Appendix C:
Relevant Legal Requirements for Health Data Exchange for Health Care Organizations

APPENDIX C: RELEVANT LEGAL REQUIREMENTS FOR HEALTH DATA EXCHANGE FOR HEALTH CARE ORGANIZATIONS[1]

1. INTRODUCTION

The following materials are intended to provide project participants with basic information about key legal issues affecting health information sharing. This is not intended to be a comprehensive, detailed, or authoritative review of these issues, but is intended to serve as a resource for a basic understanding of the issues, as a baseline for participants. While many participants will have considerable experience and education in these areas and may not need this reference, others may not be as experienced, or may not be experienced in all these areas. These materials are therefore not a substitute for other, more detailed resources or legal advice, but should provide a quick, useful reference when analyzing privacy and security issues.

The following materials will discuss both federal and state laws. For convenience, the first two sections discuss federal and state laws separately. The next section discusses legal issues relevant to electronic commerce (e-commerce) and electronic signatures, while the last section deals with issues usually subject to contracts, including intellectual property, risk allocation provisions (warranty and indemnification), and dispute resolution.

2. FEDERAL LAWS AFFECTING HEALTH INFORMATION SHARING

While state laws play an important role (see below), federal law tends to be the dominant legal influence on health information sharing. Most discussions of federal laws focus on those of general application, but some laws which apply directly only to federal agencies can have important secondary implications for other kinds of organizations.

2.1 The Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996, known as "HIPAA," is the most important federal legislation affecting health information sharing.

HIPAA was passed by Congress in 1996 principally to reform health care financing, but it also included a set of "administrative simplification" provisions directing the US Department of Health and Human Services (HHS) to publish a set of regulations setting standards for health care organizations conducting electronic claims transactions. While the main intent was to require health care organizations to conduct claims transactions using standardized formats and codes, HIPAA also required HHS to publish privacy and security regulations appropriate to the increased use of standardized electronic transactions involving sensitive

[1] John R. Christiansen, Christiansen IT Law.

personal information. "HIPAA," therefore, tends to be shorthand for the privacy, security, or other regulations issued by HHS under HIPAA.

The HIPAA regulations were developed and published by HHS through a process including publication of proposed drafts ("notices of proposed rule-making" or "NPRM"), a public comment period, and publication of a final, legally binding version. The regulations are codified in the Code of Federal Regulations (CFR) at 45 C.F.R. pts. 160, 162, and 164. Copies of the HIPAA regulations are available at the HHS website and the project portal.

2.1.1 Organizations Required to Comply with HIPAA (Covered Entities)

HIPAA is not a universal law, but applies only to health care organizations which engage in certain electronic claims transactions. This seemingly artificial restriction is a legal consequence of the limited results from the relatively limited congressional intent behind the law, to reform claims transactions practices. The result, however, is that the law reaches almost all health care organizations but has some anomalous results at its margins.

HIPAA applies to all health plans, since health plans necessarily engage in claims transactions and HIPAA requires that they do so electronically. It also applies to all health care clearinghouses, by definition because a health care clearinghouse is a claims transaction processor as well as a business associate of Covered Entities it engages in business with. HIPAA also applies to Medicare Part D plans. Finally, HIPAA applies to health care providers, but only if they engage in electronic claims transactions (either directly or indirectly, eg, by contracting with a claims processing vendor). Any corporation, limited liability company, partnership, professional services firm, sole proprietor, or individual which fits in any of these categories is called a "Covered Entity" and is required to comply with HIPAA.

It is possible to be a health care provider and not be a Covered Entity, as long as the provider does not submit claims or receive claims payments—or engage in any other HIPAA-regulated claims transaction, such as checking eligibility—electronically. The definition of "health care provider" under HIPAA is extremely broad, including not only hospitals, outpatient clinics, laboratories, and pharmacies as well as physicians, nurses, dentists, long-term care and other professionals, but any person or entity which is paid for providing health care-related services or products.

In practice, the vast majority of health care providers are probably Covered Entities, since they participate in health plans which require them to use electronic transactions directly or indirectly. Some "boutique" or other niche health care providers paid in cash or otherwise directly by patients may not be Covered Entities, however. It is also important to note that participation in other kinds of electronic transactions not regulated by HIPAA would not trigger HIPAA Covered Entity status coverage. For example, the transmission of clinical data

between providers for diagnostic purposes, such as the sending of digital radiology images for review alone, would not make the sender a Covered Entity.

2.1.1.1 Hybrid Entities

A "hybrid entity" is an organization that performs some functions which are defining characteristics of Covered Entities, and some functions which are not. For example, many grocery stores also include pharmacies, and pharmacies are Covered Entities. This could be interpreted to mean that any grocery store which includes a pharmacy is a Covered Entity and must comply with HIPAA in all its operations, even if the pharmacy is a very small component of the whole organization.

This kind of result goes beyond what HIPAA intended and is likely to produce impractical results for many organizations. The HIPAA regulations, therefore, permit organizations that perform both "covered functions"—functions which make it a Covered Entity—and noncovered functions, to designate "health care components" and comply with HIPAA as hybrid entities. When a hybrid entity has designated one or more health care components, including all covered functions, only that component or those components are required to comply with HIPAA.

In practice, this means that a hybrid entity's health care component or components must interact with other components of the hybrid entity as if they were separate organizations. Health care components must be governed by policies and procedures which prevent them from disclosing information protected by HIPAA (called "PHI"—see below) to noncovered components except under conditions in which a Covered Entity could disclose the information to another organization, and must otherwise comply with HIPAA as if they are independent legal entities.

2.1.1.2 Organized Health Care Arrangements

Health care services are often delivered in organizationally complex settings in which two or more Covered Entities act jointly to provide services to the same individuals. For example, physicians providing care in hospitals are frequently members of legally separate physician practices.

This could lead to a confusing and burdensome paperwork problem, since the HIPAA privacy regulations require Covered Entities (health plans and direct care providers) to provide a Notice of Privacy Practices (NPP) to the patients or beneficiaries they serve. In a complex setting, this could mean each individual would get a number of different NPPs, some from entities they might not even recognize.

In order to avoid this result, HIPAA permits Covered Entities to agree to publish a joint NPP, as long as they meet certain joint activity conditions and all participants comply with the NPP. Participation in an organized health care arrangement (OHCA) does not in itself affect

limitations on information use and disclosure among participants, however, and each participant is otherwise separately required to comply with HIPAA.

2.1.1.3 Affiliated Covered Entities

Another HIPAA concept intended to deal with the practical complexities of health care services and functions is that of the "affiliated covered entity" (ACE). In an ACE arrangement, different entities under "common ownership" or "common control" may agree to designate themselves as a single ACE. For ACE purposes "common ownership" means that an entity owns 5 percent or more of an affiliate, and "common control" means the power to directly or indirectly affect the actions or policies of another entity.

Two or more entities under common ownership or control may agree in writing to designate themselves an ACE, in which case the participants may comply with HIPAA as a single unit. However, within the ACE the participants must limit their use and disclosure of information among themselves consistently with their functions as health care providers, health plans, or health care clearinghouses.

2.1.1.4 Business Associates

One important result of the limited, transaction-oriented intent of HIPAA is the need to indirectly regulate parties which serve Covered Entities but are not themselves Covered Entities. This type of organization or individual is called a "Business Associate" (BA) under HIPAA.

As a practical matter, Covered Entities rely upon many entities which are not health plans, health care clearinghouses, or health care providers to provide services or functions involving protected health information (PHI), for a wide range of purposes. Information technology services vendors, lawyers, and quality improvement organizations, for example, may all have legitimate needs to see or use PHI on behalf of Covered Entity clients, but are not themselves subject to HIPAA. This circumstance raises a risk that once a Covered Entity has disclosed PHI to one of these unregulated entities, the information will no longer be subject to HIPAA's protections.

In order to avoid this result, HIPAA requires a Covered Entity to enter into specific contractual provisions—a "business associate contract" (BAC)—which require any entity obtaining PHI in order to provide services on behalf of the Covered Entity, to use the information subject to limitations consistent with HIPAA, and to implement safeguards for its protection.

This requirement is quite broad in its application. A BAC is required with any other entity which obtains or uses PHI to perform any services on behalf of a Covered Entity except providing treatment to an individual, unless the entity is an individual who is a member of the Covered Entity's "Workforce." A Covered Entity's Workforce includes all employees,

individual independent contractors, volunteers, students, and trainees who perform services under the direction of the Covered Entity.

A Covered Entity is generally not liable under HIPAA if its Business Associate violates its BAC, unless the Covered Entity knows of "a pattern of activity or practice" of the business associate which violates the BAC. If the Covered Entity does have such knowledge, it must take "reasonable steps" to cure the breach or end the violation; if these are unsuccessful, the Covered Entity must either terminate the BAC or, if that is not feasible for some reason, report the problem to HHS. This is true only if the Covered Entity properly executes BACs with entities the Covered Entity exchanges PHI with to conduct business on behalf of the Covered Entity. If a BAC is not executed in these cases, the BA may become the agent of the Covered Entity, with the Covered Entity liable for inappropriate actions taken by the BA.

2.1.2 Information Protected by HIPAA

Just as HIPAA can only regulate Covered Entities directly for jurisdictional reasons, there are jurisdictional limitations on the information HIPAA applies to. HIPAA-regulated information, called "PHI," is defined as:

Any information, in oral, hard-copy, or electronic form, which

- is "created or received" by or on behalf of a Covered Entity,
- identifies or can be used to identify any individual, or
- "relates to" the past, present, or future physical or mental health or condition of, provision of health care to, or payment for health care for the individual.

This is a very broad definition, which includes demographic information (name, address, age, etc) as well as clinical and payment-related information. However, due to HIPAA's jurisdictional limitations, the definition of PHI does not include information which otherwise would meet these criteria but is held by a Covered Entity in a role not related to health care or health care payment, such as disability or worker's compensation-related information. Note, however, that employee information created or received by any employer, Covered Entity or otherwise, in its role as a health plan is PHI and must be protected accordingly.

Information which cannot be identified to an individual is not PHI, but the Privacy Rule creates a strong presumption of the potential for identification. In order to be "de-identified," (1) information must not include any of 19 specified identifiers, ranging from name and address to vehicle identification numbers and website URLs, and cannot include any other data which might permit re-identification of the individual; or (2) an expert statistician or scientist must determine and document that there is only a "very small risk" of re-identifying the individual.

The Privacy Rule specifically applies to PHI in any medium: oral, hard-copy, or electronic. The Security Rule applies only to PHI in electronic form (often called "ePHI"). However, the

Privacy Rule includes a general standard comparable to (but much more general than) the Security Rule, which requires Covered Entities to implement administrative, physical, and technical safeguards to protect PHI in any medium. This is sometimes called the "little Security Rule" in the Privacy Rule and will be discussed more below.

2.1.3 Privacy Under HIPAA

Generally, "privacy" in the health care context refers to the concept that individuals have the right to know what information may be gathered about them and how it may be used and disclosed; to review and if necessary seek correction of errors in information about them; and to have some control over how information about them is used and disclosed. These principles, sometimes called the "Fair Information Practices Principles" or "FIPPs," are the foundation of the Privacy Rule.

As a practical matter it would be difficult if not sometimes impossible for health care organizations to implement privacy rights unconditionally. The Privacy Rule recognizes some of these practical difficulties, and therefore puts conditions on the exercise of many individual privacy rights and limits Covered Entity privacy obligations.

Covered Entities generally are required to implement procedures necessary to fulfill the rights specified in the Privacy Rule and to comply promptly with individual requests. Most activities required by the Privacy Rule must be documented and the documentation maintained for at least 6 years from the later of the date of creation or last effective date.

2.1.3.1 Notice of Privacy Practices (NPP)

All Covered Entities are required to publish a Notice of Privacy Practices, often abbreviated "NPP," to formally advise individual data subjects of their Privacy Rule rights. The contents of the NPP are specified in the Privacy Rule, with limited opportunity for variation, and must include

- a specific form of header;
- descriptions of the types of uses and disclosures the Covered Entity is permitted to make for purposes of treatment, payment, and health care operations;
- a description of each of the other purposes for which the Covered Entity is permitted or required to use or disclose PHI;
- a statement that any other type of use or disclosure will be made only with the individual's authorization;
- statements describing individual rights to view, copy, and request amendment of PHI, and obtain an accounting of disclosures of PHI (as discussed below);
- rights to request special confidential means of communication and to request privacy restrictions greater than what HIPAA requires;
- statements of the Covered Entity's legal obligations to comply with legal requirements to protect PHI, and to provide and comply with the NPP;

- a description of how the NPP may be revised;
- a statement of the individual's right to complain to the Covered Entity and HHS in case of a violation of his or her privacy rights, and description of the Covered Entity's complaint filing procedures;
- identification of the Covered Entity's contact person for purposes of the NPP; and
- an effective date.

Health plans must provide individuals with the NPP within 60 days of their enrollment, and every 3 years thereafter provide notice of the availability of the NPP and how to obtain a copy. Health care providers must provide their NPP on the first date of service to an individual, except where that is impractical due to an emergency, and make a good faith effort to obtain the individual's acknowledgment of receipt. Health care providers maintaining physical service delivery sites (eg, hospitals and clinics) must post the notice there prominently and make copies available. Any Covered Entity which maintains a website for customers must post its NPP there.

2.1.3.2 Individual Data Subjects' Information Rights

Under the Privacy Rule, individual data subjects are required to be provided with the following rights:

- the right to view and copy PHI about them,
- the right to request amendment of PHI about them,
- the right to request restrictions on PHI use and disclosure in addition to those required by the Privacy Rule (as discussed below),
- the right to an accounting of all disclosures of PHI about them, and
- the right to receive confidential communications at an alternative address or other method of contact.

Covered Entities may establish reasonable procedures for individuals to exercise these rights, such as requiring that requests be in writing. They may also charge a reasonable fee for copies of records, but not for the exercise of other rights.

The PHI required to be subject to individual privacy rights of access and amendment is that contained in "designated record sets," which generally is any set of information or documentation used in connection with decisions with respect to the individual; informal or sporadic records such as telephone messages confirming appointments which are not included in a patient's files, for example, would ordinarily not be included.

a. Minors' Privacy Rights. The age at which an individual is entitled to exercise privacy rights on his or her own behalf is determined as a matter of state law. While this is usually the age of 18, younger individuals may be entitled to exercise their own privacy rights where they are legally emancipated, or with respect to PHI regarding health care for which they otherwise have a legal right to make their own decisions. This may be the case in

particular with respect to decisions about mental health and substance abuse care, abortion and contraception, and sexually transmitted diseases (STDs).

b. Exercise of Rights by Guardians and Personal Representatives. The legal guardian for an individual who has been adjudicated incompetent has the right to exercise that individual's privacy rights, as does a person whom an individual has legally designated his personal representative with power to make health care decisions.

c. Limitations on Access Rights. Individual rights to view and copy PHI do not apply to the following:

- Psychotherapy notes, defined as notes in any medium made by a mental health professional documenting or analyzing the contents of conversations during any private, group, or joint counseling session, as long as the notes are kept separate from the medical record;
- Information compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action or proceeding;
- Information maintained by a laboratory which is subject to the federal Clinical Laboratory Research Amendments (CLIA) or a state law equivalent;
- Information about an inmate of a correctional institution, if providing the information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or any other inmate or the safety of any other person at the facility;
- Information obtained or created by a health care provider in the course of research, while the research is in progress, as long as the individual has been informed or and agreed to limit his or her access;
- Information contained in federal governmental and contractor records subject to the federal Privacy Act, to the extent access may be denied under that law; and
- Information obtained from a third party under a promise of confidentiality, if the grant of access would be reasonably likely to reveal the information source.

Access can also be denied if a licensed health care provider has determined, in the exercise of professional judgment, that granting access would be reasonably likely to endanger the life or physical safety of the individual or another person or, if the information refers to another person, access would be reasonably likely to cause substantial harm to the other person. In such a case, however, the individual may request that a different licensed health care professional, who did not participate in the original decision denying access, review that decision.

d. Conditions for PHI Amendment. Individuals do not have an absolute right to have PHI about them amended, but they may request it. Such a request may be denied, in whole or in part, to the extent that:

- the information was not created by the Covered Entity, unless there is a reasonable basis to believe that the originator of the PHI is no longer available to act on the request;
- the information is not part of a designated record set;

- access to the record could be denied, under one of the limitations discussed above; or
- the information is accurate and complete.

If the Covered Entity accepts the request, it must advise the individual, amend the information appropriately, and make reasonable efforts to communicate the amendment to any persons the individual identifies as needing the amended information and any person who may rely on the unamended information to the detriment of the individual. Any Covered Entity receiving notification of another Covered Entity's amendment must amend any affected PHI in its own designated record sets.

If the Covered Entity denies the request, it must provide a written statement identifying the reason for the denial and describing the individual's right to file a statement disagreeing with the denial. If a statement of disagreement is filed, the Covered Entity must attach or link it to the disputed portion of the record and may file a rebuttal statement. A copy of any statement of disagreement must be included in any subsequent disclosure of the information; if the individual does not file a statement of disagreement, he or she may request that copies or summaries of any denied requests and the reasons for denial be included in subsequent disclosures.

e. Right to Request Additional Restrictions. Covered Entities must allow individuals to request additional restrictions on PHI use and disclosures for treatment, payment, and health care operations; to family members, other relatives, and close personal friends of the individual who are involved in the individual's health care; and for disaster relief. Covered Entities are not required to agree to such restrictions, however. If the Covered Entity agrees to a restriction it must comply with it, unless the restricted PHI is needed to treat the individual in an emergency.

An agreed restriction may be terminated upon the individual's request or with his or her consent, or by the Covered Entity by notice to the individual. The termination of a restriction is only effective as to information created or received by the Covered Entity after it has notified the individual of the termination.

f. Accounting of Disclosures. Individuals have the right to an accounting of disclosures of PHI about them for the 6-year period preceding the request, for disclosures other than those made

- for purposes of treatment, payment, or health care operations;
- to the subject individual;
- incidental to a permitted use or disclosure;
- pursuant to an individual's written authorization;
- in a health care facility's directory or to persons involved in the individual's care or for other permitted notification purposes;

- for national security or intelligence purposes;
- about an inmate, to correctional institution or law enforcement officers;
- as part of a limited data set, for research or public health purposes; or
- before the date on which the Covered Entity was required to comply with the Privacy Rule.

A Covered Entity is also required to temporarily suspend an individual's right to an accounting of disclosures to health oversight agencies or law enforcement officials upon a written or oral statement by the agency or official that the accounting would be reasonably likely to impede the agency's activities, and specifying the period of time during which the suspension is required.

An accounting of disclosures must include

- the date of the disclosure;
- the name of the person or entity who received the PHI, and address if known;
- a brief description of the PHI disclosed; and
- a brief description of the reason for the disclosure or copy of the written request for the disclosure, if applicable.

If multiple disclosures for the same purpose to the same person or entity have been made the accounting may identify the period during which they were made and their frequency. Disclosures made for research on 50 or more individuals may use a summary of the research and identify the researcher and research sponsor.

g. Confidential Communications. Covered Entities must allow individuals to request confidential communications of PHI by alternative means and/or to alternative contact addresses. Health care providers must accommodate such requests and may not require an explanation, but may require information about how payments will be handled, if applicable. Health plans must accommodate such requests if the individual states that the disclosure of the PHI could endanger him or her and, if applicable, upon information about how payment will be handled.

2.1.3.3 Information Use and Disclosure Rules

PHI uses and disclosures by Covered Entities must either be for a purpose authorized by a provision of the Privacy Rule or authorized in writing by the subject individual. Any use or disclosure which does not fall into an authorized category is prohibited.

With two exceptions the Privacy Rule does not require any specific uses or disclosures of PHI. The only exceptions are for disclosures to the subject individual in the exercise of his or her privacy rights, as discussed above, and to HHS for purposes of investigating the Covered Entity's HIPAA compliance. Other federal and state laws may require other types of use or disclosure, and these are generally accommodated by the Privacy Rule.

a. Authorizations. If an authorization from the individual is used, it must be in writing, describing the information to be disclosed and the purposes of the disclosure, and identifying the party authorized to disclose the information, the person or class of persons to whom the disclosure may be made. The authorization must include an expiration date or event, and be dated and signed by the individual. It must also include statements specifying the individual's right to revoke the authorization. An authorization may not be a condition to the provision of treatment unless the treatment is research-related and the authorization is for purposes of the research, nor may it be a condition to health plan enrollment or benefits unless sought for pre-enrollment determinations related to the individual, underwriting, or risk rating.

b. Limited Data Sets. Because there are some legitimate activities which cannot be performed using de-identified information but do not really require very detailed PHI and so pose relatively lower risks, the Privacy Rule allows for the use of "limited data sets" for purposes of health care operations, public health reporting, and research. A limited data set, like de-identified information, is based on the exclusion of identifiers such as names and addresses. However, it does allow for more specific demographic information than is permitted for de-identified information.

The content of a limited data set is still considered PHI. The recipient of a limited data set must first enter into a "data use agreement" which, like a business associate contract, establishes the permitted uses and disclosures for the limited data set and requires the recipient to protect it against unauthorized use or disclosure.

c. "*Minimum Necessary*" Rule. Almost all nontreatment uses and disclosures of PHI are subject to the "*minimum necessary*" rule. Covered Entities are required to comply with the *minimum necessary* rule whenever they use, disclose, or request PHI. The only exceptions are for

- disclosures to or requests by health care providers for treatment purposes;
- disclosures to the individual who is the subject of the information as required or permitted under the Privacy Rule;
- uses or disclosures authorized by the individual, to the extent authorized by the individual;
- uses or disclosures to HHS for HIPAA compliance investigative purposes;
- uses or disclosures required by law; and
- uses and disclosures required to comply with HIPAA.

In implementing the *minimum necessary* rule, Covered Entities are required to (i) identify those persons or classes of persons in their Workforce who need access to PHI to carry out their duties, and (ii) specify the PHI to which each such person or class may have access and any conditions to that access.

For recurring requests for or disclosures of PHI, Covered Entities are required to implement policies and procedures limiting the PHI to that "reasonably necessary" to achieve the purpose of the disclosure. For nonrecurring requests or disclosures, Covered Entities must develop criteria designed to limit the PHI disclosed to that "reasonably necessary" given the purposes of the disclosure, and a process for reviewing requests for such disclosures.

Covered Entities may generally rely upon requests made by public officials, other Covered Entities, and professionals providing services to the Covered Entity as establishing the *minimum necessary* PHI to be disclosed, unless such reliance is not "reasonable under the circumstances."

An individual's "entire medical record" may not be requested, used, or disclosed unless the entire medical record is specifically justified as the *minimum necessary* for purposes of the request, use, or disclosure.

d. Proof of Identity and Authority to Request or Receive Disclosures. Covered Entities are required to verify the identity and authority of persons requesting PHI for almost all disclosures. In most cases the Covered Entity is entitled to rely on documents, statements, or representations from the requestor which reasonably indicate appropriate identity and authority on their face, in the exercise of good judgment. Public officials making requests are required to provide agency identification badges or other official credentials, letterhead or other evidence of identity and authority, and written documentation providing evidence of the legal basis for the request.

e. Treatment. Health care "treatment" is broadly defined to include not only the provision of "health care and related services" by one or more health care providers, but also the coordination and management of such care, consultation about care between providers, and referrals for care.

f. Payment. "Payment" is also very broadly defined, to include not only activities directly involving the reimbursement of health care providers for treatment but also obtaining health insurance premium payments; coverage and benefits determinations; enrollee risk adjustment; billings, claims management, and collection activities; review of services for medical necessity, appropriateness of care, and justification of charges; utilization review, including certification, authorization, and review of services; and collection-related activities.

g. Health Care Operations. "Health care operations" is a broad set of activities related to administration and management of health care payment and treatment activities, including the following:

- quality assessment and improvement; outcomes evaluation and clinical guidelines development not principally intended to provide "generalizable knowledge" (ie, not principally intended for general research purposes); population-based health improvement and cost reduction activities; case management and care coordination; and contacting providers and patients with information about treatment alternatives

- health care professional competence, qualifications, and performance review and evaluation; health plan performance; and health care practitioner, student, and trainee training, accreditation, licensing, and credentialing
- health insurance underwriting, premium rating, and other activities related to health benefits contracting
- medical review, legal services, and auditing functions including fraud and abuse detection and compliance
- business planning and development, including cost-management and planning-related analyses
- Covered Entity business management and administration including HIPAA-related activities; customer service support; resolution of internal grievances; the sale, transfer, merger, or consolidation of the Covered Entity with another entity and related due diligence; creation of de-identified data and limited data sets; and fund-raising for the Covered Entity's own benefit, so long as this is disclosed in the NPP and individuals can opt-out.

Limited data sets may be used for health care operations purposes, subject to data use agreements.

h. Family and Friends. As discussed above, Covered Entities are required to give individuals access to PHI about them under most circumstances. Covered Entities may also disclose PHI about individuals to their family members and other close relatives or friends involved in their care or payment for care, if the circumstances indicate this is reasonable (eg, they are present during care or consultation, or the health care provider in the exercise of professional judgment determines it is appropriate), or to notify them of the individual's location, general condition, or death.

i. Public Health. Covered Entities may disclose PHI to public health authorities authorized by law to collect information for purposes of disease, injury, or disability prevention and control. This includes vital statistics reporting, public health surveillance and investigations, public health intervention, and child abuse or neglect reporting. Covered Entities may also disclose PHI to the federal Food and Drug Administration (FDA) for reporting on quality, safety, or effectiveness of FDA-regulated products or activities and to employers about individual employees for certain workplace-related medical surveillance and investigation.

Public health authorities are not always governmental agencies; in some cases, public health activities may be privatized or outsourced. In some but not all cases, public health reporting may be required by federal or state law. Covered Entities are permitted to disclose limited data sets for public health purposes, subject to entry into a data use agreement.

j. Regulatory and Licensing Agencies. Covered Entities are permitted to disclose PHI to regulatory agencies for health oversight activities authorized by law, such as audits, investigations, inspection, licensure or disciplinary actions, legal proceedings and other activities necessary for oversight of the health care system, government benefits programs, and other regulatory programs for which health information is necessary to determine

compliance. In some but not all cases, such disclosures may be required by federal or state law; for example, Covered Entities are required to make all relevant records available to HHS for purposes of investigating their HIPAA compliance.

k. Law Enforcement and Related Agencies. Generally, a Covered Entity may disclose PHI for law enforcement purposes and related purposes without the individual's authorization or a court order or other judicial process only

- to law enforcement agencies when required by law, as with certain types of wounds or physical injuries;
- to law enforcement or appropriate social or health services agencies where the Covered Entity reasonably believes the data subject is the victim of abuse, neglect or domestic, if such a report is required or expressly authorized by law;
- upon request to a law enforcement official for purposes of identification and location of a suspect, fugitive, material witness, or missing person, provided that the information is limited to a specified set of identifying characteristics;
- to a law enforcement official about a suspected victim of a crime, if the suspected victim is incapacitated or emergency circumstances preclude him or her from agreeing to the disclosure, as long as (i) the official represents the information is needed to determine whether a person other than the victim has committed a crime and that the information will not be used against the victim, (ii) the law enforcement official represents that immediate law enforcement that depends upon the disclosure would be adversely affected by waiting, and (iii) the Covered Entity determines that the disclosure would be in the best interests of the victim, in the exercise of professional judgment;
- about a decedent to a law enforcement official if appropriate to alert law enforcement about a suspicion the death was due to criminal conduct;
- to a law enforcement official in case of emergency, if it appears necessary to alert law enforcement to the commission, nature, location, and victims of a crime and the identity, description, and location of the perpetrator;
- to law enforcement authorities to identify or apprehend an individual who has admitted participation in a violent crime which may have caused serious physical harm or who may be an escapee from law enforcement custody; or
- "consistent with applicable law and standards of ethical conduct," if the Covered Entity has a good faith belief that the use or disclosure is necessary to prevent or lessen a "serious and imminent threat to the health or safety of a person or the public," to a person or persons reasonably able to prevent or lessen the threat.

Covered Entities may also disclose PHI about inmates in law enforcement custody or correctional institutions to appropriate officials for a variety of purposes, not limited to the provision of care to the individual.

l. Judicial and Administrative Proceedings. PHI may be disclosed for purposes of judicial or administrative proceedings upon receipt of an administrative tribunal order specifying the PHI to be disclosed. A subpoena, discovery request, or other legal process for disclosure of PHI which is not accompanied by such an order is not sufficient to permit the

disclosure of PHI unless the requesting party certifies specific attempts to contact the subject individual(s) to allow them to intervene and protect the information, or a protective order meeting the requirements of the rule has been obtained.

m. Other Governmental Functions. The Privacy Rule permits Covered Entities to disclose or use PHI of Armed Forces and foreign military personnel as deemed necessary by the appropriate military authorities and may disclose PHI for purposes of national security-related intelligence and federal official protection to authorized federal officials.

n. Research. For purposes of HIPAA, "research" is defined as a systematic investigation designed to develop or contribute to generalizable knowledge. Given the breadth of this definition, there may be questions whether some activities overlap with activities characterized as "health care operations." Because the rules applicable to the two categories are significantly different, such borderline cases need careful analysis.

PHI may be reviewed in the custody of a Covered Entity in order to prepare research protocols, and limited data sets may be used for research purposes subject to data use agreements (see above). Otherwise, PHI may be used or disclosed for research purposes without individual authorization only with a waiver and subject to any conditions established by a qualified institutional review board (IRB) or qualified privacy board.

2.1.4 Security Under HIPAA

From the legal perspective, information security—under HIPAA and otherwise—is an issue of organizational governance, and risk assessment and management. While it is essential to implement appropriate technological solutions for security problems, technology is only one element of information security. Technological solutions, as well as administrative policies and procedures and physical security solutions, must be integrated (or at least coordinated) in a risk-based security strategy under accountable organizational oversight.

2.1.4.1 Relationship between the Privacy and Security Rules

As noted above, the Security Rule applies only to PHI in electronic form, or ePHI, while the Privacy Rule includes a "little Security Rule" standard which applies to PHI in any medium. The "little Security Rule" is much more general than the Security Rule, but should be analyzed according to the same risk-based principles which apply under the Security Rule.

Both the Security Rule and the "little Security Rule" require Covered Entities to implement "administrative, physical, and technical safeguards" to protect PHI. Neither provides detailed specifications for these safeguards. The "little Security Rule" provides no detail at all, but simply requires that the Covered Entity "reasonably safeguard" PHI with safeguards which are "appropriate." The Security Rule specifies 43 categories of safeguards which must be implemented (or at least considered—see below). Within each category, the Security Rule

requires that the safeguards implemented be "reasonable and appropriate"[2] to ensure compliance. Note that HHS said it believes Congress set an "exceptionally high goal" for the protection of ePHI.

Both also require Covered Entities to protect PHI against any uses or disclosures not permitted under the Privacy Rule. This necessarily implies that a Covered Entity's safeguards must be consistent with and enforce its Privacy Rule-based policies and procedures, including but not limited to its *minimum necessary* policies.

2.1.4.2 Safeguard Policies and Procedures

Both the Security Rule and the "little Security Rule" require the implementation of "administrative, physical, and technical safeguards" for the protection of PHI and, in the Security Rule, also for the protection of the Covered Entity's information systems. The term "safeguard" is not defined under HIPAA, but generally refers to any measure intended to reduce the risk of a harmful or prohibited event, such as the use or disclosure of PHI contrary to Covered Entity policy and HIPAA's requirements.

It is important to note that most safeguards are organizational policies and procedures, not technical implementations such as software and hardware. Both the Security Rule and the Privacy Rule (and therefore its "little Security Rule") require Covered Entities to publish their policies and procedures in written or electronic form, make them readily available, and archive them for possible HHS review for 6 years from their last effective date.

2.1.4.3 Safeguard Categories

Security Rule safeguards are categorized as administrative, physical, or technical, as follows:

- Administrative safeguards are organizational decision-making processes (ie, risk analysis and risk management) and security oversight requirements, as well as security-related personnel and information system management. Administrative safeguards also include security-oriented provisions required in Business Associates Contracts.
- Physical safeguards are policies and procedures for facility, workstation, device, and media management.
- Technical safeguards involve the implementation of reasonable and appropriate technology solutions for information system access control and data storage and transmission. While the implementation may depend on software, the Covered Entity must establish the implementation requirements by written policies and procedures.

[2] While the phrasing of the two is not identical, the use of the terms "reasonable" and "appropriate" in both the Security Rule and the "little Security Rule" appear to indicate the two should be interpreted consistently.

2.1.4.4 Safeguard Selection Criteria

The Security Rule is based on two fundamental assumptions: that Covered Entities need a great deal of flexibility in establishing safeguards, given the great diversity of the entities regulated by the rule; and that while it is not possible to eliminate all risks to ePHI and information systems, Covered Entities must protect against "reasonably anticipated" threats and potential HIPAA violations. Given these assumptions, the Security Rule allows Covered Entities to take a "flexible approach" to safeguard selection, and in some cases to implement alternative types of safeguards.

Safeguards under the Security Rule are categorized by regulatory "standard." Most but not all standards are supplemented by "implementation specifications." Each safeguard standard identifies a type of protective measure, with specific compliance obligations listed in its accompanying implementation specifications. Standards which are not accompanied by specifications are considered sufficiently clear for compliance purposes without such elaboration. Covered Entities must comply with all standards included in the Security Rule.

Safeguards are selected based on a "flexible approach," under which Covered Entities take into account their size, complexity, and general capabilities; technical infrastructure, hardware, and software capabilities; the costs of security measures; and the probability and criticality of risks to ePHI. Further, specifications are categorized as either "required" or addressable," and all standards not accompanied by specifications are "required." As the term indicates, Covered Entities must implement the safeguards identified in "required" standards and safeguards.

The safeguards identified in "addressable" specifications are not optional but must be implemented unless the Covered Entity has conducted an analysis which demonstrates that it is not a "reasonable and appropriate" safeguard in the specific environment or circumstances for which it is considered and has implemented an equivalent alternative security measure if "reasonable and appropriate." Any decision not to implement an addressable specification must be documented by the Covered Entity.

2.1.4.5 Risk Analysis, Risk Management, and Safeguard Selection

The foundation of Security Rule compliance, and the basis for safeguard selection, is a risk analysis and risk management process. Risk analysis is required to be an "accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of" ePHI held by the Covered Entity, as well as its information systems used with ePHI. Risk management is then the implementation of "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level." Both risk analysis and risk management are required implementation specifications.

Risk analysis is therefore the source for information about "reasonably anticipated threats" and the probability and criticality of risks to ePHI, which are principal factors in safeguard

selection. The safeguards themselves are implemented as part of the risk management process, based on the "flexible approach" factors, and, where appropriate, an "addressable specifications" analysis.

2.1.5 Transactions and Code Sets Requirements

The legal core of HIPAA is its transaction requirements, even though these often seem overwhelmed by the privacy and security obligations. The fundamental transactions requirement is that all health plans must implement electronic transactions using standard formats and codes for the transactions covered by HIPAA and must accept for processing any claim which uses these standard formats and codes. Health care providers are not required under HIPAA to engage in any of the regulated transactions electronically, but if they do—whether directly or indirectly, as through a services provider—they also must use the standard formats and codes.

The HIPAA legislation specified a basic set of 9 "administrative and financial" transactions to be regulated, and granted HHS the authority to adopt standards for other transactions if appropriate, which it has done for one additional transaction to date. Transaction format and code set standards are adopted by regulation from industry standards developed by recognized standards-setting bodies.

None of the transactions standards adopted to date directly affect clinical content, though there is a claims attachment standard in development which may have indirect implications, since it may be desirable to extract claims attachment data directly from electronic clinical records. HIPAA does not otherwise have direct implications for electronic health or medical records but may serve as precedent for a regulatory approach to mandated clinical data standards (and vice versa).

2.1.5.1 Unique Health Identifiers

In order to enable electronic transactions, HIPAA requires HHS to establish standard, "unique health identifiers" for all individuals, employers, health plans, and health care providers.

- The individual identifier proved politically controversial when HHS issued the NPRM, and Congress discontinued funding for further development of this identifier. The unique individual identifier will therefore likely not be issued. Alternative approaches to individual identifiers are discussed in AHIMA Practice Brief, Using the SSN as Patient Identifier (March 2, 2006); AHIMA Practice Brief, Surveying the RHIO Landscape, with a Focus on Patient Identification (January 2, 2006); and Connecting for Health Common Framework, Correctly Matching Patients with Their Records (2006).
- The employer unique identifier is the employer identification number (EIN) used for federal tax purposes. This standard is in effect.

- The health plan identifier standard has not been published in proposed or final form. An NPRM is anticipated in the latter part of 2006 or the beginning of 2007 per the Centers for Medicare & Medicaid Services (CMS).
- The national provider identifier (NPI) standard for the health care provider unique identifier has been published and is effective. The NPI is a 10-digit numerical code, assigned by HHS through the National Provider System (NPS). Each organizational provider and individual health care provider which is a Covered Entity is required to obtain its NPI no later than May 23, 2007. Health care providers which are not Covered Entities are permitted to obtain an NPI at their discretion.

2.1.6 Electronic Signatures Under HIPAA

HIPAA requires HHS to establish a standard for electronic signatures, and a proposed standard was published in the 1998 Security Rule NPRM. The proposed standard would not have required Covered Entities to implement electronic signatures, but provided that any Covered Entity which did so would have to implement digital signatures based on a public key infrastructure (PKI) (see the discussion of Electronic Signatures, below).

In 2000, however, the federal Electronic Signatures in Global and National Commerce Act (E-SIGN) went into effect, which preempted most federal and state laws limiting or imposing conditions on electronic signatures. While HHS does have some authority to issue an electronic signature standard for some purposes under E-SIGN, there is currently no development activity for a final HIPAA standard in this area.

2.1.7 HIPAA Documentation Requirements

HIPAA requires Covered Entities to publish their NPPs in writing and electronically (only if the Covered Entity maintains a website) and to publish written policies for their compliance with the Privacy and Security Rules in writing or electronically, or both. They must also maintain documentation pertinent to individuals' exercise of their rights of access, etc, and the HIPAA Security Rule requires written documentation of risk assessments and decisions about safeguards selection.

Any written documentation required by HIPAA must be retained for at least 6 years from the later of the date of publication or the last effective date (eg, in the case of an NPP or a compliance policy). It is possible that in some cases state or other federal laws or contractual provisions will require a different retention period. In such a situation the longer period probably applies.

2.1.8 HIPAA Penalties

Violations of HIPAA may be subject to either civil (regulatory) or criminal penalties. Any incident or event which is punishable as a crime may not be the subject of civil penalties. Civil penalties are under the jurisdiction of HHS, which generally investigates potential violations in response to a complaint but also has the authority to review compliance at its

discretion. Criminal penalties are investigated and prosecuted by the US Department of Justice.

Civil penalties are assessed per violation; a violation is the performance of some act which is prohibited under HIPAA, or a failure to perform some act which is required. Any given incident or event may be a violation of one or more HIPAA requirements. Some violations may be "continuing," where a single act (or failure to act) goes on for a period of time; continuing violations are deemed to occur on each day they go on. For example, a failure to publish an NPP for a month is a continuing violation, with a penalty assessable for each day of the month.

Civil penalties are assessed at up to $100 per violation, to a calendar year maximum of $25,000 per type of violation. Civil penalty investigative proceedings are intended to be relatively informal and if the Covered Entity is cooperative and acts in good faith civil penalties may be avoided, waived, or reduced. If civil violations cannot be resolved informally HHS may pursue penalties in an adversarial administrative adjudication process generally following the administrative proceedings guidelines issued by the Office of the Inspector General.

Criminal penalties may be imposed on a Covered Entity which knowingly obtains or uses PHI for a purpose not permitted under HIPAA, or knowingly obtains PHI by using a false identifier. Criminal penalties range from 1 year in prison and a $10,000 fine per violation, up to 10 years in prison and a $250,000 fine per violation committed for profit or with malicious intent.

2.2 Federal Privacy Act

The federal Privacy Act applies directly only to federal agencies. It requires agencies to keep records (including personal information) protected against intentional or unauthorized disclosures which may result in "substantial harm, embarrassment, inconvenience, or unfairness" to any individual who is the subject of the information. Information protected under this requirement would include but go beyond the information protected by HIPAA (see below).

While the Privacy Act applies directly only to federal agencies, in order to ensure its protections are not avoided, these agencies are required to apply it indirectly to their contractors who obtain or use protected information on their behalf. For example, CMS, which administers payment under Medicare, Medicaid, and other federal health insurance programs, generally requires its contract "intermediary" health plans and contracted providers to comply with CMS security policies.

Federal agencies are required to implement "appropriate administrative, technical, and physical safeguards" to ensure the security and integrity of Privacy Act-protected records,

and frequently pass this obligation on to their contractors. Privacy Act information security safeguards, like HIPAA security safeguards (see below), are risk-based and do not generally prescribe specific implementation requirements.

2.3 Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) also applies only to federal agencies. FISMA, enacted in 2002, requires all federal agencies to develop, implement, and document an information security program for all protected information and information systems under their control.

2.4 National Institute of Standards and Technology

The National Institute of Standards and Technology (NIST), a unit of the US Department of Commerce, provides information security guidance for federal agencies which is often influential for other parties. The Federal Information Processing Standards (FIPS) published by NIST are binding on federal agencies, and generally address specific technical issues such as minimum encryption requirements.

The NIST Security Guidelines, sometimes called the "800 Series" for their numerical identification, are not binding but are persuasive guidance covering not only technical but administrative security issues. This series includes a specific publication on HIPAA security compliance, "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule" (SP-800-66, March 2005). A copy of this publication, and certain other useful NIST publications, is available from the NIST website (http://www.nist.gov).

2.5 Department of Defense Standards

The US Department of Defense (DoD) is a major health benefits payor with particularly high security sensitivities, since many of its beneficiaries are or have been active-duty military personnel. Accordingly, DoD requires its health care-related contractors to evaluate ("certify") the security of their information systems and obtain a formal DoD declaration ("accreditation") approving their use, under the Defense Information System Certification and Accreditation Process (DITSCAP).

Because of DoD's special sensitivities, DITSCAP and other DoD-developed information security standards are not usually applied in other environments. However, the difference in applicable standards may affect information sharing with DoD and its health care-related contractors.

2.6 Drug Enforcement Administration Electronic Signatures

The principal federal electronic signatures law is E-SIGN, enacted in 2000. E-SIGN, as more fully discussed below, was intended to lower barriers to electronic commerce (e-commerce)

by preempting federal and state laws which prohibited or limited the use of electronic signatures. However, E-SIGN does provide that a federal agency may impose limitations and requirements on electronic signatures if there is a "substantial justification" for the distinction.

The Drug Enforcement Administration (DEA), the federal agency charged with regulating controlled substances, has determined that it has a substantial justification for imposing specific electronic signature requirements for transactions involving Schedule I and II drug orders—ie, prescriptions and other orders for the procurement of drugs with a high potential for abuse. In particular, DEA has issued regulations requiring that any electronic signature used for such a transaction be a digital signature issued through a public key infrastructure (PKI), administered by a DEA certification authority (CA).

3. STATE LAWS

While state laws pertaining to health information data sharing, privacy, and security generally tend to follow similar principles, details and terminology frequently differ. Determining how to resolve conflicts between different state laws is therefore often problematic.

As a general rule each state has the authority (jurisdiction) to regulate the activities of any organization which "does business" in the state. "Doing business" is a broad constitutional law concept, which may be roughly summarized as intentionally engaging in any activity which reaches into the state and affects individuals or entities there. For example, for electronic transactions purposes, an e-mail to an individual in a state asking her to reply with some information would probably be considered "doing business" in that state. Conversely, maintaining a website which can be viewed by individuals in a state but which does not request information from individuals in that state probably is not "doing business" in that state.

If a state has jurisdiction over an organization because it is "doing business" there, the state can apply its laws to activities affecting residents of its state (both individual residents and organizations organized under the state's laws). This means that an organization which actively transfers information across state lines is probably subject to the laws of both states.

3.1 State Privacy and Security Laws

While HIPAA provides a health care privacy and security legal framework which applies uniformly throughout the United States, each state and territory also has its own laws with implications for health information sharing. These laws are sometimes said to provide a "patchwork" of privacy protections, since they are by no means uniform and do not have

consistent requirements. Many states (but not all) have been revising their laws to make them consistent with HIPAA, and the revisions themselves are not uniform.

State and territorial laws relevant to health information may be found in constitutions, which may provide rights of privacy; in statutes ranging from detailed codes of health information law to vague statements of confidentiality principles; in regulations applicable to specific sectors such as health care, or types of organization such as hospitals; and in published administrative and court cases establishing common law principles and requirements. Any given state or territory may have laws applicable to health information at any or all of these levels.

3.1.1 Relationship between HIPAA and State Laws

HIPAA generally supersedes state and territorial laws which apply to electronic health claims transactions and the use of electronic health records, and are "contrary" to HIPAA, unless (a) the law "addresses controlled substances"; or (b) HHS has determined that the state or territorial law is necessary to prevent fraud and abuse, ensure appropriate state regulation of insurance and health plans, for state reporting on health care delivery or costs, or for "other purposes." To date HHS has made no such determinations, and this provision has not been subject to any formal interpretation.

HIPAA also preempts state and territorial laws which are "less stringent" in their protection of privacy than HIPAA, and conversely is preempted by those which are "more stringent." (While the difference between laws "superseding" and "preempting" can be important in some legal contexts, it is not material here.) In practical terms, this means that whenever HIPAA and a state or territorial law appear to conflict regarding individually identifiable health information, the one which is more protective of individual rights or provides greater individual access to health information controls.

The analysis is often complicated, however, since many state or territorial laws explicitly and intentionally apply only to health care organizations or health care information, while others are laws of broader application which include but are not limited to health care, and some (especially common law cases) apply by implication but not clearly and directly.

Detailed analysis of the relationship between HIPAA and state and territorial laws therefore tends to be complex and very state specific. At a high level, however, it is usually possible to identify consistent principles and trends.

3.1.2 Health Care Provider Confidentiality Obligations

Health care information protection obligations are ultimately rooted in or traceable to the Hippocratic obligation to respect patient confidentiality. This obligation still applies to all licensed physicians as a matter of professional ethics, and in some states its violation by a physician can be grounds for a professional malpractice action. Over time this same

obligation has been extended to most if not all state-licensed health care provider professionals, again as a matter of professional ethics, and to many state-licensed health care provider entities by statute, regulation, or licensure requirement.

The general principle of the confidentiality obligation is that patient information must not be used or disclosed except for the benefit of the patient. While this obligation is often specified in licensing statutes or regulations, the specific application of this principle tends to be defer to the professional judgment of the provider, and to be developed through caselaw in litigation.

3.1.3 Alcohol/Drug Abuse, STD, and Other Sensitive Information

Certain categories of information are required by federal or state laws to be given more stringent protections than other categories.

Information related to alcohol or substance abuse treatment is generally not only required to be disclosed without patient consent under much more limited conditions than HIPAA requires, but when disclosed often must also be accompanied by a statement that redisclosure by the recipient is prohibited.

State laws may require additional protections or limitations against disclosure of information about communicable diseases, including sexually transmitted diseases (STDs) (including but not limited to HIV/AIDS), as well as abortion or contraceptive services. These laws are highly variable and in some states controversial.

Some states have enacted legislation requiring additional protections or limitations for genetic information about individuals. These laws too are highly variable.

3.2 Medical Records Standards

The key functions of medical records are to support clinical decisions and claims payments and provide documentation for purposes such as quality assurance, accreditation, and regulatory oversight. There are no uniform legal requirements for medical records, and specific protocols and procedures for medical records form and content are generally developed by health care providers to fit their particular needs and circumstances. However, there is a well-developed body of professional standards and knowledge which should guide medical records implementation and usage.

3.2.1 The Legal Medical Record

Because of the potential for legal disputes over patient care, qualification for payment, and other issues in which information included in medical records may be relevant, medical records generally need to meet standard for admission as evidence in court. In practical terms this means the record meets the following criteria:

- The individual creating the record must be identified. This is typically done by signature of the physician or other appropriate attending professional.
- The record must be created and maintained using procedures ensuring it is not altered without appropriate authorization or without a record of the alteration.
- The record produced for use in evidence must accurately reflect the record as it was created and maintained.

These criteria can be met by appropriately designed electronic medical record (EMR) systems, supported by appropriate business processes. If records or information derived from an EMR are challenged in court it may be necessary to obtain expert testimony demonstrating the reliable functioning of the system.

3.2.2 Distinction from Personal Health Records

The "personal health record" (PHR) is distinct from the EMR, and is intended to be a personal information resource for consumers. There is no standard legal definition of the PHR, but American Health Information Management Association (AHIMA) has published a standard professional definition.

A PHR may be paper, electronic, or a hybrid of the two. An electronic PHR may reside on the consumer's personal computer (PC) or other device, or may be hosted by a health care organization or consumer services provider. Information in the PHR is that health information which may be most useful to the consumer, including demographic information (for easy provision to a provider or plan, if necessary) and essential clinical information such as health conditions, immunizations, medications, allergies, drug sensitivities, etc. As a general rule the consumer is considered the owner of his or her PHR.

3.3 Health Insurance Companies and the Gramm-Leach-Bliley Act

Insurance companies, including insurance companies which are Covered Entities under HIPAA, are also considered regulated "financial institutions" under federal law. Financial institutions are required to comply with privacy and security requirements for the "nonpublic personal information" of their customers under the Gramm-Leach-Bliley Act (GLBA). Personal information under GLBA includes some but not all types of information defined as PHI under HIPAA. Health insurance companies are therefore required to comply with both HIPAA and GLBA.

Like HIPAA, GLBA compliance requirements are specified in regulations. For historical reasons, insurance regulation has been and continues to be a state function, generally under the office of the state insurance commissioner. Specific GLBA privacy and security compliance requirements for health insurance companies are therefore contained in state regulations and legislation.

State GLBA regulations must require at a minimum the publication of a Notice of Privacy Practices (NPP), consumer access rights, limitations on the sharing of personal information,

and implementation of an information security program. The National Association of Insurance Commissioners (NAIC) has provided a model law for the privacy and security of "nonpublic personal health information" and "nonpublic personal financial information." Most but not all states have adopted the NAIC model law, but in many cases the model law has been modified in various ways.

GLBA regulations (and legislation implementing GLBA) are relatively generalized and can be reconciled with HIPAA. A few states have explicitly provided that compliance for purposes of HIPAA satisfied GLBA compliance.

3.4 Identity Theft and Security Breach Notification Laws

"Identity theft," which is essentially the commission of fraud by use of another's personal information to obtain goods or services on credit in that person's name, emerged as a major public policy issue in 2002. Identity theft on a large scale has been enabled by the proliferation of databases of personal information held by governmental agencies, financial institutions, health care organizations, and a wide variety of commercial and nonprofit enterprises. The issue emerged as a significant public policy concern in response to a number of security breach incidents in which such databases were accessed or devices holding them were stolen, placing data subjects at risk of identity theft.

As of 2006, many but not all states had enacted security breach notification laws requiring organizations holding personal information in electronic media to notify data subjects in the event of a security breach potentially affecting their information. The state laws vary materially but, in general,

- apply to all governmental agencies in the state, and all nongovernmental entities "doing business" in the state;
- apply to a set of personal information including name and Social Security number or account number plus account access authorization code (eg, PIN number);
- exempt personal information which has been encrypted;
- require notification of all residents of the state potentially affected by a security breach potentially affecting their personal information, sometimes subject to limited ability to delay notification if necessary for law enforcement investigation or system security corrections; and
- provide for damages for data subjects harmed by a failure to comply with the law, and for civil regulatory enforcement.

4. ELECTRONIC COMMERCE

Electronic commerce (e-commerce) is principally regulated by contractual agreements and industry standards, and enabled by federal and state laws.

The principal federal law relevant to e-commerce is E-SIGN, while the principal form of state law is the Uniform Electronic Transactions Act (UETA), and secondarily the Uniform

Computer Information Transactions Act (UCITA). Almost all states have enacted UETA, while a very few have enacted UCITA.

E-SIGN enables e-commerce by prohibiting almost all federal and state laws from requiring hard-copy (ie, paper) documentation and "wet" (ie, handwritten) signatures. It is also technology neutral and prohibits laws requiring use of any specific technology for electronic signatures. The principal exceptions are for testamentary documentation (wills, etc) and for types of transactions which a governmental agency has determined are particularly risky and require a specific technology to manage the risks. E-SIGN also requires specific consumer consent to electronic notices and requires the implementation of safeguards to prevent the unauthorized alteration of transactions and signature records.

E-SIGN preempts any state law which conflicts with it. UETA is consistent with E-SIGN, and E-SIGN specifically does not preempt UETA where it has been enacted in its standard form. Most states have enacted UETA in its standard form. Because of the effects of E-SIGN, for present purposes UCITA is also generally consistent with UETA and E-SIGN, though it adds a number of additional provisions.

4.1 Electronic Signatures

Legally, an electronic signature is the record of any electronic process or event which is associated with an individual and is intended to demonstrate an "intent to sign." An electronic signature can therefore be an e-mail, a "click" (or "double-click") on a web page graphic (eg, an "I accept" button), an oral statement electronically recorded, a digital certificate, etc. By law, parties can agree to—or a single party can consent to—the use of any of these and more as a valid electronic signature for most purposes.

In the absence of a legal requirement, the decision of which electronic signature solution to implement depends on the parties' balance between risk and convenience. In order to avoid a party repudiating his electronic signature—denying that he executed the process or event, or denying his intent in doing so—the solution must both reliably associate the event or process with the specific individual and demonstrate his intent in executing that process or event. Procedures which tend to increase the reliability of an electronic signature for these purposes tend to decrease the convenience of the user in executing the electronic signature and increase the administrative burdens of the organizations which must accept and maintain records of the electronic signature.

An electronic signature can be as simple as the entry of an identifier (identifying information), such as the individual's name or an assigned user name. However, this is a relatively unreliable solution, since anyone who knows an individual's identifier, which may be well known or easy to guess, can fraudulently "spoof" his electronic signature.

Most electronic signatures therefore require both "identification and authentication," a process often also used to obtain access to computer systems and data resources. In this process the user must submit both her identifier and some distinguishing data which cannot be readily spoofed by someone else. These data "authenticate" the individual.

Authentication data may be "something the individual knows," such as a password or PIN; "something the individual has," such as a "swipe card" with a magnetic stripe or an activation token with the authentication data encoded in it; or "something the individual is," a biometric characteristic such as a fingerprint. If a biometric solution is used, the biometric data are used to generate digital authentication data.

Any party accepting an electronic signature including authentication must have the ability to match the authentication data with the same data and information which associates it with the correct individual. This is readily accomplished in relatively "closed" environments, such as networks operated by a single organization, since the network operator can issue the password, card, or token, or arrange to collect the biometric information. However, authentication is more difficult in "open" networks, used by individuals who do not have a prior relationship to the organizations which may need to be able to accept their signatures. For open network purposes, some trusted third party generally must provide the necessary authentication.

For general e-commerce purposes, the role of trusted third party is usually filled by credit card companies. An e-commerce merchant is willing and able to accept the electronic signature of a previously unknown consumer on a purchase order when the purchase is made by credit card, because the credit card company assumes the risk that the transaction is fraudulent. The credit card company, in turn, can assume this risk because it already has a relationship with the consumer which has provided the credit card company with sufficient authentication information, and because the credit card company has procedures to detect and deter fraud and reserves to cover losses from fraud.

This model does not work for all open networks, however, since there may be many nonfinancial transactions in which a reliable electronic signature is desirable—for example, electronic prescribing (e-Rx—see below). The most reliable, though not necessarily the only electronic signature solution for this type of transaction, is a digital signature administered through a PKI.

In a PKI authentication, data in the form of a "digital certificate" are provided by a trusted third party called a "certification authority." The digital certificate includes basic information about the party executing an electronic signature (called a "subscriber"), along with a unique encryption "key" (computational algorithms used to alter digital code). When a user executes a PKI-based digital signature, the certification authority confirms the validity of the authentication to the party receiving the signature (called a "relying party). There is a well-developed body of technical standards and legal theory behind PKI, but in practice it has

proven burdensome to implement, and it is generally used only for relatively sensitive transactions. One of the things a digital signature provides is what is referred to as "nonrepudiation." In other words, the person using his or her own digital signature is not able to state later that he or she did not "legally" sign the document electronically or communicate information requested/provided.

The reliability of any electronic signature depends crucially upon the business processes used to administer it. In particular, any reliable electronic signature solution must have well-designed processes including initial user identification and registration; secure issuance and management of authentication information by both users and the organization managing authentication; and suspension or termination of acceptance of the electronic signature if the authentication information is compromised or the user's electronic signature privileges are suspended or terminated.

4.2 Electronic Prescriptions and Drug Orders

The states have traditionally been the principal regulators of pharmacies, though DEA exercises substantial authority over Schedule I and II controlled substances in particular. Under the federal Medicare Modernization Act of 2003 (MMA), however, CMS was authorized to issue regulations specifying required standards for electronic prescription transactions ("e-prescribing" or "e-Rx").

As of 2006 the first set of e-Rx regulations had come into effect for a basic set of prescription transactions, with additional standards anticipated over the next few years. These regulations are binding on Medicare Part D (prescription drug benefit) plan sponsors, and while they do not require "prescribers" (ie, health care professionals writing prescriptions) or "dispensers" (ie, pharmacies filling prescriptions) to use e-prescribing, those which choose to do so must follow the standards.

The e-Rx regulations require the states to permit electronic signatures for e-prescribing transactions, and DEA will require e-prescribing transactions involving Schedule I and II drugs to use digital signatures in a DEA certification authority-based PKI. All other e-prescribing transactions may use any electronic signature solution agreed upon by the parties, though the states may have sufficient interest in this area to require specific solutions by regulation.

5. CONTRACT LAW ISSUES

A "contract" comes into existence legally whenever two or more parties agree to one or more obligations or responsibilities among themselves in return for some benefit. Contracts may be entirely oral or entirely written, or a combination. Oral contracts "made on a handshake" may reflect a laudable level of trust but are harder to prove, especially in case of a dispute between the parties. Contract negotiations can be a useful vehicle for clarifying

the parties' expectations and understandings before they begin joint activities, and if well drafted can be a valuable resource in guiding those activities and resolving disputes.

5.1 Intellectual Property

The use of computer and networks inevitably involves the use of software and business processes which are "intellectual property." Intellectual property ownership and use are governed by somewhat different rules from those applied to tangible property.

Intellectual property is generally owned by the party who creates it, unless it is created as a "work for hire" for another party, and is most frequently "licensed" rather than conveyed outright to the users by the owner. A license is something like a lease, a limited right to use the intellectual property without all the rights of an owner. For example, a license will typically prohibit or at least limit the user's rights to copy or alter the intellectual property, incorporate it into other intellectual property, or allow others to use it, and may allow use for only a limited term. License terms are therefore crucial to the use of any computer system or network.

The principal categories of intellectual property are patent, copyright, trade and service marks and names, and trade secrets. Patents, in this context, may be obtained for hardware or business process designs which are unique, "novel," and not "obvious." Patents are obtained by filing the design with the US Patent Office, which must review and approve the patent.

Copyright applies to unique text and graphics, including computer code. The creator of copyrightable materials has an automatic "common law" copyright interest but may also register copyrightable materials with the US Patent Office by filing the materials. No federal approval is required or issued.

Trade and service mark and name intellectual property interests vest much the same way that copyright interests do, by common law with the option of federal registration. This kind of intellectual property interest can come into being when an entity does business under a distinctive graphic (mark) and/or name, which becomes associated with the entity by consistent use.

Finally, trade secrets are any information which is not known to or readily discoverable by other parties, which the party possessing the trade secret wishes to keep from being known and takes reasonable steps to protect. Unlike other types of intellectual property, trade secrets are not in the public record; conversely, unlike the other types of intellectual property, trade secret rights do not give their owner the authority to keep others from using the same information as long as they develop it independently.

5.2 Warranties, Representations, and Indemnification

Warranties, representations, and indemnification provisions are included in contracts to allocate legal risks among the parties. The Uniform Commercial Code (UCC), a law enacted in standardized (but not identical) form in all states, provides controlling rules in this area for most types of sales, personal property leases, and a number of types of financial transaction, but these rules can be varied by contract. The UCC also does not apply to intellectual property or regulatory issues, or claims by third parties.

Warranty and representation are closely related concepts. The distinction between the two is grounded in ancient legal history, and not very clear in current law. Basically, both refer to statements of fact which are relevant to the contract; "representation" tends to be used most broadly and tends to refer to statements of past or existing fact, while "warranty" tends to be used to refer to statements of the quality of goods or services. For example, a party to a data sharing contract might "represent" that it is a health care provider licensed in a given state, while a services vendor would "warrant" that the help desk will be available 24 hours a day.

Warranties and representations are therefore used to allocate risks that facts will turn out not to be true or obligations and expectations will not be fulfilled as between the contracting parties.

"Indemnification" provisions, on the other hand, are used to allocate liability among the contracting parties for claims made by third parties arising from the activities of the parties to the contract. For example, a hospital might contract to outsource its electronic medical records (EMR) system to a vendor, who will then be responsible for ensuring that there is no inappropriate disclosure of patient information from the system. The parties might anticipate that if such an incident were to occur, the affected patients might sue the hospital for breach of state confidentiality obligations. The hospital would therefore want the vendor to indemnify it against any such claims.

The term "indemnification" alone (and without a provision or definition that is more expansive) may refer only to payment of third party damages. Legal fees and other costs of litigation with third parties can also be substantial. Parties may therefore also agree to "defend" each other against third party claims, meaning that they will pay such costs. A "hold harmless" clause may also have this effect, and basically is often intended to ensure that the risk of all damages and costs arising from the contractually defined event or events are shifted to the identified party. For this reason, indemnification provisions are frequently phrased to state that a party will "indemnify, hold harmless, and defend" the other.

Representation, warranty, and indemnification issues can be difficult and complex, and there are many "terms of art" which have legal implications that may not be clear to a

nonlawyer. Provisions of this kind in particular should not be developed or interpreted without the help of legal counsel.

5.3 Dispute Resolution

While some contractual disputes cannot be resolved short of the courtroom, most contracts provide for some method of alternative dispute resolution. They also typically specify where dispute resolution proceedings, including litigation, will be conducted, and what law should apply or the laws of which state should apply. In some cases they may also provide that specific kinds of relief may be available, or may not be sought.

5.3.1 Applicable Law, Jurisdiction, and Venue

As long as one or more of the parties and/or the activities governed by a contract are located or occur in a given state or territory, the courts of that state have the authority (jurisdiction) to resolve disputes arising under it. In many cases the parties come from different states and/or their activities are conducted in more than one state, so more than one state may have jurisdiction.

The parties can agree that the laws of any given state which has jurisdiction will apply to their contract, and specify which state with jurisdiction will be the site for any litigation. They can also specify the court in which suit can be filed (the venue). This is generally desirable, since these decisions themselves might have to be litigated in the event of a dispute, if they are not specified in the contract. As with representations, warranties, and indemnification, this is an area in which there are many variations in terminology and legal terms of art, and dispute resolution provisions should not be developed or interpreted without legal counsel.

5.3.2 Alternative Dispute Resolution

A number of procedures for dispute resolution are available in addition to litigation, including arbitration and mediation. Arbitration is an adversarial proceeding but much less formal than litigation, conducted before an arbitrator who is typically a seasoned attorney, usually with legal representation of the parties, witnesses, and evidence. Mediation is a less adversarial proceeding, and is more like a facilitated negotiation intended to reach a mutually satisfactory settlement.

Almost all court systems provide for arbitration as an alternative to litigation—in some cases they may even require it—and there are a number of good commercial arbitration and mediation services available. The parties to a contract can require arbitration and/or mediation of a claim before it can be filed in a lawsuit, or can provide for binding arbitration (ie, the decision of the arbitrator is final). Contract provisions can also provide for required negotiations of disputes before resorting to any other form of dispute resolution.

The courts generally favor alternative dispute resolution provisions and will usually enforce them. Due to the high costs of litigation, alternative dispute resolution provisions are often considered desirable.

5.3.3 Remedies: Damages and Injunctive Relief

In most cases the harm a party experiences from a breach of contract is financial, or can be reduced to financial terms. In such a case, the appropriate relief for a breach of warranty or representation, or other breach of contract, is monetary "damages." Damages are awarded by the court at the conclusion of litigation or an arbitrator at the close of arbitration.

The most basic kind of damage award is for "actual" damages, which are intended as compensation for financial or property value lost as a result of the breach. Sometimes "consequential" damages are awarded, which are intended to compensate for less direct losses, such as lost opportunities. And some states allow for "punitive" damages in some cases, which are not intended as compensation but as deterrence for similar violations. Contracts frequently include "limitation of damages" clauses, which may preclude one or more of these types of damages, or limit the amount which may be awarded.

Some types of harm are not readily compensated by monetary damages, especially harms to human health or safety, reputation, and loss of intellectual property protections. In order to prevent such harms a party may seek "injunctive" relief, in the form of a court order prohibiting a harmful act, or requiring action to prevent or cure harm. If there is a threat of relatively immediate harm it may be possible to get a "temporary restraining order" (TRO) or "preliminary injunction" before the case is tried.

Injunctive relief is generally not available if the harm could be compensated by monetary damages, and injunction proceedings are subject to a variety of special rules, such as bond requirements, intended to ensure that TROs and preliminary injunctions in particular are not unfairly issued and that harm to the defendant is limited if they turn out to have been inappropriate. Because of these rules some contracts, especially intellectual property licenses, include injunctive relief clauses intended to make it easier for the plaintiff (eg, intellectual property owner) to get pre-trial injunctive relief.

6. HEALTH INFORMATION SHARING ORGANIZATIONS

Health care organizations share and have always shared information; information sharing is a fundamental and unavoidable activity. The sharing of information electronically over networks, however, has introduced management and liability issues not presented by traditional paper- and oral-based communications. The same efficiencies in sharing and processing large quantities of data at high speeds also enable the misuse of communications networks and computer systems, jeopardizing not only data but the organizations using and owning the networks and systems.

For this reason health care organizations sharing use of communications networks and systems have tended to enter into more or less formal arrangements which govern their usage. These arrangements range from highly informal agreements which may not even be fully written down, to detailed governance structures including formal incorporation with a governing board, officers, and formal membership qualifications.

At present no particular type of health care data sharing organization has any specific statutory or regulatory legal status. Many different types of arrangement and organization are in use or in development, and a number of variations have been tried in the past. The common theme to date among all of these is that participation is voluntary, and the specific arrangements used depend upon the preferences, expectations, and negotiating clout of the participants.

6.1 Subnetwork Organizations

One useful concept which has recently emerged in the Connecting for Health project is that of the "subnetwork organization" (SNO). A SNO is defined as any group of entities which communicates clinical data using a single record locator system (to locate records pertaining to individuals which are held by the various participants), contractually subject to a consistent basic set of common policies.

Connecting for Health has provided a set of policy and technical guides which are intended to establish the minimum basic framework for a SNO, along with a model contract to guide SNO formation. Links to these materials can be found in ***Appendix A, Reference Library***.

All of the types of arrangement discussed below may be considered types of SNO.

6.2 Regional Health Information Organizations (RHIOs)

A "regional health information organization" (RHIO)—sometimes called a "regional health information network" (RHIN)—is generally conceived as a network serving health care organizations in a given market. While RHIOs are not common at this time, and there are variations among those which exist, generally they are considered to be nonprofit membership organizations in which all participants have an opportunity for representation.

The RHIO is governed by a board and officers, or it may be established by contracts. RHIO "membership" is required for network usage. The RHIO governing body or contracts set the terms of use through policies and agreements to which the participants are bound as RHIO members. Sometimes, but not necessarily, governmental (especially state) agencies are considered appropriate as RHIO leaders, or even controlling entities.

6.3 Enterprise Networks

An "enterprise network" is a network established by and principally for a single large organization or group of related organizations, such as a health insurance company, large

HMO, or pharmacy chain. Internal operations and network usage are governed by enterprise policies and procedures. External users and third-party organizations may be permitted to use the network to communicate with the enterprise, with each other, and/or with other parties, by agreement with the enterprise.

6.4 Other Types of Networks

The most noteworthy predecessors to the RHIO concept are the Community Health Management Information Systems (CHMIS) and the Community Health Information Network (CHIN), both dating from the 1990s. The CHMIS was generally conceived as a centralized network serving a specified region and based on a data repository, possibly under state government control. The CHIN was a private-sector alternative to the CHMIS, principally put forward by larger private health care organizations and often essentially an enterprise network.

Neither concept was adapted to Internet technologies. The CHMIS concept met with political opposition and faced funding problems, while a few CHINs developed into reasonably useful, limited services providers.

Some health care information technology vendors in particular refer to "organic RHIOs," groups of organizations which agree among themselves to share data and contract for the technology to do so.