HIN Participants.

If OHCA status is pursued, it will permit all OHCA/HIN Participants to use and disclose health information for the joint management and operations of the HIN, as well as for the already permissible joint treatment of patients and payment, all without patient authorization and without business associate agreements in place (subject to applicable state and other federal privacy laws).[24] Without OHCA status, covered entities may not use and disclose health information for the full range of healthcare operations of the HIN Participants without patient authorization.[25] OHCA status also may minimize the HIPAA compliance burden otherwise generally applicable to OHCA participants, such as allowing for a joint notice of privacy practices and avoiding the need for business associate agreements among the HIN Participants.

Before establishing an OHCA, a HIN Participant should consider whether it may have potential liability for actions of other OHCA members, especially where the HIN

---

[22] 45 C.F.R. § 164.501.
[23] 65 Fed. Reg. 82,494.
[24] 45 C.F.R. 164.506(c).
[25] *See* 45 C.F.R. § 164.506(c) (limiting disclosures for other covered entities' healthcare operations to where the recipient covered entity has or had a relationship with the patient, and where the healthcare operations are for fraud and abuse compliance, or fall within the first two paragraphs of the definition of healthcare operations); 45 C.F.R. § 164.501 (defining healthcare operations).

Participants holding themselves out as participating in a joint arrangement, and especially if the HIN does not already possess some degree of joint integration other than that envisioned by the HIN.

1-2. Uses and Disclosures of Health Information by the HIN

1-2(a). Use and Disclosure for Treatment, Payment, and Healthcare Operations

The Privacy Rule permits uses and disclosures of protected health information (PHI) for treatment, payment, and healthcare operations (TPO) without patient authorization by the entity that cared for the patient.[26] It also permits disclosure to other entities for the treatment or payment activities.[27] However, a covered entity may disclose PHI for the healthcare operations of another entity only if that entity is a covered entity under HIPAA, the entity has or had a relationship with the patient, and the healthcare operations are for the purposes of fraud and abuse detection and compliance or those listed in the first two paragraphs of the definition of healthcare operations (including such activities as quality assurance, care coordination, peer review, training, accreditation, and licensure).[28] Alternatively, the Privacy Rule also permits the disclosure of PHI to participants in an organized healthcare arrangement, for "any healthcare operations of the [OHCA]."[29]

A HIN that limits uses and disclosures of health information by HIN Participants to treatment, payment, and the permitted healthcare operations reduces the risks of a privacy violation. Such limitations, however, may not be practical or preferable for certain HINs. The following sections discuss uses and disclosures beyond TPO that likely will be proposed for HINs.

1-2(b). Public Health Disclosures

The federal government is looking to HINs as repositories of information to be mined for public health surveillance and research. How a HIN will respond to these government requests for information will be a challenge. Disclosure of health

---

[26] 45 C.F.R. § 164.501; 45 C.F.R. § 164.506(a); § 164.506(c)(1).
[27] 45 C.F.R. § 164.506(c)(2)-(3).
[28] 45 C.F.R. § 164.506(c)(4); § 164.501 (defining healthcare operations).
[29] 45 C.F.R. § 164.506(c)(5).

information for public health purposes may be required or permissive under state or federal law. For example, with regard to public health reporting, certain HIN Participants may be required to report cancer cases to a state registry. On the other hand, reporting certain diagnoses for public health initiatives may be voluntary. Under HIPAA, HIN Participants may disclose health information to public health authorities as long as the disclosures are authorized or mandated by state or federal law.[30]

The disclosure by or through a HIN of health information for public health purposes will depend on the structure and purposes of the HIN. HIN Participants will need to address which entity is required or authorized to make the disclosure. Questions to consider include:

- Should the HIN or the HIN Participants be permitted to disclose health information for public health purposes and, if so, in which circumstances?
- Does the HIN Participant that receives reportable information from or about an individual make the report, or will the HIN handle that reporting? If it is to be reported by the HIN, through what mechanism?
- Who is responsible to log the disclosure to include on an accounting to the individual?
- Who is responsible for any required follow-up contact with public health authorities?
- Should reportable information (such as information about communicable diseases) be available to all HIN Participants, or would this violate state confidentiality laws?
- Will the HIN permit a public health authority to have access to the HIN Participants' records for public health activities?

1-2(c). Research Disclosures

The federal government and other research proponents are calling for access to health information to accelerate the pace of clinical research toward cures for disease.[31]

---

[30] 45 C.F.R. § 164.512(b).

[31] For example, *see* "Moving Medical Innovations Forward–New Initiatives from HHS," available at http://www.hhs.gov/reference/medicalinnovations.html; *see also* the goals of the Office of the National Coordinator for Health Information Technology's Health Information Technology Strategic Framework,

HINs have the potential to help meet this goal, because they will have control over a large number of medical records. Of course, in order to allow access to those records for research, the HIN Participants (or HIN on behalf of the Participants), must comply with the HIPAA Privacy Rule provisions on research,[32] the DHHS Common Rule,[33] and Food and Drug Administration (FDA) regulations on human subject research and using electronic records in submitting data to the FDA.[34] State laws may pose additional barriers to accessing EHR for research purposes. Questions to consider include:

- Who is responsible for confirming that an Institutional Review Board (IRB) has approved the research project—and the appropriate HIPAA rule has been met—before use or disclosure of any health information within or outside of the HIN for research purposes?
- Who may determine whether a research sponsor may have access to identifiable patient health information?
- Can mechanisms be created to limit use and disclosure to only the health information pertinent to the clinical trial or other research project?
- Who is responsible for accounting for disclosures if authorizations are waived for use or disclosure of the health information for the research?
- Who will be responsible for determining what other privacy laws may apply to the research (such as state genetic testing laws), which may prevent the access for research?
- If the FDA, a pharmaceutical company, or medical device manufacturer is investigating an adverse event linked to a clinical trial, how will HIN Participants determine the appropriate disclosure of health information that is held by the HIN?

---

available at http://www.hhs.gov/healthit/goals.html#improve. In addition, FasterCures.org, an organization devoted to accelerating medical research, advocates the creation of new medical records and biospecimens databases. *See* http://www.fastercures.org/sec/agenda.

[32] 45 C.F.R. § 164.512(i).

[33] 45 C.F.R. Part 46.

[34] 21 C.F.R. Parts 11, 50 and 56. For a recent discussion of the FDA regulations on electronic records submission to the FDA, see Neil F. O'Flaherty and Pamela J. Furman, *FDA Considerations Related to Maintaining Clinical Trial Records in Electronic Form,* Health Lawyers News (December 2004).

1-2(d). Law Enforcement Disclosures

HIN Participants should define the process by which a HIN may disclose health information to law enforcement agencies, or by which the HIN Participants may disclose health information that originates in a different HIN Participant. For example:

- If one participant is served with a compulsory disclosure request, such as a grand jury subpoena or a search warrant, may a HIN Participant or the HIN disclose health information to law enforcement beyond health information that originated with that HIN Participant? If so, what type of notice, if any, must the HIN Participant provide to the other HIN Participants before the disclosure?
- How will the HIN Participants apportion liability if a HIN Participant improperly releases health information to law enforcement agencies?
- If the HIN has HIN Participants in multiple states, who will be responsible for determining compliance with the different state laws regarding disclosures to law enforcement, which vary widely?
- Who will be responsible for any accountings of disclosures?

1-2(e). Fundraising Disclosures

The HIPAA Privacy Rule strictly limits the elements of health information that may be used or disclosed for fundraising purposes, and state laws also may apply to these disclosures. The Privacy Rule permits a covered entity to disclose only patient names and other demographics and dates of healthcare to an institutionally-related foundation or a business associate, but that information may be used only for the fundraising of the disclosing covered entity.[35] Therefore, the HIN must limit HIN Participants' access to other Participants' health information in accordance with these rules, and must establish rules for which entity will monitor which patients have opted-out of receiving fundraising requests.

1-2(f). Marketing Disclosures

The Privacy Rule's provisions on marketing are even more restrictive,[36] and some state laws prohibit marketing with patient health information entirely.[37] Indeed,

---

[35] 45 C.F.R. § 164.514(f).
[36] 45 C.F.R. § 164.508(a)(3).

there is real potential for liability for violating the marketing rules, as privacy advocacy groups have argued that misuse of health information for marketing purposes are egregious violations of patient privacy, in part because misuse is alleged to be motivated by financial gain.[38] As a result, a HIN will need to consider carefully at the time of its formation whether it will allow disclosures for marketing purposes, and if so, to what extent. Allowing marketing disclosures may be particularly difficult in HINs that include a large number and wide variety of HIN Participants (particularly where the HIN Participants hail from different states), or where patient authorization is logistically difficult to obtain (such as in a Community Health Record type of HIN).

1-2(g). Compliance with State Laws

There are many state laws that limit the ability to use and disclose health information. In particular, laws that protect highly sensitive information, such as those regarding HIV/AIDS, mental health, substance abuse treatment, developmental disability, and genetic testing, operate on the fundamental premise that the use and disclosure of this sensitive health information is prohibited unless specifically permitted by the law. Violations of such laws may subject the offender to criminal or civil sanctions or to disciplinary action by state licensing authorities. A HIN should consider carefully how this sensitive health information will be included in the system:

- Will this sensitive information be integrated in the EHR and fully available to all HIN Participants? If so, how will the HIN Participants be protected against others' misuse of this information?
- Will this sensitive information be segregated into an electronic "lock-box" that requires special access rights? Does segregating this health information and thus making it less accessible to care providers, pose a risk to patients by depriving potential care givers of complete information?
- If the HIN includes providers or plans from more than one state, how will the HIN structure accommodate differing state laws on the protection of this sensitive information?

---

[37] Confidentiality of Medical Information Act, Civil Code §§ 56-56.07 (restrictions on marketing).
[38] *See*, *e.g.*, the "medical information used for marketing" stories collected by the Health Privacy Project, available at: http://www.healthprivacy.org/usr_doc/Privacy_storiesupd.pdf.

In determining whether these state laws will apply to the HIN, counsel must determine whether these state laws are preempted by HIPAA. The HIPAA regulations preempt "contrary" provisions of state law, with certain exceptions.[39] A state law is "contrary" if a covered entity would find it impossible to comply with both the state law and HIPAA, or if the state law is an obstacle to accomplishment of full purposes and objectives of HIPAA.[40] Therefore, if the covered entity cannot comply with both state and federal requirements—the covered entity would actually violate one law by following another—the state law would be contrary to the HIPAA regulations.

Even where a state law is contrary to the HIPAA regulations, however, the state law would not be preempted in four circumstances: (1) The DHHS Secretary has determined that the state law is necessary to prevent fraud and abuse, to regulate insurance and health plans, or to report on healthcare delivery and other purposes, or that the state law regulates controlled substances; (2) the state law "relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter" [the Privacy Rule]; (3) the state law provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention; or (4) the state law requires certain health plan reporting.[41]

1-2(h). Dealing with Unauthorized Downstream Disclosures

Even when the Privacy Rule and other applicable laws permit the use or disclosure for specific purposes without patient approval (such as for treatment, payment, and healthcare operations), significant questions arise about the potential for unauthorized "downstream" use, disclosure, or re-disclosure of such health information for non-permitted purposes. In creating the HIN, HIN Participants should consider whether any additional safeguards can or should be established to govern the use, disclosure, or re-disclosure of health information by HIN Participants.

---

[39] 45 C.F.R. § 160.202.
[40] 45 C.F.R. § 160.202.
[41] 45 C.F.R. § 160.203.

1-3. Verifying Identity and Authority of Persons and Entities Accessing EHR

Any time a HIN or HIN Participant discloses health information to a third party, the HIN or HIN Participant must verify the identity of the party requesting the health information and that party's authority to have access to the information, unless the identity and authority of such requesting HIN Participant or other party is known to the disclosing HIN Participant.[42] What structure has been chosen for the HIN will greatly impact how verification is handled.

In a Pointer System, each HIN Participant will retain the responsibility for verifying the identity and authority of the requestor. Thus, the sending HIN Participant will have to interact with the requesting HIN Participant to determine, among other things, the purpose of the requested disclosure and the validity of the request, including the requester's identity and authority to access the information. Unless the HIN is set up with this restriction in mind, these procedural hurdles may act as impediments to efficient communication of health information. Accordingly, HINs and HIN Participants may wish to establish mechanisms, including lists of trusted HIN Participants or use of codes that can readily confirm a requesting HIN Participant's identity The HIN itself also might, consistent with its role in this model as an intermediary, confirm a requesting HIN Participant's authority to access information.

Under the Data Warehouse-Silo System HIN model, HIN Participants most likely will look to the HIN to be responsible for ascertaining the purposes of requests for health information and verifying a requesting HIN Participant's identity and authority to access the health information, because the HIN (or a designated HIN Participant or business associate), will be pulling and distributing the health information to other HIN Participants. Because of this reliance, a HIN of this model should expect HIN Participants to demand assurances that the privacy of their health information is being appropriately protected by the HIN. To meet these concerns without creating undue impediments to sharing health information for appropriate purposes, the HIN should consider establishing mechanisms to determine the purposes of permitted disclosures.

---

[42] 45 C.F.R. § 164.514(h)(1).

If the HIN operates under the Community Health Record System model, as in the Data Warehouse-Silo System model, the HIN will have to establish protocols for the HIN to process the requests of HIN Participants, including mechanisms to efficiently verify a requesting HIN Participant's identity and authority to access the health information to meet the stated goals of the HIN/EHR system.

1-4. Complying with the Minimum Necessary Standard

HIN Participants must coordinate closely regarding how they will achieve compliance with the HIPAA Privacy Rule's "minimum necessary" requirements for use and disclosure of health information through the HIN. A HIN may involve many different types of uses and disclosures of health information among participating covered entities. The HIN design and architecture of shared information systems should consider the following:

- What type of workforce members will be permitted to access health information from the HIN? What conditions should be placed on that access, and how will those conditions be enforced? Will the HIN create technological mechanisms to restrict access to health information, such as access controls, auditing of access, and authentication of users? (*See* Chapter 2, Security.)
- How will the HIN exempt disclosures for treatment purposes from the minimum necessary standard? In other words, how will the HIN establish that a request for access is for treatment?
- How will the HIN Participants establish the minimum amount of health information for disclosures for payment or healthcare operations?
- What are other routine disclosures and requests that the HIN Participants may make, that can be identified in advance and accommodated in the HIN rules?
- How will non-routine disclosures be handled? Will the HIN or an individual HIN Participant be responsible for the minimum necessary documentation on these requests?
- How will assurances from business associates be secured to limit PHI uses, discloses, and requests only the minimum necessary amount of health information?

- How will the HIN determine and implement any state law restrictions on the amount of health information to be used or disclosed?

1-5. Individual Rights

The Privacy Rule, as well as a number of state laws, impose obligations to honor various rights of individuals with respect to their health information. For example, individuals have rights to access and request amendments to their information, to be informed of the privacy practices of the covered entity, and to request various protections to their health information.

Although in most cases the HIN itself will not be a HIPAA covered entity and may not be directly covered by many state requirements, the HIN likely will be significantly affected because such privacy requirements will apply to most of the HIN Participants. In setting up the HIN, the HIN Participants should decide whether they wish to adopt a centralized approach, a decentralized approach, or a combination approach in addressing individual rights.

Under a centralized approach, the HIN itself or an identified HIN Participant acting as an agent of the other Participants would assume responsibility for implementing individual rights. Such an approach would provide for more consistency for the individual patients or members. The disadvantage of this centralized approach, however, is that it will impose technical and practical burdens on the HIN, which may distract from its core mission and result in additional costs of operation. It also may be difficult to create rules with enough specificity to address all conceivable situations with regard to individual rights, such that the HIN can implement these requirements without consultation with the individual HIN Participants. Finally, some HIN Participants may prefer to implement these requirements on their own, as these requirements directly impact customer service and patient satisfaction efforts.

Alternatively, a HIN may adopt a decentralized approach to responding to individual rights, either by having each HIN Participant continue to respond individually, or by having each HIN Participant follow pre-established rules for responding individually to requests. While providing more control to the HIN Participants may reduce costs for the HIN, the disadvantage to this approach is that patients and

members may be confused by different approaches, particularly where their health information is held by different HIN Participants.

The following sections explore issues raised by particular individual rights.

1-5(a). Right to Access and Obtain Copies of Health Information

Under the Privacy Rule and many state laws, individuals (or their personal representatives) may access, and receive copies of, their own health information.[43] Responding to requests for access to health information, as well as denials of access and implementing appeal processes, represents a significant challenge for HINs, regardless of the model chosen.

If a centralized model is chosen, HIN Participants will need to create express rules to govern the HIN's processing of the requests for access that comply both with HIPAA and relevant state laws. This approach may include situations in which the HIN will need to consult with one or more HIN Participants in making its decision, such as when a licensed healthcare professional has determined that provision of access is reasonably likely to endanger the life or physical safety of the individual or other person. If a decentralized model is chosen, each HIN Participant will be individually responsible for administering the right to access health information, although the HIN will have to address whether the HIN Participants may access other Participants' records when responding to individual requests for access.

In creating a system to respond to requests for access, HIN Participants must determine what constitutes a "designated record set" under HIPAA for purposes of individual access to the records.[44] For example, in the Community Health Record model, is the designated record set the individual's entire health record that is maintained in the EHR? In the Pointer System, does the designated record set include other HIN Participants' records? The OCR may need to clarify how the term "designated record set" fits within the HIN context, particularly as the application may change based on the HIN model. HIN Participants also will need to review state law to determine if other definitions of health information or rights to access apply.

---

[43] 45 C.F.R. § 164.524.

[44] 45 C.F.R. § 164.524(a) (right to access designated record set); 45 C.F.R. § 164.501 (defining designated record set).

1-5(b). Right to Amend Health Information

Covered entities must give individuals the right to request amendment of their health information, if that information is incomplete or erroneous.[45] HIN Participants will need to address routing and processing of amendment requests, the grounds for denial, and processes for appeal. If HIN Participants decide to centralize amendment responsibilities within the HIN, HIN Participants will need to provide detailed guidance regarding the criteria to apply in evaluating amendment requests that comply both with HIPAA and applicable state laws. Given that risk management considerations dictate different methods of responding to requests for amendment, it may be difficult to arrive at a set of substantive and procedural rules for the HIN to apply in a centralized model.

For a decentralized model, the challenge will be how to communicate amendments to other HIN Participants that have incorporated the individual's health information into their own records. HIN Participants thus will need to address documentation in the EHR of requests for amendments, grants or denials of those requests, and resolutions of any subsequent "appeals."

1-5(c). Accounting of Disclosures of Health Information

Covered entities must log certain disclosures of health information to include in an accounting upon request of the individual.[46] As is the case with other individual rights, requests for accountings of disclosures received by the HIN would need to be routed promptly to the relevant responder. If a centralized HIN is being considered, the HIN Participants would need to determine whether it is possible or feasible for the HIN to log all disclosures for which an accounting is required, and how the HIN will respond to the individual. Moreover, in a centralized process, the HIN Participants will have to determine what type of database of such disclosures will be maintained and how HIN Participants will contribute to the database.

In a decentralized model, the HIN Participants should consider establishing parameters for systems to track disclosures and agree on the particular disclosures and the amount of information to be tracked, so that individuals obtain consistent accounting

---

[45] 45 C.F.R. § 164.526.
[46] 45 C.F.R. § 164.528.

information from each HIN Participant that holds their health information. Moreover, the HIN Participants should address whether a Participant's response to a request for accounting should include accounting of disclosures provided by another HIN Participant and reflected in the HIN records.

1-5(d). Requests for Alternate Confidential Communications

If the HIN will transmit communications of health information to individuals on behalf of HIN Participants (such as appointment reminders, treatment follow-up, Explanation of Benefits, and other communications), then the HIN must be able to offer alternate means of communication, such as alternate mailing addresses or telephone notification of results.[47] If a centralized process is used, then the HIN itself will make decisions about alternative modes of communication. If a decentralized process is used, the HIN will need to develop processes for the HIN Participants to communicate its agreements about alternative communications with individuals to the HIN. If this approach is used, the HIN Participants should consider placing restrictions on the Participants' ability to agree to communicate with individuals in ways that are not reasonably feasible.

1-5(e). Requests for Restrictions on Use and Disclosure for Treatment, Payment, and Healthcare Operations

Under the HIPAA Privacy Rule, individuals have the right to ask a covered entity not to use or disclose their health information in a manner otherwise permitted by the rule (for example, not to disclose their health information to a health insurance company for payment purposes). In setting up the HIN, the HIN Participants will have to determine whether the HIN or each HIN Participant will make the decisions regarding individual requests for privacy restrictions.

If a centralized approach is taken where the HIN itself makes the decisions, HIN Participants will pass requests received by their patients to the HIN, which then will make the decision and implement the agreement with the individual as to any subsequent use and disclosure made by the HIN.

---

[47] 45 C.F.R. § 164.522(b).

If a decentralized approach is used, implementing individual requests may become particularly complicated. For example, if one HIN Participant grants a restriction request for an individual, but another HIN Participant denies the request from the same individual, the HIN would be required to carry out different directions relating to health information coming from different HIN Participants with respect to the same individual. This situation obviously could be avoided in advance in designing the HIN. If a decentralized approach is taken and the HIN Participants will handle the requests, the HIN should develop processes for HIN Participants to communicate to the HIN any privacy restrictions granted to individuals. For example, in the case of a HIN that does not hold the health information but acts as a Pointer System, as long as the HIN Participant controls the dissemination of the information relevant to the granted privacy restriction, the individual restrictions are met. In this situation, the HIN should avoid any duty to point to a healthcare provider with PHI about a particular individual, which could present a significant technical hurdle.

1-5(f). Notice of Privacy Practices

The Privacy Rule requires covered entities to provide their patients or members with a notice of privacy practices (NPP).[48] In setting up the HIN, the HIN Participants should determine whether they want to use: (a) single, joint NPP if the HIN is structured as an OHCA (*see* Section 1-1(c) above); (b) separate NPPs that contain common required language, such as language to describe the HIN or common language to avoid conflicting descriptions of the HIN or conflicting rules regarding implementing individual rights; or (c) completely different NPPs. Moreover, the HIN will have to establish processes to carry out applicable NPP provisions. If different NPPs are used, the HIN may have to comply with different (and sometimes conflicting) provisions of the multiple NPPs of its participants.

State law may significantly affect the NPPs of HIN Participants. Some HIN Participants will be required under state laws to provide notices giving individuals the right to opt-out or opt-in to certain types of disclosures (generally for purposes other

[48] 45 C.F.R § 164.520.

than as necessary to treat or to provide health insurance coverage).[49] If health insurers are involved in the HIN, they may have a duty to provide NPPs that also meet state insurance laws that implement the Gramm Leach Bliley (GLB) Act.[50] These state requirements for notice must be considered in setting up the HIN and in designing the method of providing notice.

1-6. Administrative Requirements

The Privacy Rule and many state laws impose administrative requirements on most HIN Participants, including standards for training the workforce, imposing sanctions on workforce members who violate an institution's policies, handling complaints, mitigating the effect of violations on individuals, and documenting compliance.[51] To handle these administrative requirements, the HIN Participants should determine whether or not they will centralize the handling of these standards, or whether the individual HIN Participants will manage the administrative obligations at the institutional level. Multiple users of health information may make it more difficult to track, mitigate, and cure privacy breaches related to that health information unless sophisticated personal identity management and other protocols are implemented in advance.

1-6(a). Conducting Workforce Training

HIN Participants should consider centralizing or at least standardizing training related to the operation of the HIN. Centralized training or standardized requirements for training would ensure that all HIN Participants' workforce receive a minimum level of training. HIN Participants most likely will continue to handle workforce training with regard to their individual institutions, although the HIN could provide contracted assistance with regard to the individual institutions.

1-6(b). Implementing Workforce Sanctions

Sanctions for violations among HIN Participants may raise similar complexities and should be well documented and communicated. If the HIN Participant handling the complaint process is different than the HIN Participant whose workforce member

---

[49] *See, e.g.,* California Financial Information Privacy Act, California Financial Code § 4050 et al.
[50] *See, e.g.,* Insurance Information and Privacy Protection Act, Insurance Code §§ 791-791.27.
[51] 45 C.F.R. § 164.530(b), (e), and (f).

committed the policy or procedure violation, only the workforce member's employer may of course impose sanctions, although a different entity may assist in or conduct the investigation. Keep in mind, however, that a third party's investigation may not be protected under attorney-client or work product privilege in the event that litigation develops from the incident.

1-6(c). Handling Complaints

The HIN Participants should consider centralizing the process for handling complaints and sanctions related to the operation of the HIN, or that involve two or more HIN Participants. The complaint process should address complaint "ownership" and disposition. For example, if an alleged breach occurred with HIN Participant X's health information by HIN Participant Y's workforce, the process should contemplate whether Participant X (the owner of the information) or Participant Y (the employer) will handle the complaint *vis-a-vis* the individual. For example, the HIN Participants might agree that the first entity that receives the complaint investigates the complaint and processes it on behalf of other affected entities, or the Participants might agree that the entity that is subject of the alleged violation handles the complaint. The HIN Participants should agree upon channels of communication for complaint disposition. Again, HIN Participants need to be sensitive to the issue of attorney-client and work-product privileges in conducting investigations of complaints that may develop into litigation.

In the NPP, the HIN (or individual HIN Participants) should clarify to whom a patient or member may complain if there is a problem. An individual whose health information is improperly used or disclosed through a HIN may have difficulty in identifying where the complaint should be made. It will not be unusual for one HIN Participant to receive a complaint and, after investigation, to discover that another HIN Participant is the cause of the breach. Uncertainty as to which HIN Participants committed a breach could foster complaints (or additional complaints) to the Office for Civil Rights (OCR) of DHHS, which may trigger investigation of multiple HIN Participants to ascertain the cause of a single breach. To avoid this, HIN Participants may insist that HINs provide electronic tracking mechanisms to identify and isolate the sources of health information misuse.

1-6(d). Mitigating the Effect of Violations

The HIN Participants should agree upon what steps each will take to mitigate harmful effects resulting from actions taken by members of their workforce on another HIN Participant's health information or patient or member. To the extent that the HIN has established itself as a single covered entity or an OHCA, HIN Participants may desire to protect themselves by including indemnification or contribution provisions in the HIN governing documents.

CHAPTER 2:
SECURITY

In this Chapter, we will discuss the legal issues that may arise with respect to HINs under the HIPAA security standards[52] (the Security Rule). These issues are likely to be presented by any of the structures used for a HIN, including the Pointer/Locator system, the Data Warehouse/Silo system, and the Community Health Record system described in the Introduction to this Briefing.

The HIPAA Security Rule requires covered entities to "ensure the confidentiality, integrity and availability of electronic protected health information"[53] (often referred to as EPHI). *Confidentiality* of EPHI is necessary for compliance with the HIPAA Privacy Rule and for the public to have confidence that EPHI has not been improperly disclosed or made available through the HIN. Perhaps less visible to the public but equally important to an effective HIN are the goals of *integrity* (to assure that the EPHI has not been improperly altered or destroyed) and *availability* of EPHI when needed (to ensure continuity of care). Both integrity and availability of EPHI are essential to improve patient safety and reduce medical errors.

Security issues presented by HINs and EHRs will vary depending on the structure of the HIN, the identity of the participants in the arrangement and its operations. Our discussion focuses on a HIN with multiple participants, but substantially the same issues would be presented by an interoperable EHR used by a small group of providers. Due to space constraints, this Chapter will assume the reader is already generally familiar with the legal requirements of the Security Rule and the HIPAA Privacy Rule (*see* Chapter 1, Privacy).

2-1. General Requirements

The Security Rule contains general provisions that require covered entities to:

- Ensure the confidentiality, integrity, and availability CIA of all EPHI that the covered entity creates, receives, maintains or transmits;

---

[52] 45 C.F.R. Parts 160, 162 and 164, published at 68 Fed. Reg. 833 (2003).
[53] 45 C.F.R. § 160.304.

- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the Privacy Rule; and
- Ensure compliance with the Security Rule by its workforce.[54]

To reach these goals, the Security Rule requires covered entities to implement three types of safeguards—administrative,[55] physical,[56] and technical.[57] Each of these safeguards contain "standards," some of which have additional "implementation specifications," or further details to implement the standards. To account for both the speed of advancing technology available to implement the safeguards and the need for flexibility in implementing safeguards by covered entities of varying sizes, DHHS designated the implementation specifications as "required" or "addressable."[58] A "required" implementation specification must be implemented by the covered entity as described in the Security Standards, although the technology neutrality in the Security Rule provides some flexibility to covered entities in the implementation. In contrast, the "addressable" implementation specifications require the covered entities to determine whether it is reasonable and appropriate, then the covered entity may: (a) implement the implementation specification as described in the Security Rule; or (b) if implementing the specification is not reasonable and appropriate, (i) document why it would not be reasonable and appropriate to implement the implementation specification; and (ii) implement an equivalent alternative if reasonable and appropriate, or do nothing, if that is the conclusion documented in the risk analysis.

Whether the covered entity performs the HIN functions itself or participates in a HIN structure with services provided by a third party, the covered entity must determine how to comply with the Security Rule in the context of its particular HIN. The compliance analysis will depend on many factors, including the details of how EPHI is generated,

---

[54] 45 C.F.R. § 164.306(a).
[55] 45 C.F.R. § 164.308.
[56] 45 C.F.R. § 164.310.
[57] 45 C.F.R. § 164.312.
[58] 45 C.F.R. § 164.306 (d).

transmitted, altered and stored and the security levels of other HIN participants. This Chapter will discuss those standards and implementation specifications likely to be of significance to establishing a HIN, but it should not be regarded as a full checklist for Security Rule compliance. Due to the variations in HIN structures and the likelihood that new approaches to EHRs and HINs will evolve over time, counsel must carefully consider all aspects of Security Rule compliance in advising their clients.

2-2. The "Flexibility" of the Security Rule

A covered entity may use any security measure that allows the covered entity to "reasonably and appropriately" implement the standards and implementation specifications. The "reasonable and appropriate" provision permits a covered entity to comply with the Security Rule by considering factors such as its own size, complexity and capabilities, the sophistication of its information system infrastructure, the costs of implementing a particular safeguard, and the level of various risks to EPHI within that covered entity's organization.[59]

This flexibility presents a challenge in the context of HINs, because each covered entity may customize its approach to implementing the standards and implementation specifications. Large and sophisticated covered entities, for instance, may establish expensive state-of-the-art data backup and disaster recovery procedures, to recapture the loss of data from multiple servers. By contrast, to comply with the same standards, a small physician's office may utilize an external "back-up" hard disk purchased off the shelf from the local computer store. Both would appear to be compliant with the Security Rule despite disparate solutions, although the disparity may create a weak link in the HIN chain for the more sophisticated participant. Moreover, some HINs may include non-covered entity participants who are not subject to the HIPAA Security Rule at all, which certainly raises a concern that the HIN Participants who maintain the weakest security measures in the network could compromise data.

Consequently, in order to promote confidence by HIN Participants and the public, a HIN will need to determine whether the HIN itself, as well as all HIN Participants, should impose uniform or minimum security requirements on the HIN Participants. To

---

[59] 45 C.F.R. § 164.306 (b).

the extent that this security bar is set too low, patients may not trust that their electronic records are secure or covered entities may refuse to participate, fearing intrusion into their data. If that bar is set too high or made too inflexible, smaller covered entity participants may not be able to participate, because they lack the sophistication, infrastructure, or capability to comply.

Moreover, even if minimum security requirements are established for the HIN participants, the HIN Participants must determine how Participant compliance will be confirmed and monitored by the HIN, and whether contractual obligations to comply will provide adequate assurances for the HIN Participants. One potential option to address this barrier would be to establish a nationally-recognized security certification or accreditation process to instill public confidence, perhaps with periodic review required of the HIN Participants. Of course, establishing any threshold security requirements or imposing any certification or accreditation process likely will increase costs to the HIN and HIN participants and may be a barrier to participation unless funded by the HIN. Moreover, if the HIN Participants have taken a different approach to compliance with the Security Rule and are required to implement different security measures to meet the HIN's chosen standards, that will impose additional costs on the Participants. Further complicating the issue, if multiple HINs impose multiple different minimum security requirements, such variability could pose an impediment to the establishment of an interoperable National Health Information Network (NHIN).

2-3. Risk Analysis and Management

The starting point for security compliance is the first administrative safeguard standard, entitled "security management process." This standard requires covered entities "to implement policies and procedures to prevent, detect, contain and correct security violations."[60] Risk analysis and risk management, two of the implementation specifications for this standard, are central to selecting and implementing security measures to comply with the Security Rule. To comply with the Security Rule, a covered entity must review and understand the goals and requirements of the regulations, the

[60] 45 C.F.R. § 164.308(a)(1)(i).

importance of risk analysis in evaluating appropriate safeguards and the significance of risk management in establishing and maintaining effective security practices.

Most covered entities participating in a HIN will have already performed the required risk analysis and implemented security policies and procedures because the deadline for compliance with the Security Rule was April 20, 2005 (with an extra year for small plans). However, in joining or creating a HIN and receiving services from a BA or providing HIN services itself, a covered entity will need to assess how the HIN will affect its security risks and the procedures that it has put in place to address security concerns. For example, if the entity providing HIN services or the HIN Participants are significantly less secure than the covered entity, it might elect to not join the HIN if participation would materially increase the covered entity's risk in a way that it could not effectively mitigate.

The following sections provide examples of Security Rule provisions that are likely to present challenging compliance issues for HINs and their participants.

2-4. Information Access Management

This administrative standard requires covered entities to implement policies and procedures for authorizing access to EPHI that are consistent with the Privacy Rule.[61] It is tied directly to the minimum necessary standard of the Privacy Rule,[62] and has three implementation specifications:

Isolating healthcare clearinghouse functions (Required). If any entity within the HIN is a healthcare clearinghouse and is part of a larger organization that is a clearinghouse, policies and procedures must be implemented to isolate and protect the EPHI used for clearinghouse functions from access by parts of the organization that are not involved in clearinghouse activities.[63]

Access authorization (Addressable). Policies and procedures must be implemented for granting access to EPHI,[64] including access to a workstation, transaction, program, process, or other mechanism. Within a single covered entity,

---

[61] 45 C.F.R. § 164.308(a)(4).
[62] 45 C.F.R. § 164.502(b).
[63] 45 C.F.R. § 164.308(a)(4)(ii)(A).
[64] 45 C.F.R. § 164.308(a)(4)(ii)(B).

compliance usually requires coordination between human resources, the department that hires the individual and the IT department, which controls technical mechanisms for granting access. In a HIN, procedures must be established that will coordinate these functions across all of the participants.

Access establishment and modification (Addressable). This specification requires policies and procedures that, based upon the covered entity's access authorization policies, will establish, document, review and modify a user's right of access to a workstation, transaction, program, or process.[65] This requirement will also need to be coordinated across a HIN's Participants to satisfy this requirement without undue delay in granting or revoking authorization.

2-5. Access Controls

This standard is the technical counterpart to the administrative security safeguard establishing, modifying, or terminating system access rights.[66] It limits access to systems or applications to only those persons or software programs that have been granted access rights.[67]

Unique user identification (Required). In order to gain access to a system or application, each user must be provided a unique name and/or number. This identifier can be used to control access and to identify and track system users. The HIN will need to implement an adequate mechanism to accomplish this requirement across multiple covered entities. The accurate identification of users is critical to audit controls, activity logging, and other security mechanisms. It may be necessary to have unique identifiers for each individual user at each HIN Participant rather than just identifying the Participant, although the Security Rule is not entirely clear on this point.

Emergency access procedure (Required). As the name suggests, this specification requires procedures to obtain necessary EPHI during an emergency.[68] This is a procedure that will be part of a covered entity's contingency plan to allow rejection of access controls in emergency situations. For example, if a disaster occurs in

---

[65] 45 C.F.R. § 164.308 (a)(4)(ii)(C).
[66] 45 C.F.R. § 164.308(a)(4).
[67] 45 C.F.R. § 164.312(a)(1).
[68] 45 C.F.R. § 164.312(a)(2)(ii).

which the two persons with "root system access" are unavailable due to injury, these procedures would give another person or persons a method to override access controls. This procedure must balance the need for access against the other security measures guarding the confidentiality, integrity, and availability of EPHI during disasters.[69]

Encryption and decryption (Addressable). Covered entities must consider whether encryption and decryption of EPHI is a reasonable and appropriate safeguard, in addition to standard access controls.[70] The encryption mechanisms in this specification are for EPHI at rest, as opposed to EPHI in transit. EPHI in transit is covered by the transmission security standard discussed in Section 2-8 below.

2-6. System Activity Reviews and Audit Controls (Required)

Covered entities must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking.[71] The audit control requirements of the technical safeguards are the technical companion to information system activity reviews. They require hardware, software, and/or procedural mechanisms to record and examine activity in information systems containing or using EPHI.[72] Compliance with these requirements has proved to be challenging for stand alone covered entities and will be much more complex in a HIN context. For example, covered entity participants in a HIN will need to address how audit logs will be maintained and examined and how security incidents will be monitored and handled.

2-7. Integrity and Authentication (Addressable)

This technical standard will be met by implementing procedures to verify the identity of a person or entity seeking access to EPHI.[73] Authentication may be provided by something the user knows (e.g., a password), something the user has (e.g., a token) or something the user is (e.g., biometric characteristics). The procedures selected must be available to all members of the HIN but there is no requirement that all individuals or entities use the same procedure.

---

[69] 45 C.F.R. § 164.308(a)(7).
[70] 45 C.F.R. § 164.312(2)(iv).
[71] 45 C.F.R. § 164.308(a)(1)(ii)(D).
[72] 45 C.F.R. § 164.312(b).
[73] 45 C.F.R. § 164.312(d).

2-8. Transmission Security

This standard requires implementation of technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.[74] HINs may face challenges in determining what level of technical protection is appropriate for this standard if the members of the HIN are at different levels of technical sophistication.

Integrity controls (Addressable). Security measures should be implemented to ensure that electronically transmitted EPHI is not improperly modified without detection until destroyed.[75] Alternatives commonly considered include one-way hashing, message authentication, or digital signatures for EPHI transmitted over the Internet.

Encryption (Addressable). The covered entity is required to implement a mechanism to encrypt EPHI that is being transmitted whenever deemed appropriate.[76] The preamble to the Security Rule states that some forms of transmission, including dial-up lines, have a small probability of interception so encryption generally would not be required. The burden of encryption on small and rural providers was also noted. However, covered entities were "encouraged" to consider using encryption, particularly for transmissions of EPHI over the Internet.[77]

Encryption is an example of the challenges presented in standardizing processes across HIN Participants. A number of encryption products currently are available, and covered entities may already have adopted different methods or products to encrypt data during transmission. The HIN will not be interoperable unless the encryption mechanisms and keys work easily between the HIN and HIN Participants.

2-9. Isolating Healthcare Clearinghouse Functions

If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures to isolate and protect the EPHI of the clearinghouse from unauthorized access and use by the larger organization.[78] If the HIN or a HIN Participants functions as a healthcare clearinghouse (*see* Chapter 1), counsel

---

[74] 45 C.F.R. § 164.312(e)(1).
[75] 45 C.F.R. § 164.312(e)(2)(i).
[76] 45 C.F.R. § 164.312(e)(2)(ii).
[77] 68 Fed. Reg. 8356-8357.
[78] 45 C.F.R. § 164.308(a)(4)(ii)(A).

should consider whether or how those clearinghouse functions should be separated from the other HIN functions.

2-10. State Regulation of Security

While few states today have laws or regulations specifically addressing the security of electronic health records, such laws inevitably will be passed as EHRs become more common. For example, states may have laws regulating computer security, mandating security breach reporting, requiring specific steps for introduction into evidence, prohibiting or allowing electronic signatures in different situations, or combating identity theft.

If these state laws differ from the Security Rule requirements, counsel must determine whether those state laws are preempted by the federal regulations. The HIPAA regulations preempt "contrary" provisions of state law, with certain exceptions.[79] A state law is "contrary" if a covered entity would find it impossible to comply with both the state law and HIPAA, or if the state law is an obstacle to accomplishment of full purposes and objectives of HIPAA.[80] Therefore, if the covered entity cannot comply with both state and federal requirements—the covered entity would actually violate one law by following another—the state law would be contrary to the Security Rule.

Even where a state law is contrary to the HIPAA regulations, however, the state law would not be preempted in four circumstances: (1) The DHHS Secretary has determined that the state law is necessary to prevent fraud and abuse, to regulate insurance and health plans, or to report on healthcare delivery and other purposes, or that the state law regulates controlled substances; (2) the state law "relates to the privacy of individually identifiable health information and is more stringent than a standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter" [the Privacy Rule]; (3) the state law provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation or intervention; or (4) the state law requires certain health plan reporting.[81]

---

[79] 45 C.F.R. § 160.202.
[80] 45 C.F.R. § 160.202.
[81] 45 C.F.R. § 160.203.

None of these exceptions likely are applicable to the Security Rule, although counsel should monitor developments in this area.

By way of example, California recently passed a law requiring businesses (including healthcare providers) to report breaches of the security of unencrypted electronic "personal information," defined broadly enough to include most forms of EPHI.[82] The Security Rule also requires reporting of "security incidents"[83] but does not specify to whom the incidents must be reported.[84] The California law is not contrary to the Security Rule, because it does not contain provisions that, if followed, would result in violating the Security Rule.

Because the Security Rule is flexible and does not specify particular methods to reach the required security goals, state laws are unlikely to be preempted by the Security Rule. These state laws will affect HIN design and operations, and may indeed impede the formation of multi-state HINs.

---

[82] *See* California Civil Code section 1798.82.
[83] 45 C.F.R. § 163.308(a)(6).
[84] In response to a comment in the Final Rule, DHHS states: "This regulation does not specifically require any incident reporting to outside entities. External incident reporting is dependent upon business and legal considerations." 68 Fed. Reg. 8350 (February 20, 2003).

CHAPTER 3:
STARK AND ANTI-KICKBACK

3-1. The Stark Law

The federal physician self-referral prohibition (the Stark Law) [85] prohibits a physician from referring Medicare patients for certain designated health services (DHS) to an entity with which the physician has a financial relationship, unless an exception applies. The Stark Law is notorious for both its breadth and ambiguity. Given that virtually any exchange of remuneration with a physician could potentially create a financial relationship, the Stark Law prohibitions must be considered if the development of an electronic health record (EHR) is directly or indirectly funded by a hospital, health system, or any other entity furnishing DHS, such as a large physician group. There are essentially two approaches to addressing the Stark issues: (1) construe the establishment of the EHR network as not constituting remuneration to the physician users; or (2) identify one or more Stark exceptions and structure the physicians' relationships with the network to fit within the exceptions.

3-1(a). No Remuneration

Some industry observers have argued that the establishment of an EHR network does not change the fundamental obligation of hospitals and other providers to share information with physicians and others relating to common patients. Historically, hospitals have shared information by copying records, using a fax machine, and employing other lower-tech methods of transmitting data. Thus, the establishment of an EHR network by a hospital, without more, does not necessarily change the fundamental "benefit" a hospital provides to a physician when it transmits data to a physician concerning his or her hospital patients. Indeed, the Preamble to the most recent Stark regulations supports this analysis. In the Preamble, the Centers for Medicare and Medicaid Services (CMS) states that a "hospital's provision of a computer or other technology that is wholly dedicated to use in connection with hospital services provided to the hospital's patients would be for the hospital's benefit and convenience and would

[85] 42 U.S.C. § 1395nn; 42 C.F.R. Parts 411 and 424.

not constitute remuneration" for the purposes of the Stark Law.[86] In other words, merely providing access to a entity's clinical information to provide treatment will most likely not constitute "remuneration" triggering the Stark referral prohibition. Arguably, the benefit to the physician—access to the patient's medical information—is the same whether hard copies are delivered to her door or an electronic copy is downloaded from her computer.

However, where the computer and software provided to the physician permits the physician to communicate with entities other than the entity that provided the computer and software, as would be the case in a community-wide interoperable EHR where many providers in the community would use the system to communicate patient information, it falls outside of the narrow activity blessed by CMS in its Comments. Similarly, where the electronic medical record platform provides more than access to patient information, such as medical decision support or access to an electronic medical library, it also falls outside of comfortable parameters.

Therefore, counsel advising in establishing a HIN carefully should consider the manner in which the network sponsor makes information available to providers in the community and whether services outside access to the sponsor's information are provided. For example, will a hospital sponsor be providing computer hardware, whether desktop or mobile, to the physician so that she can access the network? If the hospital is not providing hardware, is it providing software or paying license fees associated with connecting to the network? If hardware or software is provided, may it be used for purposes other than connecting to the network? If the answer to any of these questions is "yes," counsel should consider structuring the HIN to meet an exception to the Stark Law, discussed below.

DHHS (and the Office of Inspector General (OIG)) in connection with enforcement of the Anti-Kickback Law) should consider issuing direct guidance as to when the provision of EHR technology free or below cost will not be viewed as illegal remuneration.

---

[86] 69 Fed. Reg. 16,054, 16,113 (Mar. 26, 2004).

3-1(b). Potential Stark Exceptions

At least four Stark exceptions may be useful in the context of establishing an interoperable EHR. Each of the exceptions has specific requirements and limitations, and the configuration of the network will determine which exception is most useful.

3-1(b)(1). Non-Monetary Compensation Up to $300

The Stark Law includes an exception for non-monetary compensation up to $300 per year.[87] This exception allows a referring physician to receive compensation from an entity in the form of items or services (not including cash or cash equivalents) that does not exceed an *aggregate* value of $300 per year. In other words, the total amount of other non-monetary benefits the hospital (or network sponsor) provides to the physician on an annual basis must not, collectively, exceed $300.

Any form of non-monetary compensation can be used under this exception so long as the following conditions are met:

- The compensation is not determined in any manner that takes into account the volume or value of referrals or other business generated by the referring physician;[88]
- The compensation may not be solicited by the physician or the physician's practice (including employees and staff members);[89] and
- The compensation arrangement does not violate the federal healthcare program Anti-Kickback Statute (or any federal or state law or regulation governing billing or claims submission).[90]

Parties seeking to rely on this exception should recognize some obvious limitations in the context of an EHR network. First, it may be difficult to establish the value of the network benefit to a physician, and the $300 limit may severely restrict the network's utility. Second, once the value is established, tracking other forms of non-monetary compensation would arguably be necessary to ensure that the $300 limit is not exceeded.

---

[87] 42 C.F.R. § 411.357(k).
[88] 42 C.F.R. § 411.356(k)(1)(i).
[89] 42 C.F.R. § 411.357(k)(1)(ii).
[90] 42 C.F.R. § 411.357(k)(1)(iii).

3-1(b)(2). Medical Staff Incidental Benefits

The Stark Law also includes an exception for certain incidental benefits provided by hospitals to their medical staffs. This exception allows compensation in the form of items or services (not including cash or cash equivalents) from a hospital to its medical staff provided specific conditions are met. The purpose of this exception, according to CMS, is to allow medical staff benefits that are "incidental to services being provided by the medical staff at the hospital."[91] CMS recently expanded this exception to non-hospital facilities that have *bona fide* medical staffs.[92]

As revised, the exception permits a facility to provide its medical staff benefits as follows:

- The benefits must be offered to all members of the medical staff practicing in the same specialty without regard to the volume or value of referrals or other business generated between the parties;[93]
- The benefits must be offered only during periods when the medical staff members are making rounds or are engaged in other services or activities that benefit the facility or its patients;[94]
- The benefits must be provided by the facility and used by the medical staff members only on the facility's campus.[95] CMS notes that the use of the phrase "or are engaged in other services or activities that benefit the hospital or its patients" was intended to clarify that dedicated electronic or Internet items or services, dedicated pagers or two-way radios may meet the requirements of this exception. In its commentary to the most recent Stark Law regulations, CMS states that it explicitly revised this exception to provide that the "on campus" requirement will be satisfied if these communication devices are used exclusively to access hospital medical records, patient information, or patients or personnel located on campus;[96]

---

[91] 69 Fed. Reg. at 16,112.
[92] 42 C.F.R. § 411.357(m).
[93] 42 C.F.R. § 411.357(m)(1).
[94] 42 C.F.R. § 411.357(m)(2).
[95] 42 C.F.R. § 411.357(m)(3).
[96] 66 Fed. Reg. at 16,113.

- The benefits must be reasonably related to the provision of, or designed to facilitate directly or indirectly the delivery of, medical services at the facility;[97]
- The benefits must be of low value (*i.e.,* less than $25, now indexed for inflation by reference to the CPI) with respect to each occurrence;[98]
- The benefits must not be determined in any manner that takes into account the volume or value of referrals or other business generated between the parties;[99] and
- The compensation arrangement does not violate the federal healthcare program Anti-Kickback Statute.[100]

Relying on the medical staff benefits exception in the context of a community network would not solve the Stark issues for providers who do not have *bona fide* medical staffs. In addition, it is not clear whether this exception has much use in communities with more than one hospital and where not all physicians are typically on the medical staffs of each hospital in the community. This exception would not permit use of the network for purposes other than servicing hospital patients—such as a primary care physician sharing clinical information with a specialist for a non-hospital patient. Finally, the $25 limitation makes this exception unavailable for most EHR networks, where the value for hardware, software, or support services may exceed $25.

3-1(b)(3). Payments at Fair Market Value

If the EHR network charges (or imposes some concrete obligation on) physicians for participation in or use of the network, it may be possible to fit the arrangement within the Stark Law exception for payments by a physician for items or services at fair market value.[101] As the name of the exception suggests, the key issue is determining whether the network charges are in fact fair market value for the items or services provided. Counsel should consider whether the charge takes into account the cost of system development or may be limited to the incremental costs associated with the physician's

---

[97] 42 C.F.R. § 411.357(m)(4).
[98] 42 C.F.R. § 411.357(m)(5).
[99] 42 C.F.R. § 411.357(m)(6).
[100] 42 C.F.R. § 411.357(m)(7).
[101] 42 U.S.C. § 1395nn(e)(8); 42 C.F.R. 411.357(1).

use of the network. Moreover, counsel should consider whether the value of the physician's time and commitment to learn and use an EHR and to comply with the system's (HIN's) policies might be considered a "service" of value provided by the physician that can offset the value of the item provided by the HIN. Ultimately, the need to support the fair market value determination may prompt the network sponsor to retain a valuation consultant to review the arrangement.

3-1(b)(4). Community Health Information Systems

In the most recent revisions to the Stark regulations, CMS introduced a new exception that permits a hospital or other DHS entity to provide items or services "of information technology" to a physician to allow access to electronic healthcare records and complementary drug information systems, general health information, medical alerts, and related information for patients.[102] The new exception is intended to encourage use of electronic technology. To qualify for this exception:

- The items or services must be principally used by the physician as part of the community-wide health information system;[103]
- The items or services must be provided to the physician in a manner that does not take into account the physician's volume or value of referrals;[104]
- The health information system (including both hardware and software) must be "community-wide," *i.e.*, it must be available to all providers, practitioners, and residents of the community who desire to participate; and[105]
- The arrangement does not violate the Anti-Kickback Statute or any federal or state laws or regulations governing billing or claims submission rules.[106]

CMS warns that the DHS entity may only provide items and services that are necessary to enable the physician to participate in the EHR network. Thus, for example, if a physician already owns a computer, it may only be necessary to provide software or

---

[102] 42 C.F.R. § 411.357(u).
[103] 42 C.F.R. § 411.357(u)(1).
[104] *Id.*
[105] 42 C.F.R. § 411.357(u)(2).
[106] 42 C.F.R. § 411.357(u)(3).

training specific to the network.[107] To provide more items or services than necessary will not only not comply with the new exception, but could also implicate the Anti-Kickback Statute.

This new Stark exception is useful but several ambiguities remain. For example, network sponsors are struggling to define the scope of the obligations created by the requirement that the system be made "available" to all providers in the community, and the scope of the "community." It is also unclear (1) whether the network must be available to all providers from the onset; (2) whether certain features of the network can be offered only to those physicians on a hospital's medical staff or who have some sort of existing relationship with the network sponsor; and (3) how to reconcile patient privacy and security concerns with the exception's mandate for broad access. Another challenging aspect of the exception is the requirement that the system be available to community "residents." If this means that a network must establish a public portal at the beginning of its operations, both the cost and logistics will be daunting. As part of the "Stark II, Phase III" regulations, CMS has an opportunity to issue either additional preamble language or new regulatory text clarifying the ambiguities in this exception.

Congress and DHHS also have an opportunity to encourage the development of HINs and other EHR networks by creating a much broader Stark exception for provision of EHR technology below cost, either via regulation or statute. Ideally, these standards should mirror those of a new Safe Harbor Regulation under the Anti-Kickback Statute or a new statute protecting certain financial arrangements for the provision of EHR technology from criminal and civil prosecution under the Anti-Kickback Statute.

3-2. The Anti-Kickback Statute

The Anti-Kickback Statute prohibits the payment or solicitation, offer, or acceptance of any remuneration in cash or in kind in exchange for referring or recommending the referral of items or services to be paid by a federal healthcare benefit program.[108] The language of the statute is extremely broad and the courts have construed it liberally. For example, violations may be found if only one purpose of the

---

[107] 69 Fed. Reg. at 16,113.
[108] *See*, 42 U.S.C.A. § 1320q-7b(b).

remuneration is to induce referrals.[109] Some courts have held, however, that to establish an Anti-Kickback violation the government must prove that a defendant had the specific intent to violate the law.[110] The OIG has adopted a liberal construction of the Anti-Kickback prohibition, noting that kickbacks distort medical decision-making, cause over-utilization, increase costs to the federal healthcare programs, and result in unfair competition by freezing out competitors unwilling to pay kickbacks.[111]

The generation of electronic medical records requires the use of computer equipment and software, usually at the point of delivery of care such as in a hospital or physician's office. Making the record interoperable among several providers requires a telecommunications network. According to a 2004 GAO Briefing Report, physicians "may be reluctant to accept such resources from a hospital or other provider, knowing that the resources may be viewed as remuneration and that any referrals the physician subsequently makes to the provider may be viewed as having been made in return for such resources in violation of the [Anti-Kickback] law."[112] Similarly, hospitals and other providers may be unwilling to provide those resources to physicians, for fear that this will be a violation of the Anti-Kickback statute.

This reaction is at least partially attributable to the historically aggressive enforcement position of the OIG. The OIG has long suggested that offers of free or discounted electronics are suspect under the Anti-Kickback Statute. For example, in 1991, as part of its initial safe harbor rulemaking, the OIG observed that the functionality of free computers shipped to physicians' offices should be limited to the medical services being acquired. If the physician is free to use the computer for a variety of other purposes, then "the computer has a definite value to the physician, and, depending on the circumstances may well constitute an illegal inducement."[113] In 1997, the OIG reiterated its concerns: "[I]f the [computer] equipment is used by the recipient

---

[109] *United States v. Katz*, 871 F.2d 105 (9th Cir. 1989); *United States v. Greber*, 760 F.2d 68 (3d Cir.), *cert. denied*, 474 U.S. 988 (1985).
[110] *Hanlester Network v. Shalala*, 51 F.3d 1390 (9th Cir. 1995).
[111] OIG Special Advisory Bulletin, "Contractual Joint Ventures," p. 2 (April 2003).
[112] "HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption," GAO Briefing for Congressional Staff, Senate Committee on Health, Education, Labor and Pensions, Report GAO-04-991R, p. 46 (August 13, 2004) (the GAO Briefing).
[113] 56 Fed. Reg. 35,978 (July 29, 1991).

for any purpose other than in connection with the ordered service, there is potential illegal remuneration and potential liability for both parties to the transaction."[114] While the OIG acknowledged that general-purpose computer equipment may not always have separate value to a physician, the OIG nonetheless views all such free equipment arrangements with skepticism.[115]

3-2(a). Remuneration

As noted above, institutional providers have an obligation to share clinical information with physicians and others about common patients. Therefore, a physician using an EHR network to obtain information about his or her patients is not necessarily accepting remuneration from the network sponsor. If, however, the EHR network provides hardware, software, and practice management services to its users, this bundle of goods and services may constitute remuneration. The difficulty is determining where to draw the line. At what point do the services provided to the EHR users constitute "remuneration" and under what circumstances will such remuneration constitute an illegal inducement under the Anti-Kickback Statute?

In the context of the establishment of an EHR network, the purpose of the network, its design and function, and the level of benefit the sponsors bestow on potential referral sources will be critical components in determining the level of Anti-Kickback risk. Clearly, conditioning access to the network on referrals or offering higher support levels relative to the volume or value of referrals to the network sponsor would significantly increase the Anti-Kickback risk associated with the venture.

3-2(b). Anti-Kickback Safe Harbors

The Anti-Kickback Statute includes a number of regulatory "safe harbors." If an arrangement fits within a safe harbor, it is immune from attack under the statute. Failure

---

[114] *See* Kevin G. McAnaney, General Observations Letter Regarding Free Computers, Facsimile Machines and other Goods, (July 3, 1997), http://oig.hhs.gov/fraud/docs/safeharborregulations/freecomputers.htm.

[115] *Id*. Along these lines, Mr. McAnaney stated that the OIG would examine the following criteria in determining the propriety of the offer of free or discounted equipment:
- the criteria used by the supplier of the equipment to determine which customers receive the equipment;
- the ownership of the equipment;
- the location and access to the equipment at the customer's place of business;
- the procedures used by the customer and supplier to police unauthorized use of the equipment;
- the value added to the core service being provided by the additional general purpose equipment; and
- the number and extent of similar arrangements with other parties.

to comply with all the requirements of a safe harbor does not mean the arrangement is illegal. Rather, arrangements falling outside of a safe harbor are subject to a facts and circumstances analysis.

When a pharmaceutical company, hospital, or health system finances an EHR network, the terms under which physicians and other providers participate should be reviewed in light of the Anti-Kickback Statute's broad prohibition. If the EHR sponsor stands to benefit from the referral of patients covered by a federal healthcare program by network users, the level of Anti-Kickback exposure may hinge on the parties' intent. Because of the inherent uncertainties in divining intent, parties may prefer to structure the EHR to fit within a regulatory "safe harbor" to obtain immunity from Anti-Kickback prosecution. Unfortunately, practical limitations may make that difficult.

The Anti-Kickback safe harbor criteria uniformly require that any payments be at fair market value, that the terms be set in advance and that the transaction be commercially reasonable even if it is entered into between parties that do not share any patients. Although these criteria are not patently unreasonable, the creation of an EHR network presents unique challenges. EHR networks generally are not sufficiently valuable to physicians and other non-institutional providers to justify either the initial investment or the ongoing operational costs. Given this, if EHR networks are to succeed, the amount physicians are required to invest usually will have to be subsidized by another party. Any such subsidy will generally result in the EHR network falling outside of the Anti-Kickback safe harbors.

Despite these limitations, it is worthwhile to outline the requirements of the Anti-Kickback safe harbors that have potential application to EHR networks. Even if the EHR network cannot fully comply with the safe harbor requirements, structuring the venture to meet as many of the safe harbor elements as possible should reduce the parties' risks.

3-2(b)(1). Personal Services and Management Contracts[116]

The safe harbors for personal services and management contracts could protect at least some of the payments to an EHR network if the following conditions are met:

- The arrangement is documented in a written agreement signed by the parties;
- The agreement covers all services the EHR network will provide to the user;
- If the arrangement is for part-time or sporadic use, versus full-time use, the agreement specifies the exact schedule;
- The term of the agreement is for at least one year; and
- The aggregate compensation over the term of the agreement is set in advance, consistent with fair market value, and is not determined based on existing or expected referrals or other business generated between the parties.

However, even if network users pay a fair price, structuring an arrangement to satisfy all of the above requirements may be problematic. For example, it is unclear whether the use of the EHR would be construed as part-time or full-time use. This would likely depend on the particular features of the EHR and could vary from provider to provider. Likewise, it may be impractical to determine in advance the exact schedule or "aggregate" compensation over the term of the agreement.

Finally, determining whether the EHR's charges to healthcare providers are fair market value may be both difficult and costly. In making this determination, network sponsors should consider whether the EHR charges must take into account the cost of system development or if they can be limited to the incremental costs associated with the use of the network. As noted in the Stark Law discussion above, the need to support the fair market value of the network's charges may make it prudent for the EHR sponsor to retain a valuation consultant to review the arrangement.

3-2(b)(2). Equipment Rental[117]

Another potentially applicable Anti-Kickback safe harbor is the equipment rental safe harbor. This safe harbor would permit healthcare providers to lease equipment and related software from the EHR network. The equipment rental safe harbor requirements

---

[116] 42 C.F.R. § 1001.952(d).
[117] 42 C.F.R. § 1001.952(c).

are nearly identical to the personal services and management contract safe harbor requirements discussed above and raise the same practical problems. In addition, the equipment rental safe harbor requires that the aggregate rental amount not exceed that which is reasonable and necessary to accomplish the commercially reasonable business purpose. This requirement could likely be satisfied by limiting any use of leased equipment to that which is reasonably necessary for the use of the EHR.

3-3. State Laws

Some state laws prohibit healthcare providers being paid for referrals, generally limited to state-paid healthcare programs.[118] While this Chapter will not discuss these laws, counsel should carefully consider the impact of state anti-referral laws on the development of HINs, particularly with multi-state Participants.

3-4. Policy Issues

As discussed above, the Stark and Anti-Kickback Laws will inhibit the development and dissemination of electronic medical record technology because of the potential civil and criminal penalties for violation. Given that the President has set a timetable of ten years for implementing electronic medical records, policymakers will need to resolve the clear tension between the desire to promote electronic medical record technology and anti-fraud programmatic goals, and identify strategies to lower the barriers to implementation of EHR networks. Such efforts are currently underway to address these barriers, and counsel should keep abreast of these developments, as the Stark Law and Anti-Kickback Statute are some of the more substantial barriers to the effective development of HINs and other EHR networks.

---

[118] *See, e.g.,* A.R.S. § 13-1371(A) (making it a felony to knowingly offer, deliver, receive or accept "any rebate, refund, commission, preference or other consideration as compensation for referring a patient, client or customer to any individual, pharmacy, laboratory, clinic or healthcare institution providing medical or health-related services or items" under the state Medicaid or county indigency programs, "except for payments from a medical researcher to a [licensed] physician" "in connection with identifying and monitoring patients for a clinical trial regulated by the [FDA]."

CHAPTER 4:
NON-PROFIT TAX

4-1. Background and Introduction

As addressed in other chapters, the federal government's vision for widespread electronic health record exchange calls for the creation of regional health information organizations (or Health Information Networks—HINs—as we call them in this Briefing). Notably, however, the government has neither prescribed nor defined the form or structure of a HIN, nor has it clearly and precisely described a HIN's relative role and relationship in the EHR network vis-à-vis the various network participants. In some cases, an existing hospital or health system will, at least initially, acquire and implement the EHR system that will provide the core technology infrastructure for the EHR network, as well as provide the ongoing services needed to operate the system. The extent to which the hospital or health system will be taking on the role of a HIN is likely to depend upon various factors, including how long it plans to continue to serve in that capacity and the extent to which it includes individuals and organizations other than its physician employees and medical staff members, such as competing hospitals and health systems, and unrelated laboratories, pharmacies, and the like. In other cases, factors such as the nature and number of the initial participants or the source of funding may lead to the formation of a new entity to function as the HIN. Whether an existing hospital or health system or a new entity functions as the HIN, it may be necessary in certain cases to subcontract significant initial support obligations to the technology vendor providing the core system.

Regardless of whether an EHR network constitutes a HIN and, if so, which entity serves as the HIN, the implementation of an EHR network will involve the development of a series of complex and interrelated agreements. Such agreements must establish clear lines of ownership, financial and operational responsibility, accountability, and liability. Failure to do so at the outset will generally create problems, even in the early years of an EHR network relationship, including tax-exemption problems for the HIN and one or more of the exempt organizations participating in the relationship.

The principal tax-exemption issues that arise in planning for the creation and operation of a HIN include:

(1) Whether providing the funding, technology infrastructure, and support services needed to establish and maintain a HIN is an activity that will support stand-alone or integral part tax-exempt status for a new entity under the community benefit standard of Section 501(c)(3) of the Internal Revenue Code (Code);

(2) Whether a new entity created to conduct such activities will qualify for public charity status under Code Section 509(a);

(3) If such activities will not support stand-alone or integral part exemption under Section 501(c)(3), whether an alternative basis for exemption is available under Code Section 501;

(4) If conducted by an existing tax-exempt organization such as a hospital or a health system, will such activities qualify as related to such organization's tax-exempt purposes under the unrelated business income tax rules applicable to Section 501(c)(3) organizations; and

(5) Whether provision of and/or participation in the health information network with individuals (e.g., physicians) and unrelated taxable organizations violates the private inurement and private benefit prohibitions of Section 501(c)(3).

Threshold considerations in addressing some or all of these issues include:

(1) Who is providing the funding, technology infrastructure, and support services needed to implement and maintain the EHR system?

(2) Who manages the relationship that exists between and among the various participants in the network?

(3) Are those roles the primary functions of the applicable entity?

(4) To whom is participation in the EHR network available (all or only some in the community)?

(5) On what terms is participation made available (e.g., funding contributions, license fees, implementation, and support fees)?

(6) Who owns the information in the health records?

(7) Who owns the underlying technology?

(8) Who operates the technology?

Following is a discussion and analysis of these tax-exemption issues and corresponding considerations.

4-2. Section 501(c)(3) Tax-Exempt Status for a Newly-Formed HIN Entity

The threshold tax-exemption issue for a new entity formed to function as a HIN is whether the entity will qualify for tax-exempt status. The principal advantages of Section 501(c)(3) tax-exempt status are: (a) exemption from tax on net income; (b) ability to issue tax-exempt debt; (c) ability to attract philanthropic funding; and (d) support for obtaining exemptions from state and local taxes such as real property taxes and sales and use taxes.

A HIN may attempt to qualify for tax-exemption under Section 501(c)(3) either as a "stand-alone" exempt organization or as an "integral part" or "derivative" tax-exempt organization. To qualify for stand-alone exempt status, a HIN must demonstrate that providing the funding, technology infrastructure, and support services needed to establish and maintain an EHR network satisfies the community benefit standard of Section 501(c)(3) of the Code. To qualify for integral part or derivative tax-exempt status, a HIN must demonstrate that the nature of this role, the extent of the participation in the HIN by other 501(c)(3) tax-exempt organizations, and the relationship of the HIN entity to those exempt HIN participants is sufficient to support Section 501(c)(3) "integral part" or "derivative" tax-exempt status.

4-2(a). Stand-Alone Section 501(c)(3) Tax Exempt Status

Section 501(c)(3) grants tax-exempt status to charitable organizations. The "promotion of health" has been determined to constitute a charitable purpose. Whether the activities and purposes of a HIN entity promote the healthcare of the community under the community benefits standard of Section 501(c)(3) may be considered a case of first impression that will be comprised of various compelling but yet untested arguments.

The first component of the case is the articulation of the government's EHR vision and corresponding rationale. As discussed in the Introduction, President Bush has called for the widespread adoption of electronic medical records for most Americans within the next ten years. In fact, the President has created a new office within DHHS, the Office of the National Coordinator for Health Information Technology (ONC), which is devoted exclusively to the implementation of that mandate. ONC's goals, as articulated in its Framework for Strategic Action (*see* Introduction), may be

characterized as promoting the health of the community by improving the quality and efficiency of healthcare, preventing medical errors, and enhancing patient safety. Collateral benefit also exists in the potential for contributions to research and education.

Two revenue rulings may be relevant and helpful in making the case for stand-alone exempt status for a new HIN entity. First, Revenue Ruling 76-455 involved the formation of a not-for-profit regional health data system to conduct studies and propose improvements regarding quality, utilization, and effectiveness of healthcare and healthcare agencies and to educate those involved in furnishing, administering, and financing healthcare. Specifically, the organization furnished aid for the development of uniform health data record-keeping and reporting procedures, and conducted related studies and educational programs. The data gathered was useful for reviewing patient management patterns, planning for regional and community health needs, and conducting epidemiological research. The members of the organization were other not-for-profit health information organizations, but the health data system maintained by the organization was open to everyone on a free, non-discriminatory basis. The Internal Revenue Service (IRS) ruled that the organization in this ruling was exempt as an organization that was organized and operated primarily for scientific and educational purposes under Section 501(c)(3). Nonetheless, the facts and circumstances would be persuasive in making the case for exemption under the community benefit theory for exemption as a charitable organization under Section 501(c)(3).

The second relevant ruling, Revenue Ruling 81-276, involved a professional standards review organization (PSRO) formed pursuant to the mandate of the Social Security Act Amendments of 1972 and designated to review medical necessity of services billed under the Medicare program. DHHS fully funded the PSRO. The IRS ruled that the organization promoted the health of the community by reducing over-utilization and relieving the burdens of government. An important parallel between the PSROs in this ruling and HINs is that Congress mandated the creation of PSROs for the purpose of relieving the burdens of government. Arguably, HINs have been mandated for the same reason.

Additional support for the case for stand-alone exemption may exist if the HIN qualifies for the community health information network exception under Stark. Arguably,

the enactment of that exception recognizes the significant community benefits of a health information system (including both hardware and software) that is made available on a "community wide" basis (i.e., it is available to all providers, practitioners, and residents of the community who desire to participate).

4-2(b). "Integral Part" or "Derivative" Section 501(c)(3) Status

An organization involved in healthcare that cannot qualify for stand-alone Section 501(c)(3) status because its activities are not considered to be inherently charitable may nonetheless qualify for tax exempt status under the Section 501(c)(3) "derivative" or "integral part" theory of exemption if it meets both of two essential requirements: (1) the activities of the organization are ones that could or otherwise would have been performed by another exempt entity on whose behalf the organization is conducting the activities; and (2) a sufficient structural or financial relationship exists between the organization seeking exemption and such other exempt entity.

The predominant focus of the IRS in making derivative exemption determinations has been on the relationship requirement. In the healthcare context, the IRS has displayed a preference for a formal structural relationship. Common examples of healthcare organizations that have relied on the derivative/integral part theory include parent corporations of diversified hospital systems, malpractice insurance trusts created to pool risk among various related healthcare providers, and joint operating companies formed to implement a "virtual merger" between two previously unrelated healthcare systems.

An important corollary to the derivative theory of exemption is that the provision of services by one exempt organization to one or more other exempt organizations that do not satisfy the relationship requirement is not necessarily an exempt activity. A HIN entity seeking derivative or integral part exemption under Section 501(c)(3) has a strong case for satisfying the essential services requirement. Satisfying the relationship requirement, however, may be more difficult. A HIN by its nature is likely to be providing services and support to various exempt organizations in the community who are not otherwise related to one another through formal corporate control. The fact that some or all of those organizations establish a corporate relationship as co-members of the HIN is not sufficient to meet the integral part relationship requirement.

4-3. Section 509(a) Public Charity Status

A Section 501(c)(3) tax-exempt organization is presumed to be a private foundation unless it demonstrates that it qualifies as a “public charity” or “non-private foundation” under Code Section 509(a). The advantages of qualifying as a public charity include: (1) fewer reporting requirements; (2) ability of donors to qualify for a larger tax deduction for their charitable contributions to the entity; and (3) fewer restrictions such as those relating to self-dealing and investments.

Section 509(a) describes various types of public charities. Section 509(a)(1) public charities include: (1) organizations, such as hospitals or medical research organizations, whose principal activities are by nature ones that will assure the organization is responsive to the needs of the public; and (2) organizations that are responsive to the public because they derive a certain percentage of their financial support from a broad segment of the donor community. Section 509(a)(2) public charities are organizations that derive a certain portion of their financial support from gross receipts from the provision of services for a broad segment of the community. Finally, Section 509(a)(3) public charities are organizations that provide support for and have a certain relationship with 509(a)(1) and 509(a)(2) public charities.

A HIN entity is unlikely to qualify under Section 509(a)(1) either by virtue of the services it provides or by virtue of its sources of support. Its operations are unlikely to qualify, for example, as a “hospital” or “medical research” organization. Further, a HIN is likely to derive its support from one or a small number of donors. Section 509(a)(2) may be an alternative for a HIN depending upon the nature and extent to which it charges for participation in the EHR network. Section 509(a)(3) may be an alternative as well, depending upon the extent to which the participants in the network are other exempt organizations with whom it has the requisite relationship. As the scope of the community participation in the HIN expands, however, the HIN’s prospects for qualifying under Section 509(a)(3) are likely to diminish.

4-4. Section 501(c)(4) and Section 501(c)(6) as Alternative Avenues for Exemption

A HIN that is unable to qualify for Section 501(c)(3) status should consider Section 501(c)(4) and Section 501(c)(6) as alternatives. Section 501(c)(4) provides

exemption for organizations that operate primarily to further in some way the common good and general welfare of the people of a community. While the “community benefit” standard of Section 501(c)(3) does not technically apply, Section 501(c)(4) organizations must also demonstrate that their activities benefit a reasonably broad segment of the public. Section 501(c)(6) provides exemption for trade associations, such as business leagues, formed to improve the business conditions of one or more lines of business.

Both types of exemption lack certain of the advantages of Section 501(c)(3) exempt status. First, neither type of organization will be eligible for tax-exempt financing. Second, contributions to these organizations are not eligible for tax deductions by the donors. On the other hand, both 501(c)(4) and 501(c)(6) organizations have more flexibility to engage in political and lobbying activities. They also are not treated as private foundations and, therefore, qualifying for Section 509(a) public charity status is unnecessary. The private inurement prohibition and intermediate sanction provisions apply to Section 501(c)(4) organizations. While the inurement prohibition does not technically apply to Section 501(c)(6) organizations, Section 501(c)(6) business leagues must be able to demonstrate that their activities are not directed to the performance of particular services for individual persons.

Revenue Ruling 74-553 provides support for the availability of Section 501(c)(6) exempt status for a HIN entity. That ruling involved a medical peer review board created by members of a state medical association in response to concerns of physicians, insurers, the government, and the public. The purpose of the board was to establish and maintain standards for quality, quantity, and reasonableness of the costs of medical services through the operation of peer review boards throughout the applicable state. The IRS found that the objective of the organization's principal activity was to maintain the professional standards, prestige, and independence of the organized medical profession and thereby to further the common business interest of the organization's members rather than the public at large. Accordingly, the IRS ruled that the organization qualified for exemption under Code 501(c)(6) rather than Code Section 501(c)(3).

4-5. Unrelated Business Income Tax Liability of Section 501(c)(3) Organizations

Even though Section 501(c)(3) organizations are generally exempt from income taxation, they may still have to pay taxes (unrelated business income tax, or UBIT) on amounts derived from certain activities outside the scope of their exempt functions. The purpose of the UBIT rules is to prevent tax-exempt organizations from unfairly competing against taxable entities conducting the same or similar types of activities.

UBIT is imposed on income derived from an "unrelated trade or business." An "unrelated trade or business" exists where three factors are met: (1) the activity constitutes a "trade or business;" (2) the trade or business is regularly carried on; and (3) the trade or business is not substantially related to the organization's exempt purposes. The relatedness test is a "facts and circumstances" test and can be difficult to apply. As a general rule, the purpose for which the activity and the means by which it is conducted, rather than the nature of the activity itself, drive the determination of relatedness. The fact that an activity may serve as a source of funding for the organization's other exempt activities is not, in itself, sufficient to show "substantial relatedness."

Excessive UBIT can prevent qualification for exemption in the first instance and lead to loss of tax-exempt status after it has been obtained. How much UBIT is too much is also entirely a facts and circumstances determination and no bright line exists for making it.

The nature of the activities of a HIN or other organization supporting an EHR network on their face might be characterized as a trade or business regularly carried on. Again, however, the purpose for which the activities are conducted is the determinative factor. Therefore, such activities are not likely to raise a UBIT issue for a new HIN entity that has successfully qualified as a "stand-alone" exempt organization because those activities themselves are what support the exemption overall. A HIN entity that has qualified for Section 501(c)(3) exemption under the integral part theory, however, will need to assess its potential for UBIT liability to the extent it provides the EHR funding, infrastructure, and services for one or more other exempt organizations that do not satisfy the relationship requirement. As noted above, a HIN by its nature is likely to be providing services and support to various exempt organizations in the community that

are not otherwise related to one another through formal corporate control. The fact that some or all of those organizations establish a corporate relationship as co-members of the HIN is not sufficient to meet the integral part relationship requirement.

A similar UBIT issue will exist for an exempt hospital or health system that provides the EHR funding, infrastructure, and support services to unrelated exempt organizations, to for-profit entities, or to individuals who are not individuals who are patients of the hospital or system. In this context, the arguments that can be made to support stand-alone exemption should also be considered as a basis for demonstrating relatedness to the exempt purposes of the hospital or health system. The success of the argument may depend on whether the exempt organization has extended the reach of the EHR to a sufficiently broad scope and cross section of participants in the community.

4-6. Private Inurement and Private Benefit

One of the most challenging issues in the implementation of an EHR network, or HIN, is whether the financial relationship between and among the participants violates the prohibitions against private inurement and more than incidental private benefit that apply to Section 501(c)(3) and Section 501(c)(4) organizations. An important related consideration is whether a violation will result in an excess benefit transaction that will subject one or more of the exempt organizations involved to intermediate sanction excess taxes under Code Section 4958. These tax exemption considerations bear a close relationship to the Medicare anti-kickback laws and the fair market value exception under the Stark law that are addressed in detail in Chapter 3, and there will be significant overlap among all of them in the approaches developed to achieve compliance.

The risk of intermediate sanctions or revocation of exemption arises primarily in the context of financial relationships with “insiders” or “disqualified persons,” who are essentially individuals in a position to exercise substantial influence or control over the exempt organization. Avoidance of these compliance risks lies primarily in structuring the financial relationships at fair market value and on commercially reasonable terms.

Accordingly, an important tax-exemption planning consideration is whether and to what extent the participants in the EHR network must be charged for their

participation generally, for the infrastructure costs of the EHR network technology, and for the ongoing support services. The answer to this question may vary depending upon various factors, including, among others, how broadly the EHR network is being made available in the community, and whether a stand-alone tax-exempt HIN entity or an existing exempt hospital or health system is making it available. There is no published guidance that provides clear direction or draws any bright lines for answering this question; rather, we are again blazing new trails.

Arguably, if a HIN entity that provides a true community-wide health information network as contemplated by the DHHS EHR vision and the corresponding exception under the Stark law also qualifies on the basis of that function as a stand-alone exempt organization, charging for the availability of the network may be unnecessary to qualify for and maintain exemption. Some might argue that not charging the participants in fact supports the case for exemption in such a situation. In that case, the decision to charge for participation may be motivated primarily by financial considerations rather than exemption compliance considerations.

At the other end of the spectrum is a single exempt hospital or an exempt health system that is simply extending participation in its EHR system to physicians on its medical staff. Charging for participation in this case may be worthwhile from an exemption compliance perspective, as well as for purposes of Medicare Anti-Kickback and Stark anti-referral, unless and until the Stark community health information network exception is expanded to include participants other than networks that are made available on a community-wide basis.

Once again, there is no published guidance that provides clear direction or draws any bright lines for determining what to charge for participation. Key considerations will be the amount of the initial and ongoing investment in the core information technology infrastructure needed to support the network (including amounts such as payments to third-party vendors and support organizations for equipment, license rights, and implementation services and the value of internal human resources devoted to the implementation); incremental capital or operating costs incurred to support a particular individual or organization's participation (*e.g.*, additional equipment needs, specific customization or retrofitting, increases in volume (patient visits, number of facilities,

etc.); and whether the functionality of the infrastructure being provided is limited to the functionality needed to use and access the network for the community-wide goals of improved quality, etc. or whether it also provides capabilities that serve only the particular participant (e.g., software that serves the general practice management needs of a physician group practice participant). A common question that arises in the development of the pricing model is whether to vary pricing according to factors such as when a participant joins (e.g., giving more favorable pricing to encourage early participation and to take into account the additional risks involved in early participation), the nature of the participant, and the length of the term of participation. The terms and conditions of the written participation agreement also should address related issues such as payment of fees for early termination, pass through of sales or other taxes for non-exempt participants, and payment terms (e.g., timing, late payment fees).

4-7. Creation of the HIN as a Joint Venture Entity

As discussed in the Introduction, the structure of a new entity created to serve as a HIN may take various forms. One possibility is the creation of a partnership or limited liability company (LLC) owned by both exempt and non-exempt participants. In such case, the tax planning for the venture must include consideration of the extensive case law, IRS rulings, and other guidance concerning whether an exempt organization can participate in a partnership or LLC with one or more non-exempt participants without jeopardizing its exempt status or incurring unrelated business income tax liability on its distributions from the partnership or LLC.

CHAPTER 5:
ANTITRUST

The antitrust laws should *not* be viewed as an impediment to the formation and operation of HINs, including their legitimate collaborative activities such as information exchanges, standard setting, and vendor selection associated with interoperable heath records. The courts and the federal antitrust agencies have recognized that competitor collaborations can promote competition by enabling participants to combine complementary capabilities or resources, to jointly fund expensive innovation efforts, or otherwise to achieve efficiencies that result in lower prices, improved quality, or expedited development of new products.[119] In general, any competitive restraints associated with collaborative activities must be "reasonably related . . . and no broader than necessary to effectuate" legitimate, procompetitive business purposes.[120]

A HIN, however, can create antitrust exposure under the Sherman Act to the extent its activities are designed to, or have the effect of, reducing competition and stabilizing prices.[121] For example, antitrust risk could be created if a HIN orchestrates information exchanges that facilitate collusion among competitors or establishes IT standards that favor HIN Participants and disadvantage excluded competitors. Likewise, antitrust risk could result from agreements or common understandings that limit the

---

[119] *See, e.g.*, *Broadcast Music, Inc. v. CBS, Inc.,* 441 U.S. 1, 19-20 (1979) (a competitor collaboration can increase output and make new products available); *Federal Trade Comm'n v. Indiana Fed'n of Dentists*, 476 U.S. 447, 459 (1986) (dictum) (joint activities can create operational efficiencies); *Board of Regents v. NCAA,* 468 U.S. 85, 101-102, 117 (1984) (collaborative activities can enhance product or service quality and increase consumer choices); *see also* Federal Trade Commission (FTC) and Department of Justice (DOJ) *Antitrust Guidelines for Collaborations Among Competitors* (*Collaboration Guidelines*), 4 Trade Reg. Rep. (CCH) ¶ 13,160 (2000) (setting forth the analytical framework for assessing the lawfulness of a particular competitor collaboration); DOJ/FTC Statements of Antitrust Enforcement Policy in Healthcare (*Healthcare Statements*), 4 Trade Reg. Rep. (CCH) ¶ 13,153 (1996) (setting forth the framework for antitrust analysis and "safety zones" for certain types of collaborative activities involving healthcare participants).

[120] *SCFC ILC v. Visa USA, Inc.,* 36 F.3d 958, 970 (10th Cir. 1994), *cert. denied*, 515 U.S. 1152 (1995); *see also Collaboration Guidelines*, 4 Trade Reg. Rep. ¶ 13,160 (describing the seven-step analytical framework used by the federal antitrust agencies to evaluate the competitive effects of a competitor collaboration).

[121] Other applicable federal antitrust laws include the Clayton Act and the FTC Act. The Clayton Act prohibits exclusive dealing arrangements, tying arrangements, and requirements contracts in the sale of goods or commodities where the effect of those arrangements may be substantially to lessen competition. 15 U.S.C. § 14 (2000). The FTC Act prohibits unfair methods of competition, including but not limited to the acts and practices condemned by the Sherman and Clayton Acts. 15 U.S.C. § 45 (2000).

nature or degree of the Participants' competition outside the formation and operation of the HIN.

Antitrust guidance for a particular HIN should be specifically tailored to its unique characteristics and contemplated activities. No single set of guidelines can anticipate the extent to which different HINs may be formed or operated in a manner that creates unnecessary antitrust risk. That said, the adoption of appropriate safeguards could help to minimize unnecessary antitrust exposure associated with legitimate collaborative activities such as information exchanges, standard setting, and vendor selection.

5-1. Framework for Antitrust Analysis

Sherman Act Section 1 prohibits contracts, combinations, and conspiracies that unreasonably restrain trade.[122] Sherman Act Section 2 prohibits monopolization, attempts to monopolize, and conspiracies to monopolize.[123] In determining whether a particular practice unreasonably restrains trade under Sherman Act Section 1, courts generally have relied upon two methods of analysis: the "*per se*" rule and the rule of reason.[124] The *per se* rule flatly prohibits "agreements whose nature and necessary effect are so plainly anticompetitive that no elaborate study of the industry is needed to establish their illegality . . . ."[125] Most conduct that is alleged to be anticompetitive is evaluated under the rule of reason. Under this rule, the "test of legality is whether the restraint imposed is such as merely regulates and perhaps thereby promotes competition or whether it is such as may suppress or even destroy competition."[126]

The central issue in assessing potential antitrust exposure arising from a HIN's formation and operation is whether those activities are likely to create a substantial anticompetitive effect and, if so, whether that potential effect is outweighed by procompetitive efficiencies.[127] "Rule of reason" analysis requires an extensive market

---

[122] 15 U.S.C. § 1 (2000).
[123] 15 U.S.C. § 2 (2000).
[124] *FTC v. Indiana Fed'n of Dentists*, 476 U.S. 447 (1986).
[125] *National Soc'y of Prof'l Engineers v. United States*, 435 U.S. 679, 692 (1978). Examples of activities considered *per se* unlawful include agreements among competitors to fix price; agreements among competitors to allocate or divide markets; agreements among competitors to engage in certain types of boycotts or concerted refusals to deal; and some tying arrangements.
[126] *Chicago Bd. of Trade v. United States*, 246 U.S. 231, 238 (1918).
[127] Where competitors form collaborative ventures to achieve legitimate, procompetitive efficiencies,

inquiry into the reasonableness of the activity in view of the surrounding circumstances, including the facts peculiar to the HIN in question and the nature, purpose, and effect of any agreement or restraint. Competitive harm is presumed where a restraint is likely to create market power or to facilitate its exercise.[128] However, there can be no antitrust violation to the extent that the HIN's activities have neither the purpose nor the effect of stabilizing prices.[129]

Participants in a particular HIN must determine:

- Who is sharing data and how are they related to each other? Do they compete? Are they financially or clinically integrated?
- Who will have access to the interoperable EHRs (e.g., physicians, hospitals, multiprovider networks, pharmacies, and payors)?
- What information will be exchanged among HIN participants? For example, what data will be captured in the interoperable EHRs (e.g., patient and clinical information, lab and radiological reports, transcribed patient records, office visit information, treatment plans, prescription information, and insurance coverage or other payor information)? Exchanges of pricing information (e.g., fee schedules or reimbursement rates) are most likely to raise potential antitrust exposure.
- How may HIN Participants legitimately share information (e.g., facilitating communication and coordinating services among referring and referral physicians, reducing unnecessary or duplicative tests or procedures, reducing medical errors and adverse drug reactions, and monitoring provider adherence to practice protocols)? Anticompetitive uses include payor or provider coordination with respect to reimbursement or other price-related terms of contracting.
- Is there a need (and a technological ability) to limit access to competitively sensitive information or otherwise to guard against impermissible use of EHRs

---

agreements that are reasonably necessary to accomplish those benefits generally will not be condemned as *per se* unlawful. *See id; see also*, *Northwest Wholesale Stationers, Inc. v. Pacific Stationery & Printing Co.,* 472 U.S. 284 (1985).

[128] *See, e.g., Indiana Fed'n of Dentists*, 476 U.S. at 460.

[129] *See, e.g., Citizens & Southern Nat'l Bank*, 422 U.S. 86, 113 (1975); *L.C.L. Theatres, Inc. v. Columbia Pictures Indus., Inc.*, 421 F. Supp. 1090, 1106-07 (N.D. Tex. 1976) (when neither the purpose nor the effect is to stabilize prices, there is no antitrust violation), *rev'd in part on other grounds*, 566 F.2d 494 (5th Cir. 1978).

(e.g., limiting provider or payor access to clinical information to minimize any risk of improper agreement among competitors on reimbursement or other competitive terms)?

- What other activities will the HIN pursue once EHR interoperability is established (e.g., developing and implementing practice protocols, monitoring and evaluating provider performance relative to established benchmarks, sharing financial risk for performance, and evaluating patient outcomes or costs)?
- Will participants pool their intellectual property (e.g., software) to create highly standardized EHRs that enhance interoperability?[130]
- Who will pay the development, implementation, and operational costs of EHR and other HIN activities?

5-2. Information Exchanges

5-2(a). Potential Antitrust Exposure Associated with Information Exchanges

The formation and operation of HINs by definition involves exchanges of data and information, including exchanges of data among competing payors and providers of the information contained in the interoperable EHR. The antitrust laws do not prohibit information exchanges. The Supreme Court has held that the mere exchange of information among competitors is not unlawful and can promote competition.[131] However, if the circumstances surrounding information exchanges permit the inference of a *per se* unlawful agreement (e.g., price fixing) or suggest an express or tacit agreement to restrain trade, the information exchanges can create substantial antitrust exposure under Sherman Act Section 1.[132] Under rule of reason analysis, the lawfulness of a particular information exchange depends on many factors, including the number of competitors in the market, the nature of the information exchanged, ease of

---

[130] Please refer to section 6-2(b)(2) for a discussion of patent pooling.

[131] *See Maple Flooring Mfrs. Ass'n v. United States,* 26 U.S. 563, 582-83 (1925) (upholding the exchange of price information by a trade association where the exchange was made available openly and consisted purely of statistical information of past prices and did not identify particular customers).

[132] *See United States v. Container Corp. of America*, 393 U.S. 333, 335, 337-38 & n.4 (1969) (*citations omitted*) (considering market characteristics in condemning information exchanges among sellers of corrugated shipping containers and noting the absence of any legitimate or "controlling" justification, such as the need to protect against fraud).

entry into the market, and elasticity of demand for the products or services involved.[133] Exchanges of current price information have the greatest potential for generating anticompetitive effects and, although not *per se* unlawful, have consistently been held to violate Sherman Act Section 1.[134]

Statement 5 of the *Health Care Statements* sets forth a "safety zone" for fee-related information exchanges between providers and payors that meet three requirements.[135] First, the exchange must include only factual information, such as current or historical fees or discounts. Second, a third party must manage the collection and assembly of fee-related information. Finally, the information disclosed to the payors (or to the providers themselves) must be properly aggregated "such that it would not allow recipients to identify the prices charged by any individual provider," with at least five providers reporting data upon which each disseminated statistic is based and no individual provider's data representing more than 25% on a weighted basis of that statistic.[136] For surveys of price or cost (e.g., surveys of employee compensation), there is an additional requirement that the data collected must be more than three months old.[137] Information exchanges that fall outside the safety zone are evaluated under the rule of reason.[138]

5-2(b). Recommendations for Information Exchanges

Practical guidelines that can help to minimize antitrust exposure potentially associated with a HIN's information exchanges include:

Limit exchanges of competitively sensitive data. Only the information required for a particular activity should be included in any exchange, and the communication of that information to individual HIN participants should be restricted as much as possible while still meeting the goals of the exchange. For example:

---

[133] *United States v. United States Gypsum Co.,* 438 U.S. 422, 441 n.16 (1978).
[134] *See, e.g., id.; see also American Column & Lumber Co. v. United States,* 257 U.S. 377 (1921) (holding that the exchange of price information among competitors violates Sherman Act Section 1); *United States v. American Linseed Oil Co.*, 262 U.S. 371 (1923) (same); *Container Corp.*, 393 U.S. at 337 (same).
[135] *Healthcare Statements,* 4 Trade Reg. Rep. ¶¶ 20,809-11.
[136] *Id.*
[137] *Id.*
[138] *Id.*

- If the information is price- or cost-related, only historical or current information should be communicated, and then only for specified, procompetitive purposes.
- Information that is shared with individual HIN participants should be collectively discussed only for specified, procompetitive purposes.
- Any recommendations developed by the HIN based on analysis of the information exchanged should be communicated to individual participants without reference to specific, non-aggregated data, and only for specified, procompetitive purposes.

Use third-party data administrators if feasible. If feasible, the information should be collected and analyzed by an independent third party, not by the individual HIN participants themselves.

Perform an antitrust review. Because the analysis of antitrust liability is fact-intensive, antitrust review and approval should be obtained before the HIN conducts any information exchanges (i.e., at least until the accepted practices in this area become more settled).

Use confidentiality agreements. HIN participants who participate in a particular information exchange should sign confidentiality agreements identifying individuals who may access competitively sensitive information, and stating the specific, procompetitive purpose of the information exchange.

5-3. Standard Setting and Vendor Selection

5-3(a). Potential Antitrust Exposure Associated with Standard Setting and Vendor Selection Activities

To facilitate the development and operation of interoperable EHRs, a HIN will need to establish standards and protocols for a number of organizational and IT issues including membership, IT protocols, access to records, and the form, content, and frequency of data submission. It may choose to contract with third-party vendors to perform certain functions, such as providing EHR storage and retrieval systems. Absent appropriate safeguards against antitrust risk, certain of these activities can create

substantial exposure.[139] In particular, antitrust liability can arise if the HIN's generally legitimate activities are used by participants as a competitive weapon to injure their excluded competitors. For example, where a collaborative venture, such as a trade association, adopts biased standards that benefit the group who promulgated the standards and disfavor its competitors, the participants have been held liable under Sherman Act Section 1.[140] Similarly, when an individual competitor is excluded or disciplined for failure to satisfy an organization's standards, accreditation or credentialing activities, the organization can face substantial antitrust exposure.[141]

5-3(b). Recommendations for Standard Setting and Vendor Selection

Practical guidelines that can help to minimize potential antitrust exposure associated with a HIN's standard setting and vendor selection include:

Full disclosure and non-biased standards. All HIN participants should be required to disclose any competitive interest they may have in the HIN's standard-setting activities.

- All interested parties should be afforded an opportunity to be heard with respect to proposed standards.
- HIN Participants should not promulgate standards with the purpose or effect of harming competitors.

Vendor selection processes and objective criteria. The HIN's vendor selection process should ensure all prospective bidders the same access to bid evaluation information. For example:

- The HIN's vendor selection process should include: (1) the issuance of a Request for Proposal (RFP); (2) a statement of objective, fair, and impartial standards or criteria for vendor evaluation and selection; and (3) a public process

---

[139] *See, e.g., American Society of Mechanical Engineers, Inc. v. Hydrolevel Corp.*, 456 U.S. 556 (1982).

[140] *See, e.g., Allied Tube & Conduit Corp. v. Indian Head, Inc.*, 486 U.S. 492 (1988) (upholding Sherman Act Section 1 liability where a member of a fire safety association influenced the association to adopt a biased safety code benefiting its product and disadvantaging competing products).

[141] *See, e.g., Kreuzer v. American Academy of Periodontology,* 735 F.2d 1479, 1492-96 & n.25 (D.C. Cir. 1984) (in determining whether, on balance, the restraint increases or decreases competition, it is necessary to consider whether it is "the least restrictive means" of achieving procompetitive benefits such as improved patient care).

for potential bidders to ask and obtain responses to questions about the RFP (e.g., an open meeting or internet postings of questions and answers).

- Any public reporting by the HIN on RFP responses or the capabilities of particular vendors should be designed to permit individual purchasers to exercise their independent judgment about the vendor(s) with which they may choose to do business outside the HIN.
- Public reporting should provide only factual information about vendors and should not make any recommendation or suggestion about vendors to be used by individual purchasers outside the HIN.

Use third-party data negotiator, if feasible. If feasible, an independent third party should conduct vendor negotiations on behalf of the HIN.[142]

- HIN participants may share "Best Practices" generally applicable to vendor contracting. They should not, however, disclose competitively sensitive information relating to their respective employer's contracts, negotiations, or strategies for contracting with individual vendors outside the HIN.

5-4. Antitrust Exposure Associated with Sharing the Costs of Implementing EHRs

HIN Participants may wish to share the costs associated with implementing EHRs. As a practical matter, the allocation of costs should be closely linked to the HIN Participants' actual cost of network participation. While HIN Participants also may have a shared interest in using financial or other incentives to encourage providers to use the EHRs and to achieve agreed-upon quality measures, agreements on whether and how much to pay providers could create substantial antitrust exposure. Each Participant therefore should individually determine whether and how much they will pay to incentivize provider participation. HIN participants should observe the following guidelines when establishing mechanisms to share costs.

---

[142] It is not an antitrust violation for a participant who negotiates with vendors on behalf of his or her employer (i.e., outside the HIN) to also negotiate on behalf of the HIN. However, the antitrust agencies have stated that where an independent employee or agent who is not also an employee of a participant conducts negotiations on behalf of a collaborative venture, antitrust risk is reduced.

The allocation of costs should benefit all participants. The closer the link between charges and the actual costs of network participation, the less the risk of antitrust liability. For example, an agreement to divide initial, fixed hardware/software costs for providers would benefit all participants, including payors, providers, and patients.

Avoid agreements to pay specified per-patient or per-transaction fees. Each participant should individually determine whether and how much they will pay to incentivize providers to use EHRs and to achieve agreed-upon quality measures.

Establish quality standards (but not financial incentives). Agreements among HIN participants establishing healthcare quality measures should help to promote procompetitive goals.

5-5. Spill-Over Collusion

5-5(a). Potential Liability

HIN Participants must continue to compete outside the limited context of their collaborative venture. Agreements or understandings that limit their ability to do so, or so-called "ancillary agreements," create a risk of *per se* unlawful "spill-over" collusion.[143] Agreements among HIN Participants must be reasonably necessary to achieve the legitimate, procompetitive goals of the HIN. For example, while it may be reasonably necessary for the participants to jointly set prices for the products and services purchased or sold by the HIN, they should not reach any agreement or common understanding relating to the prices of products or services they individually purchase or sell outside the HIN.

5-5(b). Recommendations for Avoiding Spill-Over Collusion

Practical guidelines that can help to minimize potential antitrust exposure of a HIN and HIN Participants for spill-over collusion include:

Prepare and adhere to written agendas. Antitrust counsel should prepare or approve a written agenda in advance of all HIN meetings, the meeting participants should strictly adhere to the agenda, and official meeting minutes should be

---

[143] *Collaboration Guidelines*, 4 Trade Reg. Rep. (CCH) at ¶ 13,160.

prepared for distribution after review by counsel. For antitrust purposes, there is no such thing as “off-the-record” or “unofficial” discussions among HIN participants.

Avoid any appearance of collusion. HIN participants must avoid giving any false impression that they make competitive decisions based on any consideration other than their own independent business judgment, or otherwise are jointly coordinating their competitive activities outside the HIN. HIN participants should avoid communications that incorrectly suggest they are following “the HIN’s instructions” or a “unified policy,” or seeking to create “leverage” or “power in numbers.”

Document legitimate justifications for excluding particular competitors. The HIN should develop, document, and consistently apply objective membership or participation criteria, if participation in the HIN will be limited in any manner. The legitimacy of a particular HIN can be substantiated by identifying any competing organizations and documenting any benefits that will accrue to customers and patients as a result of competition among the organizations.

Document legitimate justifications for including large percentages of competitors. If the HIN will include large percentages of competitors, it should document legitimate justifications for doing so, such as:

- The extent to which the HIN’s inclusion of large numbers of competing participants will increase the degree of shared access to a particular set of EHRs and therefore will increase the opportunities to realize clinical benefits relating to improving communications among participants and reducing the potential for unnecessary duplication of medical testing and services.
- The extent to which the HIN’s inclusion of large numbers of competing participants will lower costs by increasing volume purchasing power for supplies (e.g., equipment and software) and reducing overall administrative costs.

5-6. Conclusion

With appropriate planning and safeguards, a HIN can minimize any unnecessary antitrust exposure associated with the development of EHR, including any necessary information exchanges, standard setting, and vendor selection activities.

CHAPTER 6:
INTELLECTUAL PROPERTY AND OWNERSHIP

In testimony regarding HINs, Dr. David J. Brailer, National Coordinator for Health Information Technology, cited as one of the "great urgencies" surrounding HINs the need to answer the question, "What benefits does being a [HIN] convey upon the participants that they individually or loosely collaboratively couldn't gain themselves?"[144]

From an intellectual property perspective, this question might be rephrased, "What property interests may participants be required to share or relinquish to facilitate the creation of HINs, and are the incentives sufficient for them to do so?" The following discussion addresses the types of intellectual property rights that may be relevant to HINs and interoperable EHR networks, potential issues that counsel should address in advising clients that intend to sponsor or participate in these initiatives, and approaches that may facilitate successful implementation of HINs in the years to come.

Intellectual property issues are seldom the main focus of attention when a provider is selecting an EHR system or a group of healthcare organizations are structuring a HIN. Yet the right to own and use the information compiled and the processes used in conducting these operations will be governed in large part by intellectual property laws and the agreements between the parties. No matter which structure a HIN takes, the participants will need to obtain the necessary rights and licenses to have access to, store, use, or display information contained in a medical record. Specific circumstances and local law may make it appropriate to handle these issues differently and to address conflicts that may arise between these bodies of law.

This Chapter identifies issues from the perspective of a user of technology provided by a vendor (typically pursuant to a license) and from the perspective of a member of a HIN that may contribute to the creation of new intellectual property. Attorneys structuring such arrangements should consider which type of intellectual property protection would be most suitable for each type of asset in the HIN or EHR arrangement and the extent to which contractual arrangements among the parties

---

[144] Testimony before the National Committee on Vital and Health Statistics (Nov. 4, 2004), http://www.ncvhs.hhs.gov/041104tr.htm.

should affect the rights of the parties both during the term and after termination or expiration. The complexity and intertwined nature of these possible protections and contractual provisions makes it appropriate to seek the advice of specialized intellectual property counsel at an appropriate stage.

6-1. Types of Intellectual Property

The primary types of property to be addressed in this analysis include the following:

- Software used in operating the EHR or HIN;
- Databases of information regarding the patients, their diseases and conditions and the care provided;
- Aggregated forms of such patient information which may be de-identified to some degree;
- Research results developed using patient information;
- Ideas and inventions regarding how the EHR or HIN should operate (business processes); and
- Trade names, trademarks, service marks, trade dress, and logos used in conducting the activities.

Each of these types of property may be subject to one or more types of intellectual property protection as described briefly below.[145] They may also be the subject of agreements among the parties governing ownership, rights to use and sublicense to others, and non-disclosure. Such contractual provisions may limit use of databases and other information beyond the scope of a party's intellectual property rights in order to achieve business objectives.

[145] Due to space limitations, this Chapter does not address issues relating to trademarks, service marks, trade dress, or trade names that may be used in HINs and EHRs. However, the use of any party's name or mark (or a substantially similar name or mark) should be carefully reviewed with respect to protection, possible consumer confusion and liability for acts of the licensee, dilution of the intellectual property and the appropriate use or prohibition of further use after termination of the arrangement.

6-2. Intellectual Property Laws Affecting Interoperable EHRs

6-2(a). Copyright Law

6-2(a)(1). General

Copyright protection is an ownership right in an original work of authorship fixed in a tangible medium of expression.[146] Copyright protection does not extend beyond the specific copyrighted "form of expression" of the copyrighted material and therefore does not protect the information or idea itself. For example, a copyrighted database is protected with respect to the form of the database, including its contents, but the actual information contained within the database is not independently protected.

Copyright protection does not require registration with the Copyright Office, although registration is required to bring an infringement action under federal law. Protection is not lost if the owner fails to include a copyright notice on the work (usually the © symbol or the word "copyright," the year, and the name of the owner). However, use of a copyright notice is recommended to reduce the risk that a defendant claims to have innocently copied the work.

Copyrightable subject matter in the context of EHRs and HINs includes computer software, compilations of data, written text, and images fixed to electronic storage media, but generally does not protect processes, systems, methods of operations or other inventions. Forms, patient information, databases, information contained on Web sites and other written materials used in an EHR or HIN, whether electronic or paper, would also be subject to copyright, although the protection is limited to the form of expression, not the information itself.

6-2(a)(2). Open Source Software

If software is being developed for the EHR or HIN, counsel should ask whether any components used in the software are "open source." Computer programs for which the source code is publicly available (and for which copyright and patent protection has been intentionally given up in whole or in substantial part under specified conditions) are referred to as open-source software. Inherent in the open source philosophy is the freedom of an often unrelated community of programmers to modify and improve the

---

[146] 17 U.S.C. § 102(a).

code. The most widely known example of open-source software is the Linux operating system.

Although sometimes referred to loosely as an approach that makes software "free" to all, open source is a creature of contract, namely the license terms posted by a variety of groups. One of the best known is the "GNU" General Public License,[147] which includes the following terms with respect to the programs that some software authors have elected to make subject to its terms:

> 2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
>
> a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
>
> b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License . . . .
>
> 3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
>
> a) Accompany it with the complete corresponding machine-readable source code . . . or
>
> b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code . . . .[148]

For most commercial software developers, the terms of the GNU General Public License would be unacceptable because they require further distribution without charge

---

[147] Available at http://www.gnu.org/copyleft/gpl.html.
[148] *Id.*

and require the distribution of source code (often viewed as destroying the ability to charge a license fee). Use of open source programs in developing software therefore may have very serious consequences, depending on the terms of the open source license.[149] Those opposed to open source point out potential concerns, including that the availability of such "free" software will decrease the profit motive of proprietary software development and decrease the pace of technological advancement for those companies that do not feel that enabling everyone to share their intellectual property is profitable.

However, the open source approach has strong adherents. Advantages of open source are thought to include: (a) broad peer review to detect and correct bugs and make improvements that contribute to reliability and performance features; (b) the ability to avoid dependence on a monopoly supplier, resulting in lower costs; and (c) the promotion of rapid and accessible software development.[150]

6-2(b). Patent Law

6-2(b)(1). General

Patent rights can be viewed as an agreement between the inventor and the United States government. In effect, the inventor agrees to disclose the invention to the public in exchange for being granted the legal right to prevent others from making, using, selling, offering for sale, or importing the invention for a specific period of time.[151] Subject matter that may be patented is defined as "any new or useful process, machine, manufacture, or composition of matter, or any new or useful improvement thereof."[152] Patentable "machines" include computers, integrated circuit chips, and networks.

---

[149] Some "open source" licenses do not impose such extreme requirements on derivative works created by using the subject software. *See* the license for the PostgreSQL software made available by the Regents of the University of California at http://www.postgresql.org/docs/faqs.FAQ.html.

[150] Bryan Bruns, *Open Sourcing Nanotechnology Research and Development: Issues and Opportunities*, prepared for the Foresight Conference on Molecular Nanotechnology (Nov. 3-5, 2000, Bethesda, Md.).

[151] The patent term for patent applications filed after June 8, 1995 is twenty years from the date on which the patent application was filed or the earliest date to which the patent application claims priority. 35 U.S.C. §154(a)(2).

[152] 35 U.S.C. § 101.

Patentable “processes” include methods for operating computers, sending data over a network or displaying information on a screen.[153] Software may also be patentable.[154]

Unlike copyright protection, which focuses primarily on authorship of a work and form of expression, patent rights focus on the inventive system, article, or process and require:

- Novelty;
- Nonobviousness;
- Utility;
- Enablement; and
- Best mode.[155]

In order to be novel, the invention must not have been sold, publicly used, or disclosed within certain time periods prior to filing a patent application. The nonobviousness requirement involves an analysis of whether the invention would be obvious to someone of ordinary skill in the “art” (*i.e.,* the relevant field of knowledge) at the time of the invention. The enablement requirement is satisfied if the description in the patent is sufficient to enable a person of ordinary skill in the art to practice the invention by reading the patent. The best mode requirement is satisfied if the application discloses the best way to make and use the invention that is known to the inventor.

A wide range of machines, processes, and related improvements may be patentable in the EHR and HIN context, assuming that all of the required standards for patentability and filing requirements are met. For example, the computers and telecommunications equipment used may include patented components Of more relevance to the participants in a HIN or users of an EHR are possible patents on the software and the business processes used in the HIN itself or the EHR (*e.g.,* methods of data submission, data standards, or data sharing).

---

[153] Lewis C. Davis and J. Scott Davidson, INTELLECTUAL PROPERTY FOR THE INTERNET § 1.5 (1997).
[154] *Id.* at § 5.36.
[155] 35 U.S.C. §§ 102, 103 and 112.

6-2(b)(2). Patent Pooling

In a perfect world, all constituencies in healthcare would agree upon common standards for interoperability and there are indications that some vendors are trying to do so.[156] However, it may be necessary to have HIN Participants license patents and technologies protected as trade secrets or copyrights to each other.

One potential solution is patent pooling. A "patent pool" has been defined as "the aggregation of intellectual property rights that are the subject of cross-licensing, whether they are transferred directly by patentee to licensee or through some medium, such as a joint venture, set up specifically to administer the patent pool."[157]

Pooling of patents and technology may present a path to cooperation by otherwise competing companies. Additionally, patent pooling permits licensees to obtain all licenses necessary to implement the agreed upon standards without having to approach multiple companies for various licenses, with no assurance that all licenses needed will be granted or that additional licenses that arise after the initial technology development may be required. This approach is echoed in a report assessing the progress of the Santa Barbara County Data Exchange, which noted that "[p]articular attention needs to be given to fostering a *portfolio of information tools* that support all levels of information exchange sophistication that are available . . . ."[158]

Patent pooling may raise antitrust issues as noted by the Department of Justice's guidelines for forming patent pools.[159] In particular, the *IP Guidelines* state that intellectual property pooling is procompetitive when it:

(1) integrates complementary technologies;

(2) reduces transaction costs;

---

[156] A consortium of leading technology companies appears to be evaluating common standards. *See* Steve Lohr, *High-Tech Alliance on Base for a Digital Health Network*, N.Y. TIMES, Jan. 26, 2005.

[157] *See* JOEL I. KLEIN, AN ADDRESS TO THE AMERICAN INTELLECTUAL PROPERTY LAW ASSOCIATION, ON THE SUBJECT OF CROSS-LICENSING AND ANTITRUST LAW (May 2, 1997), *reprinted at* http://www.usdoj.gov/atr/public/speeches/1123.htm (noting that *United States v. Line Materials*, 333 U.S. 287, 313 n.24 (1948), states that the term "patent pool" is not a term of art).

[158] California HealthCare Foundation, *Moving Toward Electronic Health Information Exchange: Interim Report on the Santa Barbara County Data Exchange* at 34 (July 2003).

[159] *See* U.S. DEP'T OF JUSTICE & FED. TRADE COMM'N, ANTITRUST GUIDELINES FOR THE LICENSING OF INTELLECTUAL PROPERTY (1995) (IP Guidelines), *reprinted at* http://www.usdoj.gov/atr/public/guidelines/ipguide.htm.

(3) clears blocking positions;

(4) avoids costly infringement litigation; and

(5) promotes the dissemination of technology.

The *IP Guidelines* also discuss that excluding firms from an intellectual property pool may be anticompetitive if:

(1) the excluded firms cannot effectively compete in the relevant market for the good incorporating the licensed technologies;

(2) the pool participants collectively possess market power in the relevant market; and

(3) the limitations on participation are not reasonably related to the efficient development and exploitation of the pooled technologies.

The guidelines were "collapsed" at least as of 2000 into the following two overarching questions: (1) "whether the proposed licensing program is likely to integrate complementary patent rights"; and (2) "if so, whether the resulting competitive benefits are likely to be outweighed by competitive harm posed by other aspects of the program."

6-2(c). Trade Secret Protection

Trade secret protection is similar to patent protection in that it protects information rather than the manner in which the information is expressed. However, trade secret protection does not require public disclosure and further does not prevent third parties from independently developing and practicing the otherwise protected trade secret information. Unlike the federal patent law, trade secret protection is determined by state law and therefore varies by jurisdiction. We discuss the Uniform Trade Secrets Act in this Chapter, as many states have adopted the Act or close variations of it.

The Uniform Trade Secrets Act defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique or process," that "(i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by other persons who can obtain economic value from its disclosure or use, and (ii) is subject of efforts that

are reasonable under the circumstances to maintain its secrecy."[160] Definitions of trade secrets vary by state statute and case law, but typically require the presence of confidential information that is valuable to an enterprise by providing an advantage over competitors who do not have the information. To create and maintain a trade secret, the owner must take affirmative steps to keep the subject matter secret by implementing appropriate internal procedures and, where disclosure to third parties is necessary, entering into non-disclosure agreements.

However, in order to protect ideas and information as trade secrets, they must be held in confidence and steps must be taken to preserve them as secret in dealings with third parties. In the context of an EHR or HIN, protection of trade secrets will require both practical measures to limit access and disclosure to only those who need to know the information as well as non-disclosure agreements. Agreements will generally be needed with employees, consultants, independent contractors, and employees consistent with applicable state law. In drafting such agreements, careful attention should be paid to exceptions sometimes viewed as standard, such as exceptions for disclosures "required by law."

For example, the entity seeking to protect the trade secret may want to have prior notice of a disclosure required by law so that it can resist the disclosure or seek a protective order. The obligation of a recipient of trade secrets to impose similar obligations on its employees or contractors should also be included, although few entities are willing to have a separate agreement signed by each of its employees to protect the disclosing party's trade secrets. Instead the receiving entity may promise to have all employees be bound by its standard form that generally describes obligations to third parties.

It should also be noted that non-disclosure agreements are frequently used with contractual provisions that limit use of software, databases, or "know how" in order to achieve business goals of the parties that are broader than the protection of intellectual property assets. These provisions need to carefully address the ownership of interests of the parties and the rights to use various intellectual property depending on who

---

[160] Unif. Trade Secrets Act § 1.

owned it prior to the arrangement, who contributed to its development and what use is needed after termination in order to transition to another system and to avoid any interruption in care.

6-2(d). Other Theories

Although copyright, patent, and trade secret laws are most commonly applied to protect the intellectual property associated with the development and use of interoperable EHR, some further measure of protection may be available under case law pertaining to property rights, quasi-contract rights, implied contract rights, and fiduciary obligations. Such protection is beyond the scope of this Chapter and, as with the other issues raised herein, advice on these topics should be sought from competent legal counsel.

6-3. Ownership Issues

In developing a HIN, counsel should deal with the ownership of the tangible data created by an EHR—medical records and other data. It will be important to clarify in advance property and other ownership issues in negotiating and documenting the respective rights of the parties with respect to interoperable EHRs and HINs.

State statutes or regulations sometimes expressly define who controls and owns the medical record itself. These statutes and regulations generally designate the entity creating the record as having ownership rights to that record.[161] In states without such express statutes or regulations, counsel should consult the case law on these ownership issues.

State medical records laws (and HIPAA) also define when patients may access information in their own medical records. The majority of states provide a statutory right of access to a person's own medical records that are in the possession of the person's healthcare provider.[162] These laws often very specifically pertain to an individual category of healthcare provider (i.e., hospital,[163] HMO,[164] or insurance company[165]) and

---

[161] *See e.g.,* LA. REV. STAT. ANN.,§ 40:1299.96(A)(2)(b) (providing that medical records are the property and business records of the healthcare providers); *see also*, South Carolina, S.C. CODE ANN. § 44-115-20.

[162] *See, e.g.,* GA. STAT. ANN. §§ 31-33-2; 31-33-1; COLO. REV. STAT. ANN. §§ 6-18-103(3)(b); 25-1-107; 25-1-801.

[163] ME. REV. STAT. ANN. tit. 22, §§ 1711; 1711-B.

the laws are woven throughout a state's code. While states acknowledge an individual's interests in accessing one's medical record, no state has granted a broader ownership interest in medical records to its citizens.[166]

If under applicable law providers own the medical records being shared, the HIN agreements with participating healthcare providers should contain provisions that explicitly allow these records to be used by the HIN, the operator of the HIN, or other participants in these arrangements. The right to use could be documented as a license within a participation agreement or separately. Providers might try to negotiate compensation for the value of the license granted, particularly if the HIN's activities include research that could lead to pharmaceuticals or other commercial products.

The scope of permitted use under the license should be addressed. For example, the HIN Participants may wish to limit the use of their records not related to the treatment of a patient by the Participant accessing the record, so that the Participants' records may not be used for competitive or risk management reasons. The HIN Participants may also wish to limit the right of others to use the Participants' records only during the term of the agreement. On the other hand, limiting the use of the records to the duration of the agreement could reduce the comprehensive and long term nature of the databases expected to evolve from HINs, which could in turn jeopardize the expected improvements in patient care and reduction of errors. It is also possible that the operators of HINs will change over time as financial models shift and these organizations consolidate, which may result in the need to have new entities continue to operate databases that include the provider's medical records. For example, it would be extremely difficult to obtain the consent of the hundreds of providers who are expected to participate in these initiatives for the continuing use of the records after they retire or if a successor to the original HIN continued its operations.

---

[164] CAL. HEALTH & SAFETY CODE § 1364.5.

[165] North Carolina, N.C. GEN. STAT. § 58-39-10.

[166] In addition, no state provides a constitutional right to access medical records. In New York, a patient attempted to bring a private cause of action against her mental healthcare provider, claiming to have a right under the state constitution to have access to her record. The district court, and then the court of appeals, analyzed the state constitution and determined that there was no constitutional right to access to one's medical records. *See Gotkin v. Miller*, 379 F. Supp. 859 (E.D.N.Y. 1974), *aff'd*, 514 F.2d 125 (2d Cir. 1975).

The best way to address these issues is likely to be negotiation of perpetual licenses to use the Participants' records for purposes of the EHR or HIN. The provision would need to be carefully drafted to allow continued use by successors to the original entities and changing circumstances. The alternative approach would be to revise the Participants' rights at the state level, but we expect that this would be extremely time consuming, unpopular with providers and not lead to a uniform set of provisions. We expect that these fundamental issues regarding data will be of concern to vendors that operate HINs and develop databases and to members of a HIN or EHR arrangement that wish to benefit from a clinical database.

6-4. Infringement Indemnity

A licensee of a software licensor or a customer of a service provider would usually want assurances from the vendor or service provider that it has the legal rights to license the software or provide the services without infringing or misappropriating the intellectual property rights of others (usually listing copyright, patent, trademark, trade secret, and other intellectual property rights). This protection is usually provided in a representation and warranty of the licensor/service provider, with further assurances in the form of indemnification against any third-party claim of infringement or misappropriation. The licensee/customer should carefully review the limitation of liability and consequential damage provisions of the agreement to make sure that they do not limit these protections to an unacceptable extent.

These issues should also be negotiated with respect to developers who may provide custom modifications for standard software or materials or develop new software for a HIN or EHR sponsor to meet specific needs. Ownership of the copyright in modifications or enhancements should also be negotiated because in many instances an independent developer will be the copyright owner in the absence of an agreement to the contrary.

The HIN or EHR sponsor may itself be asked by the HIN Participants to provide representations and indemnification with respect to software and other materials that it makes available to the Participants. In evaluating such requests it is important for the HIN or EHR sponsor to understand the risks and the scope of protection that it obtained from third-party licensors and vendors so that it does not assume more risk than the

third-party vendors that were in a far better position to minimize these risks in development. Ideally, the Participants would have the direct right to be indemnified by the third-party licensor or vendor without having to demand indemnification from the HIN or EHR sponsor.

If participants in a HIN or EHR collaborate in producing software or other materials the agreement between them should allocate ownership and license rights in the resulting works. It may be appropriate to have the right to use the works terminate if a participant ceases to be a member of the group.

In addition, a licensee of software or a recipient of services provided by a third-party vendor should make sure that the license or services agreement includes representation, warranty. and indemnity provisions to place the risk on the vendor with respect to infringement of third-party patents and trade secrets. The participation or other agreements should also address ownership and rights to use any patentable inventions developed in the course of any collaboration or developments. Perhaps the most significant risk is that the arrangement will inadvertently infringe a business process patent that was unknown to any of the participants.

CHAPTER 7:
MEDICAL MALPRACTICE AND OTHER POTENTIAL LIABILITY

Among the legal issues that may function as a barrier to the deployment of EHRs include concerns about increased physician malpractice and similar liability exposures.[167] As we discuss in this Chapter, some of the concern about malpractice/liability exposures may be justified, while some of it may simply be resistance to change and general apprehension. However, because physician acceptance of EHRs is essential to their success, a discussion of malpractice liability may be helpful in diminishing apprehension in transitioning to the use of EHR.

Unfortunately, there is little guidance in the law regarding increased malpractice exposure. Because the technology itself is novel, there is no case law or applicable statutes to help explain the basis for liability. An analysis of the malpractice concern thus must begin with a review of two more general issues. First, under existing malpractice case law, is there a well-recognized and prevailing duty to consult a patient's past medical records? Second, how rapidly has new technology influenced the standard of care in malpractice cases in other aspects of healthcare delivery?

7-1. Medical Malpractice

7-1(a). The Duty to Consult Medical Records

Malpractice is a cause of action that by its nature differs from other liability theories in ways that may make it less susceptible to sudden change. A successful malpractice claim must demonstrate that harm arose from a departure from the "standard of care." The standard of care must be established by medical expert testimony and the harm for which the plaintiff seeks damages must proximately arise from a breach of the standard of care.

Because the standard of care in medical malpractice cases is based upon medical expert testimony, it is an evolving, normative measure of physician performance. Failure to consult medical records *may* not be negligent today, but as the standard of care evolves, failure to consult may constitute negligence in the future.

---

[167] *See*, *e.g.*, "HHS's Efforts to Promote Health Information Technology and Legal Barriers to Its Adoption," GAO-04-991R, Enclosure I, p. 51, Aug. 31, 2004.

Thus, a claim for malpractice involving an EHR would have to show that: (i) the standard of care included a duty to consult the medical record; and (ii) the electronic technology involved was the medium dictated by the standard of care to access the medical record in question.

Although the threat of malpractice as a barrier to implementation of EHRs may appear real, the case law on the basic question of whether physicians have a duty to consult a record (in any medium) is sparse and far from conclusive. For example, in a Texas case,[168] the plaintiff brought a wrongful death action against an anesthesiologist because an eighteen-year-old paraplegic died during surgery when her chest filled with intravenous fluid. Plaintiff alleged multiple departures from the standard of care as the cause of death, including the defendant's failure to obtain the patient's past medical records prior to surgery. However, three defense experts testified that it was not the standard of care to obtain past medical records prior to the type of surgery involved. Affirming a grant of summary judgment below, the court agreed that the standard of care did not require the defendant to obtain past medical records.

Likewise, in Illinois,[169] the plaintiffs alleged that a pediatrician violated the standard of care when, among other things, the pediatrician did not consult the medical records of a newborn infant prior to well baby visits shortly after the birth of the infant. The physical examination of the pediatrician evidenced a child "doing well" although four days later the infant was treated on an emergency basis for cardiorespiratory arrest. Medical experts for plaintiff and defendant differed regarding whether failure to obtain the infant's birth medical records from a hospital departed from the standard of care. Because a judgment for the defendant was supported on appeal by adequate evidence, the jury resolved the question in favor of the defendant.

Other cases have found that a failure to obtain past medical records is a departure from the standard of care. For example, the First Circuit Court of Appeals sustained a verdict for the plaintiff that involved, in part, finding that defendant was

---

[168] *Suniga v. Eyre*, 2004 Tex. App. Lexis 486 (unpublished).
[169] *Susnis v. Radfar*, 2000 Ill. App. Lexis 859, 739 N.E. 2nd 960 (Ill.App., 2000).

negligent in failing to obtain plaintiff's past medical records.[170] Medical experts for both sides testified that the standard of care either did, or did not, require obtaining past medical records. When a jury found for the plaintiff, the court concluded on appeal that the verdict was reasonably based on the evidence and could not be overturned.

In the foregoing cases, medical expert testimony on the duty to consult past medical records as a component of the standard of care was conflicting. One might then fairly conclude that there are no indications of a broad-based and prevailing duty to consult a patient's past medical records, although in some cases the duty may be a part of the standard of care. Assuming that in some circumstances there is a duty to consult medical records, the next question is whether deployment of an interoperable EHR system will expose physicians to enhanced malpractice exposure.

7-1(b). The Adoption of New Technology

Notwithstanding case law suggesting that the duty to consult past medical records is circumstantial and limited, discussion of the interoperable EHR also suggests that technology itself may drive enhanced malpractice exposure. While there is no case law specific to the interoperable EHR, there is thought-provoking scholarly comment on the role of technology and malpractice:

> Medical research and the Internet now provide physicians with more information than they have ever been able to utilize in the past. Online databases of medical literature, such as Medline, allow the physician immediate access to information that can influence treatment and possibly save lives (Kacmar, 1997). The medical profession may soon reach a point where a physician can put a patient's symptoms into a web-based form and the computer will offer a diagnosis. The physician also will be able to "chat" on-line with other doctors about the patient's symptoms to receive opinions from experts who previously would have been unavailable due to geography or time constraints. Clearly, techniques such as these call into question what constitutes reasonable care. If a physician

---

[170] *Primus v. Galgano*, 2003 U.S. App. Lexis 9803, 329 F.3d 236 (1st Cir., 2003).

> does not utilize new information or is negligent in gathering the results, this could qualify as substandard care and expose the physician to liability.[171]

As logical as the case appears that a new technology changes the standard of care and thereby enhances medical liability exposure for laggard adopters of a given technology, there is little hard evidence to support this view. Case law suggests that medical experts testifying on technology as essential to the standard of care may recognize the virtues of technology. However, expert testimony also suggests that the standard of care involving technology changes rather slowly. Thus, a new technology may change the standard of care, not in a matter of a few years, but over a number of years, as technology gradually becomes the standard of care.

Consider, for example, a New Jersey malpractice case involving fetal monitoring.[172] The defendant physician chose not to use ultrasound monitoring equipment, present and available in his office, in favor of what one expert dubbed "1960's style" maternal fetal monitoring based upon the mother counting fetal movements. Expert testimony was given both ways on whether the standard of care required the use of ultrasound. Expert testimony favoring electronic fetal monitoring noted that it had become available in the early 1970s, twenty years before the incident in question occurred. The trial court submitted the case to the jury under New Jersey's "medical judgment" rule that allowed the jury to find for the defendant. Following two lengthy appeals to New Jersey's Supreme Court, the court held that the "medical judgment" charge was improper. In a comment that captures the change cycle of medical technology, albeit one occurring at an almost glacial pace, the court stated:

> Here, plaintiff was a first-time expectant mother with gestational diabetes. Defendant was an experienced physician who had modern equipment in his office that would have enabled him to comply with the standard of care described by plaintiff's expert. Although the jury was entitled to believe defendant's expert's

---

[171] *See* Jacobsen, P. D., Medical Liability and the Culture of Technology, Project on Medical Liability in PA, 7/2004. http://medliabilitypa.org.

[172] *Das v. Thani*, 2002 N.J. Lexis 548, 171 N.J. 518 (N.J., 2002).

> testimony that using the modern equipment was not required by the appropriate standard of care, the jury was not given a road map on how to make that determination. The jury was not properly instructed that it could do so only if the decision not to use the modern equipment represented an equally acceptable and objectively reasonable determination based on plaintiff's medical condition. That shortcoming created a substantial likelihood of improperly insulating defendant from liability.[173]

Left to medical experts and the courts, new technology clearly penetrates the standard of care in medical malpractice cases, but it appears to do so very slowly. Even a casual reader of this case has to be struck by the court pushing for the technology-based standard of care, but a jury apparently accepting the practice of counting fetal kicks, fully twenty-five years after electronic fetal monitoring became available. Technology may bring change, but the standard of care changes slowly.

Left to itself, change based upon malpractice litigation, verdicts, and appeals is slow. However, other factors could come into play that would accelerate the rate of change and force the adoption of a standard of care that assumes the use of interoperable EHRs.

7-1(c). The Effect of Enabling Legislation Requiring or Incentivizing the Deployment of EHRs

Legislation mandating EHRs, setting uniform standards for EHRs, or offering incentives for their deployment and use could affect liability questions. Although the public policy debate on EHRs is in its infancy, the concept has attracted legislative interest at both the federal and state levels. In a speech to the National Press Club in July, 2004, Senate Majority Leader William Frist outlined a range of health policy initiatives, including incentives and standards to promote interoperable electronic

---

[173] *Id*. at 530.

medical records.[174] Many states have enacted or are considering legislation to support EHRs.[175]

Legislation might affect the liability issues associated with EHRs in different ways. For example, legislation could provide limitations on liabilities that would dispel the current concerns about enhanced liability from using an EHR. Conversely, legislation could change how courts look at the standard of care and accelerate a change in the standard of care that would expose those not using EHRs to greater liability. Another possible approach would be a statute providing rights and protections, even a private right of action, for patients whose medical records are stored electronically. More specific, legislation might articulate a set of standards for EHRs that a court could adopt as the standard of care. Failure to meet the legislatively ordained standard of care, sometimes called per se negligence, could accelerate the development of malpractice cases based upon a failure to consult an available EHR.

On occasion, courts have looked at the standards of accrediting bodies to articulate a standard of care in negligence cases. It seems likely that entities will seek to accredit users of EHRs.[176] Certainly, there is judicial precedent in healthcare for accreditation standards becoming the standard of care.[177] At this very early stage, one can do no more than simply observe that accreditation standards could play a comparable role in EHR development and in articulating a standard of care.

7-2. Other Potential Liability

While discussion of malpractice as a legal barrier to EHRs by its nature centers on physician concerns, liability could extend to other providers, such as hospitals or ambulatory care facilities that may be early adopters of EHR technology. These entities may be subject to claims for corporate negligence, a claim for liability based upon an

---

[174] BNA Healthcare Daily, Volume 9 No. 133, July 13, 2004.
[175] *See, e.g.,* Fla. Stat. Ann. § 381.0271; Senate Bill 5064, State of Washington, 59th Legislature, 2005 Regular Session.
[176] For example, the Certification Commission on Health Information Technology (CCHIT) has been formed recently directly in response to the federal effort to promote EHRs. CCHIT proposes to "create an efficient, credible, sustainable mechanism for the certification of healthcare information technology products." www.cchit.org. visited, 01/12/2005.
[177] *See, e.g., Darling v. Charleston Community Memorial Hospital*, 211 N.E.2d 253 (Ill., 1965) (accreditation and licensing standards helped establish the doctrine of hospital corporate liability).

independent duty of care owed by a provider institution to its patients. Corporate liability involving EHRs could be triggered by premature or inadequate deployment of EHRs that results in EHR-related errors, such as inadequate staff training, flawed applications, or inadequate IT infrastructure. As with any technology, errors may occur. For example, a recent study by United States Pharmacopeia reported that computerized physician order entry (CPOE) accounted for nearly 20% of all hospital and health system prescription errors during 2003 and that the percentage of errors attributable to CPOE has been rising steadily.[178]

Significantly, corporate liability would not be based on a standard of care established by the testimony of medical experts. Rather, corporate liability would be based upon a judicially-adopted standard of care that might reflect industry standards or accreditation criteria.[179] Experts who testified on the standard of care might be information technologists, or chief information officers whose testimony could reflect a faster moving and evolving view of their industry. In this sense, a court could move more aggressively to adopt a standard of care for corporate negligence that reflects use of EHRs as state of the art technology.

Other cases suggest that courts might be more aggressive in areas where EHRs play a central role in the relationship between the provider and the injured individual. For example, health management activities that are highly dependent on electronic health information might be more susceptible to rapid development of general negligence theories. Consumer driven healthcare or disease management programs are two areas that might be technologically dependent on forms of EHRs or similar health information technology, and therefore might owe a higher duty of care in the deployment of those systems.

---

[178] BNA, Healthcare Daily, Volume 9, Number 245, 12/22/2004. "It would seem logical that applying computer technology to the medication use process would have a significant positive impact in preventing medication errors," Diane Cousins, vice president of USP's Center for the Advancement of Patient Safety, said in a Dec. 20 statement. "Yet, depending on the computer's design or user competence, new points of potential errors can emerge. Healthcare providers need to be focused and vigilant in their use of computers."

[179] *See Darling v. Charleston Community Memorial Hospital*, 211 N.E.2d 253 (Ill., 1965).

For example, in Pennsylvania a court imposed corporate liability on a health plan that had established a health plan call center and was negligent in arranging adequate prenatal care for a subscriber of the plan.[180] The case is interesting because the legal basis for liability is explained in part on the role that the health plan voluntarily undertook to utilize telecommunications technology to manage the care of its members. If the facts were changed from a call center to an online EHR integrated into the disease management program on the Web site of a consumer driven health plan, the reasoning in this case might apply with equal force.

7-3. Conclusion

The risks of malpractice and related liability arising from the deployment and use of interoperable EHRs are somewhat exaggerated and should not be seen as a genuine barrier to an interoperable EHR system. Indeed, liability insurers may see the risk-reward equation exactly opposite; giving incentives and discounts to users of EHRs whose medical errors may diminish with EHRs. Even if left to the ordinary course of judicial scrutiny and review, EHRs will, at best, change the standard of care slowly and the risk of their adoption will be little different from the legal risks associated with many other technologies that have, on balance, greatly benefited healthcare delivery.

---

[180] *Shannon v. McNulty*, 1998 Pa. Super Lexis 282.

CHAPTER 8:
STATE LAW

This Briefing largely has addressed federal laws relevant to interoperable EHR. While it is clear that federal laws such as HIPAA have created a certain measure of uniformity among the states regarding health information, it is likewise clear that state laws may pose significant challenges to creating interoperable EHRs.[181] This Chapter discusses the impact of state laws and regulations governing medical records, pharmacies, institution and physician licensure, and electronic signatures.

8-1. State Medical Records Laws and Regulations

8-1(a). Medical Record Content Requirements

The standardization of health records is inhibited by the lack of uniformity among state laws governing the content of medical records. For example, the required content of health records may vary for different types of providers. Moreover, different states mandate different record content for the same types of providers. Some states may even require that paper forms be included in the medical record, or have differing requirements for EHRs. These differences should be analyzed during the course of creating a HIN or network of interoperable EHRs. This Chapter uses Illinois, Ohio, and Florida law as examples of differences in state laws; a fifty-state comparison would likely find many more differences.

A HIN including more than one type of provider will have to accommodate a likely patchwork of medical records laws for different types of providers—even within one state. For example, Illinois regulations require more data elements in medical records of long term care facilities serving residents under age twenty-two, versus long-term care

---

[181] The issue of the scope and authority of a state law outside its borders is, of course, inherent to any discussion of the impact of state laws, and will likewise play a role in the interoperability of EHR. For example, in *Quintiles Transnational Corp. v. WebMD Corp.,* No. 5:01-CV-180-BO(3) (E.D.N.C. 2001), the parties' dispute included the applicability of state privacy and health information laws to transactions occurring within and outside of a state's borders. In an order of March 20, 2001 that granted Quintiles' request for a preliminary injunction, the federal district court ruled that "[i]t is well established that the Commerce Clause precludes a state from regulating a commercial transaction outside of its jurisdiction, even if the article of commerce at issue had a connection to that state or the effect of the transaction would be felt by the state." Shortly thereafter, WebMD appealed this order to the U.S. Court of Appeals for the Fourth Circuit. The parties ultimately settled the case prior to the determination of WebMD's appeal. Although a full discussion of the implications of the Commerce Clause is outside the scope of this chapter, healthcare entities and their counsel need to be aware of this issue.

facilities serving residents above that age.[182] In accommodating different medical record laws, a HIN would be required to create an EHR format that includes all data elements required by the most rigorous medical record content law, even though not all providers would be required to populate all data.

A HIN that includes providers from more than one state faces an even more complicated task of accommodating the additional variation in medical records laws between states. The requirements for content of the medical record can vary considerably. For example, the Illinois and Florida requirements for hospital medical record content vary considerably.[183] Moreover, while many states regulate the content of medical records only at hospitals, nursing facilities, and ambulatory surgery centers, a minority of states regulate the records of other providers such as HMO provider sites,[184] dialysis centers,[185] or multiphasic health testing centers.[186]

A HIN also must accommodate isolated state requirements to have elements of a medical record in paper form. For example, some laws require a Do Not Resuscitate order to be on bright orange paper.[187] These state laws that require paper records potentially pose the largest challenge to the development of a fully electronic health record.

Finally, states with regulations concerning EHRs may have varying requirements for features of the system. Illinois, for example, requires an authentication process for hospital records that requires "completion of certain designated fields for each type of document before the document may be authenticated, with no blanks, gaps or obvious contradictory statements appearing within those designated fields."[188] The greater the number of unique system requirements, the more customization would be required to implement electronic records, at greater expense.

---

[182] Ill. Admin. Code tit. 77, §§ 300.1820 (a) and (b), 390.1620 (a) and (b).
[183] Ill. Admin. Code tit. 77, § 250.1510(b)(2) (eight basic elements); Ill. Admin. Code tit. 77, §§ 250.1830(h)(1) and (2) (additional requirements for obstetric and neonatal records); Florida Admin. Code Ann. r. 59A-3.270(3), (4)(24 elements in hospital medical records, with additional elements for surgical cases).
[184] *See, e.g.,* Ill. Admin. Code tit. 77, § 240.90; Florida Admin. Code Ann. r. 59A-12.005.
[185] *See, e.g.,* Ohio Admin. Code § 3701-83-23.3.
[186] *See, e.g.,* Florida Admin. Code Ann. r. 59A-6.026.
[187] Ill. Admin. Code tit. 77, § 515.380(e).
[188] Ill. Admin. Code tit. 77, § 250.1510(c)(6).

The ability to share health information among providers will be greatly enhanced if health information consists, in part, of standard data elements that may be transmitted using consistent protocols. The present HL7 process for the development standards for EHR might take into account differing state laws (or state laws might be amended to reflect a national consensus and standard-making for the content of medical records). Alternatively, federal policy makers could consider a federal law to preempt state laws inconsistent with federal EHR standards to facilitate the development of interoperable EHR.

8-1(b). Medical Record Retention Requirements

Satisfying state retention requirements in the interoperable EHR also is no easy task. In most states, the standards and requirements for creating, maintaining, and retaining patient health records are organized around a specific type of institution or provider—an approach fundamentally at odds with a standardized EHR that can be accessed and amended by a wide range of healthcare providers and suppliers in a wide range of settings. For example, the retention period for hospital patient records likely will be much longer than the retention period for laboratory records. Thus, even states that have amended their regulations expressly to allow for EHR must operate within the confines of a basic structure that is contrary to an interoperable EHR that accommodates different types of providers.

In addition, counsel should be cautious of state laws and implementing regulations that govern *where* a medical record must be retained or stored. In California for example, applicable regulations require government permission before storing patient health records off-site of the facility premises.[189] How does that requirement apply to records stored electronically, perhaps at a database kept off-site, when those records are retrievable at the facility of each HIN Participant? In Illinois, access to the EHR over the entire retention period meets the regulatory requirements.[190]

---

[189] "Health records can be stored off the facility premises only with the prior approval of the Department." CAL. CODE REGS. tit. 22, § 72543(h). "The patient health record shall not be removed from the facility, except for storage after the patient is discharged, unless expressly and specifically authorized by the Department." *Id., at* § 72543 (i).

[190] "Electronic Medical Records Policy. The facility shall have a written policy on electronic medical records. The policy shall address persons authorized to make entries, confidentiality, monitoring of record

The breadth and diversity of the information contained in EHR and potential access by a variety of providers create real challenges for counsel involved in setting up the HIN. If some information must be retained for a longer time period than other information, will the HIN permit destruction of certain portions of information in the record? Certainly, the technical challenges in such selective record destruction are substantial; moreover, the HIN should decide whether the quality and usefulness of the record will be reduced if some information is missing. On the other hand, some HIN Participants may feel quite strongly that deleting records after the retention period passes are important to reduce risk of liability. The HIN structure or agreement thus must carefully consider how long the data contained in the system will be retained, who makes the decision of when and how information may be deleted, and how that deletion will be documented.

8-1(c). Medical Record Format Requirements

Some states still require a paper record, at least for some types of records, which greatly complicates the retention process for an EHR. For example, the California Code of Regulations assumes that records of patients in skilled nursing facilities are in paper format by requiring records to be "either typewritten or legibly written in ink, [and] capable of being photocopied."[191] Illinois regulations require that certain records be authenticated by a physician's signature (but are silent as to whether an electronic signature is adequate).[192] Paper format requirements would be a large hindrance to the development of interoperable EHRs; state legislature and agencies should be approached to amend these requirements.

---

entries, and preservation of information . . . (D) Preservation. The facility shall develop a plan to ensure access to medical records over the entire record retention period for that particular piece of information. . . (j) Each facility shall have a policy regarding the retirement and destruction of medical records. This policy shall specify the time frame for retiring a resident's medical record, and the method to be used for record destruction at the end of the record retention period. The facility's record retirement policy shall not conflict with the record retention requirements contained in Section 300.1840 of this Part." ILL. ADMIN. CODE tit. 77, § 300.1810(c)(5).

[191] CAL. CODE REGS. tit. 22, § 72543 (a).

[192] "All physician's orders, plans of treatment, Medicare or Medicaid certification, recertification statements, and similar documents shall have the authentication of the physician. The use of a physician's rubber stamp signature, with or without initials, is not acceptable." ILL. ADMIN. CODE tit. 77 § 300.1810 (d).

The Electronic Signatures in Global and National Commerce Act (E-SIGN),[193] may be of assistance in this area. E-SIGN restricts the extent to which states can require written signatures and paper records, by providing that a signature, contract, or other record relating to an interstate or foreign "transaction"[194] may not be denied legal effect, validity, or enforceability solely because it is in electronic form or because an electronic signature or electronic record was used in its formation.[195] E-SIGN thus validates electronic records and signatures in interstate or foreign transactions, and indeed clarifies that the E-SIGN exceptions do not include a governmental agency "with respect to a record other than a contract to which it is a party."[196]

However, E-SIGN is not an omnibus provision that preempts all state laws that require paper records and it would not appear to apply to purely intrastate transactions. E-SIGN does not limit or supersede "any requirement by a Federal regulatory agency, self-regulatory organization, or State regulatory agency that records be filed with such agency or organization in accordance with specified standards or formats."[197] In some circumstances, moreover, federal and state regulatory agencies are permitted to require retention of a record in a tangible printed or paper form if "there is a compelling governmental interest relating to law enforcement or national security," and imposing a paper record retention requirement "is essential to attaining such interest."[198] In addition, states may modify, limit, or supersede E-SIGN through a law that either (1) constitutes an enactment or adoption of the Uniform Electronic Transactions Act (UETA), as approved by the National Conference of Commissioners on Uniform State Laws in 1999, or (2) specifies alternative procedures or requirements for the use or acceptance of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts and other records where the alternative procedures and requirements are consistent with the substantive provisions of E-SIGN

---

[193] Pub. L. No. 106-229, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001-7006, 7021, 7031).
[194] E-SIGN defines a "transaction" as "an action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons . . ." 15 U.S.C. § 7006(13).
[195] 15 U.S.C. § 7001(a).
[196] 15 U.S.C. § 7001(b).
[197] 15 U.S.C. § 7004(a).
[198] 15 U.S.C. § 7004(b)(3)(B).

and do not give preferred status to specific technologies for electronic records or signatures.[199] While almost all the states have adopted the UETA, most have done so with amendments and variations to the "official" version. As a consequence, such laws are subject to E-SIGN preemption. What remains unclear at this point, however, and could create an obstacle to EHR interoperability, is whether states that have adopted a modified version of the UETA will find the entirety of their law preempted by E-SIGN, or only those provisions that are inconsistent with the "official" UETA. In either case, healthcare entities and their counsel must be aware of these preemption standards.

As a consequence, while E-SIGN largely preempts "quill pen" laws that require paper records and contracts and handwritten signatures,[200] transactions involving healthcare records will still need to comply with state law provisions affecting the validity and enforceability of contracts (e.g., offer, acceptance, consideration) as well as the substantive elements imposed by law (e.g., regarding the content and timing of any disclosure or other records required to be provided to a "consumer" under applicable law).[201] Likewise, notwithstanding E-SIGN's prohibition on denying the legal effectiveness of a signature, contract, or record solely because it is in electronic form, parties are obligated to retain and to be able to reproduce accurately records to those persons that are entitled to retain a written contract or other record of the transaction. If the electronic record is not in a form that can be retained and reproduced accordingly, E-SIGN permits the record's legal effect, validity, and enforceability to be denied.[202]

8-1(d). Medical Record Privacy Requirements

Of course, there are many state laws that limit the ability to use and disclose health information in more rigorous ways than the HIPAA Privacy Rule. (*See* Chapter 1.) In particular, laws that protect highly sensitive information, such as those regarding HIV/AIDS, mental health, substance abuse treatment, developmental disability, and

---

[199] 15 U.S.C. § 7002.
[200] *See* American Health Lawyers Association, Health Information and Technology Practice Guide, 3-7 (2003).
[201] 15 U.S.C. §§ 7001(b), 7001(c)(2)(A). E-SIGN defines a "consumer" as "an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." 15 U.S.C. § 7006(1).
[202] 15 U.S.C. § 7001(e).

genetic testing operate on the fundamental premise that the use and disclosure of this sensitive health information is prohibited unless specifically permitted by the law. Violations of such laws often subject the offender to criminal or civil sanctions or to disciplinary action by state licensing authorities.

Healthcare entities must grapple with the difficult decision of whether to include this sensitive health information in the EHR or whether such information should be excluded or segregated into an electronic "lock-box" that requires special access rights. On the one hand, including this sensitive information without adequate controls could subject the HIN Participants to substantial liability under state laws for inappropriate access. On the other hand, segregating this health information (and thus making it less accessible to care providers) may pose a risk to patients by depriving potential caregivers of complete information about the health of the patient. This will be an exceedingly challenging decision to make when setting up the HIN.

Also, in determining whether these state laws will apply to the HIN, counsel must determine whether federal law or regulations preempt these state laws, including the HIPAA regulations. The HIPAA regulations preempt "contrary" provisions of state law, with certain exceptions.[203] A state law is "contrary" if a covered entity would find it impossible to comply with both the state law and HIPAA, or if the state law is an obstacle to accomplishment of the full purposes and objectives of HIPAA.[204] Therefore, if the covered entity cannot comply with both state and federal requirements—the covered entity would actually violate one law by following another—the state law would be contrary to the HIPAA regulations.

Even where a state law is contrary to the HIPAA regulations, however, the state law would not be preempted in four circumstances: (1) The DHHS Secretary has determined that the state law is necessary to prevent fraud and abuse, to regulate insurance and health plans, or to report on healthcare delivery and other purposes, or that the state law regulates controlled substances; (2) the state law "relates to the privacy of individually identifiable health information and is more stringent than a

---

[203] 45 C.F.R. § 160.202.
[204] 45 C.F.R. § 160.202.

standard, requirement, or implementation specification adopted under subpart E of part 164 of this subchapter" [the Privacy Rule]; (3) the state law provides for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation or intervention; or (4) the state law requires certain health plan reporting.[205]

8-2. State Pharmacy Laws and Regulations

Pharmacy practice traditionally has been the subject of regulation by both the federal and state governments, and many pharmacies are subject to regulation by the Drug Enforcement Administration (DEA) regarding controlled substances and state pharmacy boards and licensure agencies regarding pharmacy practice. This dual regulation will continue to be a challenge as both federal and state governments issue requirements governing electronic pharmacy-related healthcare transactions.

Various federal agencies have proposed or adopted standards to facilitate electronic pharmacy-related transactions. For example, the DEA outlines several electronic commerce initiatives at http://www.deadiversion.usdoj.gov/ecomm, including a controlled substance ordering system and electronic prescriptions for controlled substances. The Food and Drug Administration (FDA) has regulations governing electronic records and electronic signatures at 21 C.F.R. part 11, which apply to electronic records created, modified, maintained, archived, retrieved, or transmitted submitted to the FDA under the Federal Food, Drug and Cosmetic Act and the Public Health Service Act.[206]

Most recently, the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA) includes, within the sections establishing the Voluntary Prescription Drug Benefit Program, the directive that Part D prescriptions and related information that are transmitted electronically comply with uniform electronic prescribing standards to be adopted by DHHS.[207] On February 4, 2005, CMS issued proposed standards for electronic prescription transactions and eligibility inquiries and responses for an

---

[205] 45 C.F.R. § 160.203.
[206] *See*, however, FDA's Guidance for Industry, Part 11, Electronic Records; Electronic Signatures–Scope and Application, issued August 2003, in which FDA outlines its current thinking on these topics in light of industry concerns and FDA's Current Government Manufacturing Practice initiative, *available at* http://www.fda.gov/cder/guidance/5667fnl.htm.
[207] 42 U.S.C. § 1395w-104(e)(1).

electronic prescription drug program,[208] and expects to have these standards in place as a final rule by January 2006.

The MMA provides that electronic prescribing standards promulgated as part of the Voluntary Prescription Drug Benefit Program supersede any contrary state law or regulation that pertains to electronic transmission of medication history and information on eligibility, benefits, and prescriptions with respect to covered Part D drugs,[209] so conflicting state pharmacy and licensure regulations should not pose a problem. Of course, determining whether state statutes or rules regulating electronic prescription formats, computerized recordkeeping or drug delivery systems, and other aspects of electronic transmission of prescriptions or orders,[210] fall outside of the express MMA preemption clause will pose a real challenge for lawyers advising clients about the interoperability of pharmacy-related aspects of EHRs.

8-3. State Licensure Laws

The value of an interoperable EHR is greatly increased to the extent that providers at different locations can simultaneously use, access, and update a record for the maximum benefit of a patient. Current technologies permit physicians even a considerable distance from a patient to take a primary role in the diagnosis of the patient's condition and direction of the plan of care. However, at least in the United States, such actions might run afoul of regulatory requirements, such as physician licensing statutes.

---

[208] 70 Fed. Reg. 6,256 (Feb.4, 2005).
[209] 42 U.S.C. § 1395w-104(e)(5).
[210] *See, e.g.,* Mich. Admin. Code r. 338.3162a (permitting pharmacists to dispense electronically transmitted prescription drug orders if the order includes certain information, including an electronic signature or other board-approved means of ensuring prescription validity); N.Y. Comp. Codes R. & Reg. tit. 8, § 63.6 (authorizing pharmacists to accept electronically transmitted prescriptions, subject to certain requirements including electronic encryption of the prescription); Ohio Administrative Code Chapters 4729-5 and 4729-17 (requiring electronic prescription transmission systems to be approved by the state Board of Pharmacy, and regulating prescription format, use of computerized recordkeeping systems, automated drug delivery systems, and institutional prescribing and dispensing as well as the Board's description of electronic prescription transmission system requirements), at http://pharmacy.ohio.gov/ElectronicRx-041006.htm; 22 Texas Admin. Code § 291.34 (prohibiting the dispensing by a pharmacist of electronic prescription drug orders for certain scheduled controlled substances if the electronic prescription drug order is issued by an out-of state practitioner unless the practitioner is also registered under the Texas Controlled Substances Act).

Most states permit out-of-state physicians to act as "consultants" and to assist in the care of patients under the primary care of a state-licensed physician.[211] However, the consultant ordinarily must be invited to participate in the care by a state-licensed physician, and the consultant's role (both in the nature and the number of contacts within the state) is severely limited.[212] In addition, many states prohibit the use of remote diagnostic technologies by persons other than physicians licensed in the state in which the patient is physically located,[213] and still others require a state-licensed physician to provide the primary interpretation for any diagnostic studies before allowing a remote physician access to such studies.[214] Such statutes will limit the utility of an interoperable EHR beyond the borders of the state of the patient's site of treatment, and might even prohibit providers in other jurisdictions from adding information of a diagnostic or therapeutic nature into such records, if those acts are considered the practice of medicine in violation of these state restrictions.

The Joint Commission for Accreditation of Health Care Organizations (JCAHO) accreditation standards exacerbate this problem. For the first time in 2001, the standards were revised to recognize the reality of remote diagnosis. Currently, JCAHO Standard MS.4.120 requires that "all licensed independent practitioners who are responsible for the patient's care, treatment, and services via telemedicine link are credentialed and privileged to do so at the originating site." Coordinating this requirement with the medical staff bylaws of most healthcare facilities will mean, as a practical matter, that physicians engaging in telemedicine activities must have a license to practice medicine in the state in which the patient is located. In addition, obtaining credentials at a healthcare facility might cause some state medical boards to conclude

---

[211] At last survey by the authors of this Chapter, forty-three states and the District of Columbia permit some form of consultation by physicians not licensed in the state. Only Kansas (by an act of its board of medical examiners), Illinois, Louisiana, Maine, New Mexico, Utah, Wyoming, and Puerto Rico do not permit some form of consultative exception to their medical licensure requirements.

[212] Most statutes use the term "infrequent," "occasional," "irregular," or "incidentally called" to describe a proper consultation. Many statutes prohibit "ongoing, regular, or contractual arrangements" that would permit frequent access to in-state patients. Some statutes prohibit the unlicensed physician from maintaining an office in the state to facilitate consultation.

[213] Currently Connecticut, Nevada, Oklahoma, and Texas do not permit remote diagnosis by any practitioner not licensed in their respective states.

[214] Georgia and Massachusetts have restrictions of this type.

that the out-of-state physician is engaged in the "ongoing" or "regular" practice of medicine contrary to the consultative exception of the physician licensure statutes, thus requiring the telemedicine practitioner to obtain a state license.

Finally, and perhaps most importantly, Medicare statutes and regulations, when read in conjunction with the various state consultative and telemedicine statutes, could in many jurisdictions prohibit the remote ordering and interpretation of tests. Medicare regulations provide that, in order for payment for outpatient diagnostic services to be appropriate, the services must have been provided by a provider who was at the time licensed to provide the service and must be certified as necessary by an authorized provider.[215] In order for a physician to be able to certify as necessary an item or service, the physician must be licensed in the jurisdiction in which the service is provided, because the act of certification of medical necessity is a "function or action" as contemplated by the definition of "physician service" and is deemed to take place where the service is rendered.[216]

The restrictions on the abilities of physicians to practice in the various states should not act as a bar to the development of an interoperable EHR. However, the considerable restrictions placed on physicians in their access to and treatment of patients in remote settings could limit substantially the utility of such records outside of state boundaries, and must be considered when granting providers the authority to access and enter data into such records.

8-4. Other State Law Concerns

Other state laws may also affect the development of a HIN or other agreement to implement an interoperable EHR. For example, counsel will need to examine the state law equivalents of many of the federal laws discussed in this Briefing: state health information security laws, antitrust laws, fraud and abuse or self-referral laws, and others. Counsel must be alert for the application of state laws that may impose greater restrictions on the development of the EHR than discussed in the federal law issues identified throughout this Briefing.

---

[215] 42 C.F.R. § 424.5(a).
[216] 42 U.S.C. § 1395x(r)(1).