Communications of the Association for Information Systems

Volume 39 Article 17

11-2016

Health IT Legislation in the United States: Guidelines for IS Researchers

Karlene Cousins
Florida International University, kcousins@fiu.edu

Recommended Citation
Cousins, Karlene (2016) "Health IT Legislation in the United States: Guidelines for IS Researchers," *Communications of the Association for Information Systems*: Vol. 39 , Article 17.
DOI: 10.17705/1CAIS.03917
Available at: http://aisel.aisnet.org/cais/vol39/iss1/17

Communications of the
Association for Information Systems

Tutorial ISSN: 1529-3181

Health IT Legislation in the United States: Guidelines for IS Researchers

Karlene C. Cousins
Information Systems & Business Analytics Department
Florida International University
kcousins@fiu.edu

Abstract:

In this tutorial, I review the most pressing legal issues that health information systems (IS) professionals face and how health information technology (IT) legislation drive them. The issues I discuss include the confidentiality and security of electronic protected health information, meaningful use of health IT, health information exchanges, and information governance. I also provide directions for future research.

Keywords: Legal, HIPAA, HITECH, Protected Health Information, Health IT Legislation, Compliance, Regulations, Information Governance.

This manuscript underwent peer review. It was received 02/17/2015 and was with the author for 6 months for 1 revision. Douglas Havelka served as Associate Editor.

1 Introduction

Healthcare in the United States is a complex and highly regulated industry. A multitude of federal and state laws and accrediting and professional bodies contribute to healthcare legislation and regulation. These laws and standards define how healthcare is delivered, financed, and reimbursed, and they also protect the confidentiality and security of health information.

The underlying goal of healthcare information technology (HIT) legislation and regulation is to facilitate more efficient health information sharing to address healthcare costs and improve healthcare's quality and safety (Brodnik, Rinehart-Thompson, & Reynolds, 2012). Approaches include encouraging healthcare organizations to move from paper to electronic health records (EHRs) and to develop health information exchanges (HIEs) to enable parties to share information.

In the typical healthcare organization, health information systems (IS) professionals protect health information's confidentiality and security. As such, health IS professionals must understand healthcare law's complexity and accommodate changes to laws, standards, policies, and procedures surrounding the growing use of electronically stored health information.

This tutorial reviews the most important health IT laws and their implications for health IS researchers and practitioners. Some of the most pressing issues I discuss include the confidentiality and security of health information, the meaningful use of health IT, health information exchanges, and information governance.

The paper proceeds as follows. In Section 2, I define the legal health record and discusses its formats and ownership. In Section 3, I review the relevant health IT federal and state legislation. In Section 4, I outline the legal requirements for the use and disclosure of the patient's protected health information. In Section 5, I highlight the administrative requirements that health IT legislation necessitates. In Section 6, I discuss the information governance issues that health IT legislation presents. Finally, in Section 7, I summarize the health IT legal and regulatory research issues and raises research questions for the IS research community to consider.

Because this subject matter changes as new technologies, laws, and regulations emerge, this paper cannot adequately discuss all topics in detail. Therefore, the reader should interpret this tutorial not as a legal primer but as a guide to assist researchers and practitioners in understanding the legal issues involved in managing the health IS. Readers should always consult legal counsel when required.

2 Introduction to Health Records

2.1 Definition and Purpose of Health Records

Health information refers to the information that healthcare organizations generate and collect as a result of delivering care to a patient. The information that healthcare organizations document depends on several factors such as the state or jurisdiction of the healthcare organization, accrediting or licensing body requirements, type of healthcare organization, and the services rendered (Brodnik et al., 2012).

Healthcare providers create patient health records as they care for patients (Brodnik et al., 2012). Other terms for the health record include medical record, patient record, client record, inpatient record, outpatient record, or clinical record. (Brodnik et al., 2012). The health record contains personal, financial, social, and health data, and is the legal account of the services the healthcare provider provided to the patient and the patient's healthcare status.

Though the primary use of health information is for clinical care, it is often used as evidence in legal cases. Other uses include public health reporting, population health studies, third-party reimbursement, research, education, and patient-safety and quality-improvement initiatives.

2.2 Health Records Formats

Healthcare organizations may maintain health records in either paper or electronic format or may combine the two to create a hybrid health record. The hybrid health record may contain both paper and electronic records and media such as film, video, or imaging systems. The data come from clinical information systems such as laboratory, pharmacy, radiology, nursing, ancillary or administrative systems, and paper documents. The data may be handwritten or captured through voice entry and translated to text.

A completely electronic health record is called an EHR or electronic medical record (EMR). Research and practice often use these terms interchangeably (Brodnik et al., 2012; National Alliance for Health Information Technology, 2008). The key difference between the EHR and the EMR is that the EMR is housed in a single organization whereas an EHR may contain data or information across more than one organization (Brodnik et al., 2012).

Healthcare consumers may also maintain their own personal heath records. The personal health record is "an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared and controlled by the individual" (National Alliance for Health Information Technology, 2008). The personal health record is separate from and does not replace the legal health record. However it can form part of the legal health record.

2.3 Ownership, Custodianship, and Stewardship of Health Records

Generally, the healthcare provider who generates the record and owns the physical media that contains the record owns the patient's health record. However, the healthcare provider's ownership of the physical health record does not permit providers to share or sell patients' identifiable medical information as they desire. Further, several federal and state laws uphold the patient's right to control the information in the record. For instance, the federal Health Insurance Portability and Accountability Act (HIPAA) grants patients the right to access, view, copy, or amend their health record. In 2015, the state of New Hampshire passed legislation that explicitly states that patients own the information in their health records.

An emerging trend is the use of health record banks (McWay, 2010). These banks store electronic personal health records (PHRs), and governmental or commercial entities who serve as the data's trusted custodians operate them. Modeled on financial banks, health record banks involve both "depositors" and "withdrawers" of health information. The patient, caregiver, and other healthcare personnel add data to the PHR over the patient's lifetime. The patient and other people (with the patient's consent) can fully access the data. Some of the entities operating PHRs may not be subject to HIPAA because they may not fall under the definition of a covered entity. However, privacy laws and regulations for the entity's industry would govern how they handle the individual's PHR.

The custodian of the health records is the individual responsible for the operational functions related to developing and maintaining the health records (Brodnik et al., 2012). The custodian is responsible for the care, custody, control, and proper safekeeping and disclosure of health records. The courts may call on the custodian to testify as to the authenticity of the health record in legal proceedings. The role of the custodian in such an event is to verify that the record is what it purports to be and the normal business practices used to produce the record. The information steward's role has also begun to emerge. Stewardship is a broader role than custodianship and includes responsibility for ensuring the integrity (accuracy, completeness, timeliness), privacy and security of the health record (Washington, 2010). Stewards also play a critical role in information governance and are responsible for ensuring that high quality health electronic health information is accessible and available for legal and business purposes Washington, 2010).

Parties involved in litigation routinely request and use patient information as evidence in legal proceedings. These legal proceedings could use the health record to allege a physician's negligence or as evidence when the patient's health and treatment are at issue. Custodians of protected health information (PHI) act as gatekeepers for the appropriate access, use, and disclosure of health records for court proceedings and in accordance with federal and state laws.

2.4 Defining the Legal Health Record

In the event that PHI is requested and authorized for disclosure, the healthcare organization would release only the subset of the healthcare information related to the patient's care. This portion of the patient's health information is the legal health record. As Figure 1 shows, the legal health record is a subset of the contents of the entire patient database.

The legal health record is "generated at or for a healthcare organization as its business record and is the record that would be released upon request" (AHIMA, 2011). The legal health record documents the healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization.

An organization's legal health record definition must explicitly identify the sources, medium, and location of the individually identifiable data. The documentation that comprises the legal health record may physically exist in separate and multiple paper-based or electronic systems.

The legal health record is used for business, legal, and compliance purposes. The legal health record serves to:

1. Support the decisions made in a patient's care
2. Support the revenue sought from third party payers
3. Document the services provided as legal testimony regarding the patient's illness or injury, response to treatment, and caregivers' decisions, and
4. Serve as the organization's business and legal record.

Organizations disclose portions of the legal health record when responding to formal requests for information for evidentiary purposes. However, parties may request the release of health information outside the legal health record in the event of lawsuits or other forms of legal action.

No two organizations have the same legal health record. An organization's legal health record constitutes elements that vary depending on how the organization defines the legal health record. The determining factor for including information as part of the legal health record is not where it resides or the format it takes but whether healthcare practitioners use the information to make decisions about patient care (AHIMA, 2011).

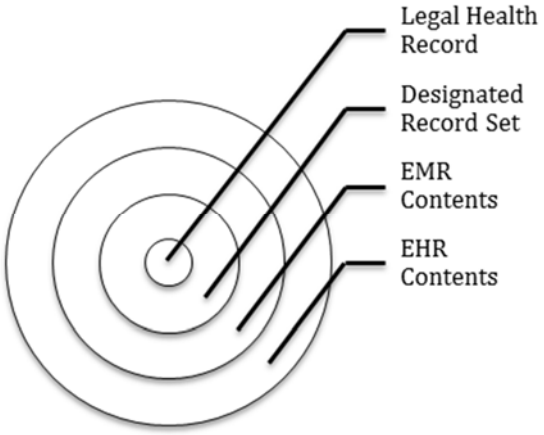

Figure 1. Location of the Legal Health Record

Healthcare organizations must also consider the organization's designated records set when defining the LHR. The HIPAA Privacy Rule requires that any healthcare provider, plan, or healthcare clearing house that electronically transmits health information must define its designated record set. Under HIPAA, the designated record set is "a group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions" (AHIMA, 2011). The designated record set also contains individually identifiable data the healthcare organization stored on any medium and collected and directly used in documenting healthcare or health status. The designated record set is generally broader than the legal health record because it addresses all protected health information. While the legal health record is generally the information used by the patient care team to make decisions about the treatment of a patient, the designated record set also contains business information unrelated to patient care.

Overall, individuals have the right to inspect and obtain a copy of their health record, request amendments, and set restrictions on the disclosure of medical and billing information used to make decisions about their healthcare. Organizations must also provide patients with a notice of privacy rights with respect to how the organization uses and discloses their information.

In Section 3, I discuss the primary health IT legislation that affects how health IT is designed, implemented, and used.

3 Health IT Legislation

The American Recovery and Reinvestment Act of 2009 (ARRA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) have all helped to shape health IT in the US. Individual states have also passed laws related to the content of health records and PHI's confidentiality and security.

In Sections 3.1, 3.2, and 3.3, I review the federal and state legislation related to health IT.

3.1 The American Recovery and Reinvestment Act (ARRA)

The American Recovery and Reinvestment Act of 2009 (ARRA) is a federal law that includes an act pertaining to health IT, known as the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

3.1.1 Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)

HITECH includes legislation that provides financial incentives to eligible entities that demonstrate meaningful use of certified EHRs and health information exchanges (HIEs) and financial penalties for those healthcare organizations that do not comply with meaningful use requirements. These penalties reduce the Medicare and Medicaid payments due to incompliant healthcare organizations.

HITECH contains important program-management standards and certification components. The act empowers the U.S. Department of Health and Human Services (HHS) to establish programs to promote health IT use to improve healthcare quality, safety, and efficiency. HITECH also establishes a health IT policy committee to govern these initiatives. This committee's role is to make recommendations on the development of standards, implementation specifications, and certification criteria for the electronic exchange and use of health information.

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

The Office of the National Coordinator for Health Information Technology (ONC) is the principal federal entity charged with coordinating nationwide efforts to implement health IT. The ONC is located in the Office of the Secretary for the U.S. Department of Health and Human Services (HHS). The HITECH Act mandates that the National Coordinator heads the ONC.

The ONC leads the government's health IT efforts and supports the entire health system in adopting health IT. As Sections 3.1.3 and 3.1.4 outline, these initiatives include the Medicare and Medicaid Electronic Health Record (EHR) incentive program and the development of enhanced health information exchange (HIE) services across the United States.

3.1.3 Meaningful Use of Health IT

The Office of the National Coordinator for Health Information Technology (2015b) defines the meaningful use of health IT as using certified EHR technology to: improve healthcare quality, safety, and efficiency; reduce health disparities; engage patients and family; improve care coordination and public health; and maintain the privacy and security of patient health information.

The Medicare and Medicaid EHR incentive program provides incentive payments to eligible entities as they demonstrate meaningful use of certified EHR technology. Eligible entities include eligible professionals, eligible hospitals, and critical access hospitals (CAH). Eligible professionals can receive approximately US$44,000 to US$63,750 and hospitals in excess of US$2,000,000 over a five-year period for the meaningful use of health IT.

To demonstrate meaningful use, entities must show that they have used certified EHR technology to achieve specific objectives above specified thresholds in three separate stages over a five-year period (2011-2016): As figure 2 shows, these stages include: stage 1: data capture and sharing; stage 2: advanced clinical processes such as rigorous health information exchange, and stage 3: improved clinical outcomes such as improved quality, safety, and efficiency. For instance, in stage 1, eligible professionals must attest that they use certified EHR to carry out 13 core activities. These stage 1 core activities include

using the EHR for maintaining patient demographics, electronic prescribing, checking for drug-drug and drug-allergy interactions, and maintaining a list of current diagnosis and allergies. For the latest meaningful use updates, please refer to the ONC's website at www.healthit.gov.

Beginning in 2015, eligible entities in the Medicare Program began to receive Medicare payment reductions if they were unable to demonstrate meaningful use. The payment reductions start at 1 percent and increase each year that the affected entity does not demonstrate meaningful use to a maximum of 5 percent.

As of April 2015, 98 percent of all hospitals have demonstrated meaningful use and/or adopted, implemented, or upgraded an EHR (Office of the National Coordinator for Health Information Technology, 2015a).

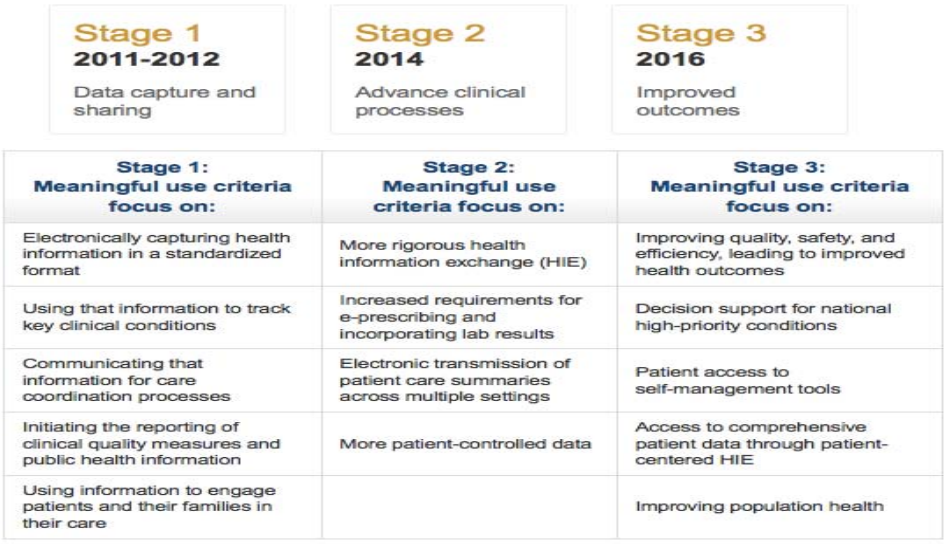

Figure 2. Meaningful Use Stages (Office of the National Coordinator for Health Information Technology, 2013b)

The meaningful use outcomes are encouraging. Healthcare organizations reported a reduction in the digital divide (Office of the National Coordinator for Health Information Technology, 2012b); better patient communication, monitoring, and engagement (Office of the National Coordinator for Health Information Technology 2012a, 2012b); improved quality outcomes (Office of the National Coordinator for Health Information Technology, 2011a, 2012a); improved health information exchange (Office of the National Coordinator for Health Information Technology, 2011b); and patient care coordination (Office of the National Coordinator for Health Information Technology, 2011b, 2011c).

3.1.4 Health Information Exchanges (HIEs)

HIEs allow doctors, nurses, pharmacists, and other healthcare providers to securely share a patient's vital medical information electronically and provide more effective, efficient healthcare services. HIEs reduce the need for patients to transport or relay their medical history, lab results, images, or prescriptions between health professionals. Meaningful use requirements and new payment approaches that stress care coordination have motivated healthcare providers to participate in HIEs. Federal financial incentives have also driven interest in and demand for HIE.

The three key forms of health information exchanges are:

- Directed exchange with which providers can send and receive secure information electronically between themselves to support coordinated care.
- Query-based exchange with which providers can find and/or request information on a patient from other providers. Providers often use it for unplanned care.
- Consumer mediated exchange with which patients can aggregate and control how providers use their health information.

One of the greatest challenges to HIEs' success is facilitating interoperability. HIE requires that healthcare organizations adopt standards to facilitate interoperability so that disparate systems in the HIE can speak to each other. To promote interoperability, the ONC and the Office of Science and Technology (OST) are trying to standardize the meaning, transport, and security of the data and services through application program interfaces (APIs) for HIEs (Office of the National Coordinator for Health Information Technology, 2014c).

The ONC designed the State Health Information Exchange Cooperative Agreement Program to increase the adoption of HIEs in 2010 (Office of the National Coordinator for Health Information Technology, 2014e). This program encourages states to develop the information technology infrastructure to facilitate HIEs. Under this initiative, HITECH provided US$560 million in grants to all 56 U.S. states to implement approaches to encourage, develop, and sustain HIE over four years. At the end of 2013, 63 percent of grantees had directed exchange services broadly available, and 68 percent had implemented query-based exchange services (Dullabh, Charles, Henry, & Lee-Wikins, 2014).

3.2 Health Insurance Portability and Accountability Act (HIPAA) of 1996

HIPAA is a federal law that mandates that healthcare organizations maintain the confidentiality and security of individuals' identifiable health information. HIPAA includes the privacy, security, and breach notification rules. The HIPAA privacy rule describes what information is protected and how covered entities can use and disclose protected information. The HIPAA security rule describes who the HIPAA privacy protections cover and what safeguards covered entities must implement to ensure that they appropriately protect electronic PHI. The HIPAA breach notification rule requires HIPAA-covered entities and their business associates to provide notification following a breach of unsecured PHI.

3.2.1 HIPAA Privacy Rule

The privacy rule defines and limits the circumstances in which covered entities may use an individual's PHI. In certain circumstances, the privacy rule may authorize or require the covered entity to disclose or use PHI without a patient's authorization, such as to treat an individual or for payment and operational activities (see Section 4). In all other circumstances, patients or their personal representative must authorize a covered entity to disclose or use their PHI via written authorization (U.S. Department of Health & Human Services, 2003a). Overall, the privacy rule strikes a balance that allows covered entities to use information where necessary while protecting the individuals' privacy.

The privacy rule protects all "individually identifiable health information" in any form or media (whether electronic, paper, or oral) that a covered entity or its business associate transmits. Individually identifiable health information is information, including demographic data, which persons could use to identify the individual. This information includes:

- The individual's past, present, or future physical or mental health or condition
- The provision of healthcare to the individual, and
- Past, present, or future payments for the individual's healthcare.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date and social security number) (U.S. Department of Health & Human Services, 2003a).

HIPAA's privacy rule does not apply to all entities. If an entity does not meet the definition of a covered entity or business associate, it does not have to comply with HIPAA's rules, though other laws may protect an individual's privacy. Covered entities may include health plans, healthcare clearing houses, and any healthcare provider who transmits PHI in electronic form. If a covered entity engages a business associate to help it carry out its healthcare activities and functions, the covered entity must have a written business associate contract or other arrangement with the business associate that establishes that the business associate needs to comply with HIPAA's requirements.

HIPAA enforcement follows PHI wherever it goes except under special circumstances. Thus, if a hospital provides PHI to a billing company and that billing company subcontracts with another entity, the enforcement body, the Office of Civil Rights, can enforce HIPAA down the chain of custody to the billing company and the subcontractor (United States Department of Health & Human Services, 2003a).

3.2.2 HIPAA Security Rule

The security rule establishes a national set of security standards for PHI held or transferred in electronic form. As such, the security rule only protects a subset of information covered by the privacy rule as it relates specifically to the electronic form of individually identifiable health information. The security rule calls this information "electronic protected health information" (e-PHI) (United States Department of Health & Human Services, 2003b) Thus, the security rule does not apply to PHI transmitted orally or in writing.

The security rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI. As such, the security rule gives well-developed guidelines on how covered entities should implement the administrative, technical, and physical safeguards. Recognizing that covered entities range from the smallest provider to the largest, multi-state health plan, the security rule is flexible and scalable to allow covered entities to analyze their own needs and implement solutions appropriate for their specific environments. What is appropriate for a particular covered entity will depend on the nature of the covered entity's business, size, and resources.

Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information
3. Protect against reasonably anticipated, impermissible uses or disclosures, and
4. Ensure compliance by their workforce.

Covered entities often use common IT security tools and techniques to comply with the security rule's requirements. For example, the security rule requires that covered entities verify that a person who seeks access to e-PHI has authorization (Gabriel, Charles, Henry, Lee-Wikins, 2015). Two-factor authentication techniques satisfy this HIPAA requirement. Two-factor authentication requires that users provide at least one additional form of identification beyond a user name and password to gain electronic access to e-PHI. Examples include requiring users to answer security questions or enter a randomly generated number sent to their personal mobile device.

Overall, the US has experienced an increase in the number of hospitals that have implemented mechanisms and procedures to comply with the security rule. For instance, the number of non-federal acute care hospitals that have adopted two-factor authentication has steadily increased since 2010 (Gabriel et al., 2015). In 2010, a third (32%) of hospitals had the capability. However, in 2014, nearly half (49%) had implemented two-factor authentication, which represents a 53 percent increase since 2010.

3.2.3 HIPAA Breach Notification Rule

HIPAA requires covered entities and their business associates to notify affected persons following a breach of their unsecured PHI. A breach refers to someone impermissibly using or disclosing PHI in a way that compromises its security or privacy. HIPAA presumes an impermissible use or disclosure of PHI to be a breach unless the covered entity or business associate demonstrates that the breached PHI was not likely compromised. Typically, the covered entity or business associate carries out a risk assessment to determine the likelihood that the PHI was breached by determining:

1. The nature and extent of the PHI involved, including the types of information that was breached or disclosed, and the likelihood that some one could use this information to identify its owner
2. The unauthorized party who used the PHI or to whom the disclosure was made
3. Whether the breaching party actually viewed or acquired the PHI, and
4. The extent to which the breached firm has mitigated the risk to the PHI.

In addition, the breach notification rule has three exceptions for what constitutes a breach:

1. The first exception applies if a person or workforce member acting under the authority of a covered entity or business associate unintentionally acquired, accessed, or used the PHI in good faith and in the scope of their authority.
2. The second exception applies to persons whom the covered entity or business associate authorized to access the PHI and who inadvertently disclosed the PHI to each other.

3. The final exception applies if the covered entity or business associate believes in good faith that the unauthorized person who received the PHI could not retain the information.

If a covered entity determined that a PHI breach occurred, they must notify affected patients no later than 60 days after they discovered the breach. If the breach of unsecured PHI affects more than 500 patients, the covered entity must also notify the media of the breach no later than 60 days after they discovered the breach.

In addition to notifying affected individuals and the media, covered entities must notify the Secretary of Health and Human Services. If a breach affects more than 500 persons, covered entities must notify the secretary within 60 days. If a breach affects less than 500 persons, then covered entities need only make a report to the secretary of such breaches annually.

Business associates must also notify the covered entity who hired them if the breach of PHI occurs by the business associate or at the business associate's premises.

In 2015, the medical and healthcare industry experienced 35.5 percent of all data breaches in the U.S. (Identity Theft Resource Center, 2015). Further, the FBI warned that healthcare breaches would continue to grow due to the low resilience of cybersecurity systems in the health sector compared to those in the financial and retail sectors (Experian, 2015). The expanding number of access points to PHI via EHRs, mobile, and wearable technology also increases the cybersecurity threat to healthcare systems (Experian, 2015).

While the breach notification rule does not prevent cybersecurity breaches, its notification provisions minimize the risk that someone will steal an individuals' medical information by notifying affected persons to take precautions. Industry reports reveal that, in 2014, medical identity theft affected 1.8 million U.S. individuals whose identities persons fraudulently used to gain medical services, procure drugs, and defraud private insurers and government benefit programs (Experian, 2015).

Notwithstanding the various federal laws that address health information confidentiality and security, states also passed legislation related to the content of health records and the use, collection, and disclosure of health information. In Section 3.3, I outline how these state laws relate to federal laws addressing the same subject matter.

3.3 State Law

As a general rule, statutes passed at the federal level address matters of national concern, and statutes passed at the state level address matters of particular interest to the individual state. As a consequence, multiple statutes written at the federal and state level can address the same subject matter. Statutes passed at the state level about a specific topic can also differ across states. When this conflict of laws occurs the courts may need to reconcile the federal and state law.

Under the preemption doctrine, for certain matters of national importance, federal law takes precedence or preempts state law. Certain federal statutes also include provisions as to which federal law should take precedence if conflicting provisions about the same topic in several statutes exist. For example, by law, the terms of the HIPAA privacy rule do not preempt the laws, rules, or regulations of the various states except where they contradict the HIPAA privacy rule. As a result, the HIPAA privacy rule provides a floor of protections that allows a state to enact more stringent protections than federal law for securing health information. Where the state laws are more stringent than a specific requirement or implementation of the HIPAA privacy rule, persons must comply with both the federal and state provisions

Most states have enacted their own laws and regulations pertaining to the use, collection, and disclosure of health information. Many states regulate the content and maintenance of patient medical records through provider-specific licensure laws. State law regulates when a provider may disclose PHI, to whom the information may be disclosed, and for what purpose. States are also free to set up their own health IT infrastructure in conformance with existing federal law. Where the statutes of different states differ on the same legal issue, a conflict of laws also arises (McWay, 2010). In a court case, a judge will decide which state's law will govern such a conflict. Lawyers try to avoid the conflict of laws in contracts by including a provision stating which state's law will govern in the event of a dispute.

Evidently, these differences in state laws present harmonization challenges when exchanging health information or providing healthcare across state lines. For example, telemedicine is an area where law conflicts at the state level present numerous harmonization challenges. Telemedicine refers to using

electronic communications and information technologies to provide or support clinical care at a distance (McWay, 2010). Patient consultations via video conferencing, transmission of still images, patient portals, remote monitoring of vital signs, continuing medical education, consumer-focused wireless applications, and nursing call centers are all examples of telemedicine (The American Telemedicine Association, 2012). In general, telemedicine presents numerous challenges because physicians must be licensed or registered in each state in which they practice telemedicine or incur civil and/or criminal penalties. Some states require physicians to have a face-to-face encounter and to conduct a physical examination for the physician to be able to prescribe medication electronically. Thus, legal issues arise when the healthcare practitioner and the patient are located in different states and the healthcare practitioner provides care via information technology. These legal issues include which state law will govern healthcare worker licensure for cross-state practice, the reimbursement for services rendered, and patient privacy and confidentiality concerns. Today, these legal barriers to telemedicine in the US remain largely unresolved.

The inconsistency in state and federal laws in terms of definitions, organizational structure, and content is often a barrier to HIE implementation (Harmonizing State Privacy Law Collaborative, 2009). As a result, in 2006, the ONC instituted the Health Information Security and Privacy Collaboration Project (HISPC) to help harmonize disparate state privacy and security laws. The project helps states to identify, analyze, and reform laws that relate to HIE. In 2009, HISPC carried out seven multi-state privacy and security projects focused on "analyzing consent data elements in state law, studying intrastate and interstate consent policies, developing tools to help harmonize state privacy laws, developing tools and strategies to educate and engage consumers, developing a toolkit to educate providers, recommending basic security policy requirements, and developing inter-organizational agreements" (Office of the National Coordinator for Health Information Technology, 2013a).

In Section 4, I discuss under what circumstances HIPAA allows covered entities to disclose PHI and electronic approaches to using and disclosing health information.

4 Use and Disclosure of Health Information

The privacy rule defines and limits the circumstances in which a covered entity may use or disclose an individual's PHI. In general, a covered entity may not use or disclose protected health information except either: 1) as the privacy rule permits or requires or 2) as the patient (or the patient's personal representative) authorizes in writing.

A covered entity must disclose PHI to individuals (or their personal representatives) upon their request. The covered entity must also disclose an individual's PHI to HHS for compliance, review, or enforcement purposes. In Section 4.1, I review the permitted uses and disclosures of PHI under HIPAA's privacy rule.

4.1 Permitted Uses and Disclosures under HIPAA

Covered entities may use and disclose PHI without an individual's authorization in several situations. They may disclose PHI:

1. **To the individual** in question.
2. **For treatment, payment, and healthcare operations**: (see the glossary for definitions of treatment, payment, and healthcare operations). However, some states such as Florida require the patient's consent for healthcare organizations to use and disclose their PHI for payment purposes.
3. **When they provide the individual with an opportunity to agree or object to disclosure**: where the individual is incapacitated, in an emergency situation, or unavailable, covered entities generally may make such uses and disclosures if, in their professional judgment, they determine that doing so is in the individual's best interests.
4. **For incidental uses and disclosures**: an individual may authorize the use of their PHI for a specific activity. However, in performing these activities, healthcare personnel may be able to deduce additional PHI about the individual, outside of the information the patient authorized for use and disclosure. The privacy rule permits the use and disclosure of PHI under these circumstances, as long as the information disclosed is limited to the "minimum necessary" (see Section 4.5 for more information on incidental uses and disclosures).
5. **For public interest and benefit activities**: covered entities may disclose PHI for health-oversight activities; for judicial proceedings; for law-enforcement purposes; for research; for essential

government functions; to funeral directors, coroners, or medical examines; to facilitate cadaveric tissue, eye, or tissue donation; to prevent or lessen a serious or imminent threat to a person or the public; for essential government functions; and to comply with workers' compensation requirements. The privacy rule aims to balance the individuals' privacy with the public interest's need for the information.

6. **In the form of a limited data set**: this limited data set contains PHI without certain specified direct identifiers of individuals and their relatives, household members, and employers such as names and social security numbers. Researchers, public health, or healthcare operations are some of the organizations that typically use the limited data set to support their activities.

4.2 Authorized Uses and Disclosures under HIPAA

A covered entity must obtain individuals' written authorization for using or disclosing their PHI for activities that fall outside treatment, payment, or healthcare operations or other purposes that the privacy rule permits. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on individuals' granting authorization to their PHI except in limited circumstances. Examples of disclosures that would require an individual's authorization include disclosures to a life insurer for coverage purposes, disclosures to an employer about the results of a pre-employment physical or lab test, or disclosures to a pharmaceutical firm for their own marketing purposes.

4.3 Super-confidential Information: Mental Health, Substance Abuse, and HIV/AIDS and Sexually Transmitted Diseases

Health information related to mental health, substance abuse, HIV/AIDS, and sexually transmitted disease is "super confidential". General authorizations do not cover super-confidential information. State laws and regulations exist in most states for authorizing the disclosure of super-confidential information, and one needs special authorization to do so. In most states, disclosing super-confidential information usually requires written patient authorization that specifies the recipient and the type of information to be disclosed (e.g., HIV, mental health), a subpoena with the patient's written authorization attached, or a court order.

4.4 Minimum Necessary Standard

Under the privacy rule, PHI's disclosure should be limited to the minimum necessary to accomplish the purpose for which the PHI is being used or disclosed (U.S. Department of Health and Human Services, 2002). This standard does not apply when making disclosures to a healthcare provider for treatment purposes, to the individual whom PHI refers to, as authorized by the individual, for compliance purposes, to the Department of Health and Human Services for enforcement purposes, and as required by law.

To use PHI, the covered entity's policies and procedures must identify the persons or classes of persons in the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. For non-routine disclosures and requests, covered entities must develop reasonable criteria for determining and limiting the disclosure or request to only the minimum amount of PHI necessary to accomplish the disclosure's or request's purpose.

4.5 Incidental Uses and Disclosure of PHI

Due to the nature of communications and practices in healthcare and the varied environments in which healthcare is delivered, the potential exists for someone to incidentally disclose an individual's PHI. For example, an individual who can see a person's list of medications can tell what a person's diagnosis may be. The HIPAA privacy rule does not encumber these customary communications and practices. Therefore, healthcare organizations need not eliminate all chance for incidental PHI use or disclosure to satisfy its standards. Rather, the privacy rule permits certain incidental uses and disclosures of PHI to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect individuals' privacy.

Section 4.6, outlines how healthcare organizations can use health IT to assure PHI's confidentiality and privacy and to help patients understand how providers will use and disclose their PHI.

4.6 Using Technology to Comply with HIPAA's Requirements for Authorized Use and Disclosure of PHI

4.6.1 Electronic Consent (E-consent) Approaches

Patients (especially those with poor literacy skills and diminished cognitive ability) can find the complex laws and regulations governing health information's privacy and confidentiality difficult to understand. The patient authorization and consent process still largely operates via paper. Thus, the patient authorization consent process can be time consuming and difficult to track and monitor.

The ONC provides guidance on how to use IT to facilitate and manage the patient authorization and consent process and facilitate meaningful patient consent. Two approaches are noteworthy: the eConsent Toolkit and the use of data segmentation technologies.

4.6.2 E-consent Tools and Architecture

Healthcare organizations may use the eConsent Toolkit to increase patient understanding and engagement for meaningful consent (Office of the National Coordinator for Health Information Technology, 2014a). The eConsent Toolkit provides a mobile, multimedia approach designed to educate patients about the provider's consent program and how the provider will use the patient's health information in a clear and accessible manner. To do so, the E-consent Toolkit uses an electronic story engine to present interactive, electronic, educational materials to patients. The eConsent Toolkit also provides a way for patients to exercise their consent electronically.

E-consent is important when HIEs share PHI. For example, the Texas Health Services Authority (TSHA) designed the architecture for a state-wide consent-management system to enable automated decisions regarding the release of a patient's medical record from one HIE to another HIE (Texas Health Services Authority, 2012). Once implemented, the consent management system will help each HIE to understand each other's policy and to have the ability to decide if a given patient's policy preference allows or disallows access to their PHI.

4.6.3 Enabling Patient Privacy Using Data-segmentation Approaches

E-consent approaches may go hand in hand with data-segmentation approaches. Data-segmentation technology allows healthcare organizations to electronically label or tag a patient's health information in a way that allows patients or providers to electronically share parts of a patient's record (Office of the National Coordinator for Health Information Technology, 2014b) (Goldstein, Rein, Heesters, Hughes, & Williams, 2010). Thus, organizations can segment data in a manner consistent with the patient's e-consent choices.

Data segmentation helps providers to comply with state and federal privacy law by helping to keep sections of the patient's electronic health record private. For instance, both the HIPAA and state law may require healthcare organizations to treat super sensitive information such as HIV/AIDS status, substance abuse treatment, and other types of sensitive topics differently than other parts of a patient's record.

HITECH advocates using data-segmentation technologies to protect sensitive information in electronic health records. To promote data-segmentation technologies, the ONC's Office of the Chief Privacy Officer funded the Data Segmentation for Privacy Initiative (DS4P), which comprises experts such as software developers, healthcare providers, patient advocates, and health informaticists.

Figure 3 illustrates how the DS4P's approach to data segmentation works in the example of super sensitive health information such as substance abuse patient records, which are subject to the strictest requirements for data privacy (Office of the National Coordinator for Health Information Technology 2014b). The example shows how disclosing the patient's electronic substance abuse records is facilitated by tagging the data elements the patient authorized for disclosure. The example also shows how re-disclosure is restricted to comply with state and federal law.

The graphics below illustrate how the DS4P Initiative's approach to data segmentation can work in the example of substance abuse patient records.

1. The patient receives care at her local hospital ("Provider/Healthcare Organization 1") for various conditions, including substance abuse as part of the hospital's Alcohol/Drug Abuse Treatment Program (ADATP).
2. As required by 42 CFR Part 2, Provider/Healthcare Organization 1 captures and records the patient's consent to share her substance abuse patient records with another provider involved in her care ("Provider/Healthcare Organization 2").
3. A clinical workflow event triggers the disclosure of the patient's substance abuse patient records to Provider/Healthcare Organization 2. This disclosure has been authorized by the patient, so DS4P technology tags a Consolidated-Clinical Document Architecture (CCDA) (or individually disclosed data element) with an indication that the document is restricted and cannot be redisclosed without obtaining the patient's consent.
4. Provider/Healthcare Organization 2 uses DS4P technology, so it is able to electronically receive and incorporate the patient's substance abuse patient records. Using the data classification labels, it can implement a Prohibition on Redisclosure Notice.

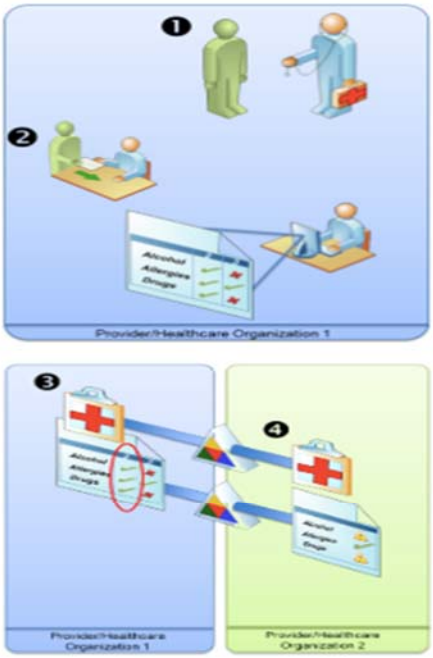

Figure 3. How Data Segmentation Works (Office of the National Coordinator for Health Information Technology, 2015a)

Overall, segmentation models can exist at the patient, individual, and organizational level (Goldstein et al., 2010). Hybrid models also exist.

4.6.4 De-identifying PHI

HIPPA contains no restrictions on using or disclosing de-identified health information. For organizations that use patient data for research, policy assessment, statistical analysis, and other endeavors, compliance with HIPAA's privacy rule requires that they de-identify the patient data before use. The process of de-identifying data (in which one removes identifiers) mitigates privacy risks to individuals and helps various systems use the data. The law states that healthcare organizations do not need a patient's authorization to use PHI once they de-identify the data in accordance with HIPPA's de-identification standards and implementation specifications. According to these standards, two ways to de-identify information exist: 1) using an expert, which involves a qualified statistician's determination that the PHI is not individually identifiable; or 2) removing specified identifiers of the individual and of the individual's relatives, household members, and employers. The latter approach is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

HIPAA permits covered entities to re-identify de-identified data provided that the re-identification method does not use the individual's information to perform the re-identification process. Also, the covered entity should not use or disclose the code or other means of record identification for any other purpose and should not disclose the mechanism for re-identification. In fact, the privacy rule considers the code and means of record identification used in the re-identification process as PHI and, thus, protects such information. However, one must take care when using an expert to de-identify data because researchers have demonstrated that one can de-anonymize previously de-identified data (Sweeney & Yoo, 2015). Indeed, researchers have developed the capacity to combine information in particular ways to identify health information (U.S. Department of Health and Human Services, 2012). However, even though covered entities may know about these re-identification methods, they are not prohibited from sharing de-

identified data unless they have knowledge that the intended recipient has the capability to re-identify the data. Under HIPAA's privacy rule, covered entities do not have to assume that all recipients would have the capacity to use these methods to re-identify information shared with them (U.S. Department of Health and Human Services, 2012).

In general, managing PHI's authorization, use, and disclosure places substantial administrative requirements on the healthcare IS organization. These administrative requirements have implications for how healthcare organizations design, implement, and use IS. As such, the administrative requirements for the privacy, security, and breach notification rules become pertinent. In Section 5, I discuss these administrative requirements.

5 HIPAA's Privacy, Security & Breach Notification Rules' Administrative Requirements

5.1 The Privacy Rule's Administrative Requirements

The HIPAA privacy rule has nine administrative requirements. The seven most relevant administrative requirements for health IS professionals include:

1. Developing and implementing privacy policies and procedures consistent with the privacy rule.
2. Designating privacy personnel (including a privacy official) responsible for developing and implementing privacy policies and procedures and a contact person or office responsible for receiving complaints and providing persons with information on the organization's privacy practices.
3. Training and managing the workforce.
4. Mitigating against harms that occur if the workforce or business associates wrongfully disclose information.
5. Implementing data safeguards, which includes reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI. These data safeguards should limit the PHI's incidental use and disclosure that may occur pursuant to the permitted or required use or disclosure of the PHI. For example, such safeguards might include shredding documents containing PHI before discarding them, securing medical records with a lock and key or pass code, and limiting access to keys or pass codes.
6. Implementing procedures and designating personnel to address complaints.
7. Documenting and retaining records: a covered entity must maintain (until six years after the date of their creation or last effective date—whatever comes last) its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions, activities, and designations that the privacy rule requires.

5.2 The Security Rule's Administrative Requirements

The security rule's administrative requirements are particularly important for health IS departments. These requirements include administrative, physical, and technical elements (U.S. Department of Health & Human Services, 2003b).

5.2.1 Administrative Safeguards

1. **Security management process:** the security rule requires a covered entity to identify and analyze potential risks to e-PHI, and it must implement security measures that reduce risks and vulnerabilities to a reasonable and appropriate level.
2. **Security personnel:** a covered entity must designate a security official who is responsible for developing and implementing its security policies and procedures.
3. **Information access management:** the security rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user's or recipient's role (role-based access).
4. **Workforce training and management:** a covered entity must appropriately authorize and supervise workforce members who work with e-PHI. A covered entity must train all workforce

members regarding its security policies and procedures and must have and apply appropriate sanctions against workforce members who violate its policies and procedures.

5. **Evaluation**: a covered entity must periodically assess how well its security policies and procedures meet the security rule's requirements.

5.2.2 Physical Safeguards

1. **Facility access and control:** a covered entity must allow only authorized access to its physical facilities.
2. **Workstation and device security:** a covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media. A covered entity must have policies and procedures about transferring, removing, disposing, and re-using electronic media to ensure appropriate protection of e-PHI.

5.2.3 Access Control

1. **Access control**: the security rule requires that a covered entity implement technical policies and procedures that allow only authorized persons to access e-PHI.
2. **Audit controls:** a covered entity must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use e-PHI.
3. **Integrity controls:** a covered entity must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. A covered entity must implement electronic measures to confirm that e-PHI has not been improperly altered or destroyed.
4. **Transmission security:** a covered entity must implement technical security measures that guard against unauthorized access to e-PHI that it transmits and receives over an electronic network.

5.3 The Breach Notification Rule's Administrative Requirements

Covered entities and business associates must demonstrate that they provided all required breach notifications to affected individuals, government entities, and the media or that a use or disclosure of unsecured PHI did not constitute a breach. This requires that a covered entity or business associate maintain documentation that all required notifications or that it did not need to make any notifications to affected parties. The documentation should include:

1. A risk assessment demonstrating a low probability that the impermissible use or disclosure has compromised the PHI, or
2. The application of any other exceptions to the definition of "breach".

Covered entities must have written policies and procedures about breach notifications, must train employees on these policies and procedures, and must develop and apply appropriate sanctions against workforce members who do not comply with these policies and procedures.

In addition to ensuring that organizations use information technology infrastructure that facilitates their compliance with federal and state legal and regulatory requirements, healthcare entities also need to implement sound information governance. In Section 6, I review information governance approaches in healthcare organizations.

6 Information Governance

Drawing from various definitions (e.g., Gartner's and ARMA International's), the American Health Information Management Association (AHIMA) defines information governance as an organization-wide framework for managing information throughout its lifecycle (AHIMA, 2014). This framework supports an organization's strategy, operations, regulatory, legal, risk, and environmental requirements (AHIMA, 2014). Information governance entails:

> *the specification of decision rights and an accountability framework to ensure appropriate behavior in the valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.* (Gartner, 2015)

Evidently, information governance is not the same as information technology (IT) governance. IT governance refers to the processes that ensure that an organization effectively and efficiently uses IT to achieve its goals (Gartner, 2015). As such, organizations may view IT governance in terms of the demand and supply of IT. Demand-side IT governance reflects what the IS organization should work on. It is the process by which organizations ensure that they effectively evaluate, select, prioritize, and fund competing IT investments; oversee their implementation; and extract measurable business benefits. Demand-side IT governance is a process that involves making and overseeing decisions about business investments in IT and is a business management responsibility. Supply-side IT governance reflects best practices on how the IS organization should operate. Supply-side IT governance focuses on ensuring that the IS organization operates in an effective, efficient, and compliant fashion, and it is primarily a CIO's responsibility.

Information governance is a strategic imperative for the healthcare industry (Knight & Stainbrook, 2014). The rapid rate of health IT's adoption, the demand for health information to measure quality and performance outcomes in healthcare delivery, and the need for using clinical and financial data in decision making drive the need for information governance in healthcare. As such, professional organizations such as AHIMA have made efforts to motivate healthcare organizations to focus on implementing sound information governance. However, a survey AHIMA and Cohasset Associates conducted in 2014 shows that only 43 percent of healthcare organizations had initiated an information governance program. The survey also revealed that healthcare organizations believed that the most important factor driving information governance programs is regulatory compliance.

A healthcare organization's credibility and legal standing rest on its ability to demonstrate that it conducts its activities in a lawful manner and manages information risks effectively. The absence of information or poor-quality information may damage an organization's credibility, impair its standing in legal matters, or jeopardize its ability to conduct business. Therefore, the health IS professional should assist the organization to identify what information it should enter into its records to demonstrate it conducts its activities in a lawful manner. The organization should ensure that their personnel enter that information into its records in a manner consistent with laws and regulations and that it maintains the information in the manner and for the time prescribed by law or organizational policy. It should also develop internal controls to monitor adherence to rules, regulations, and program requirements and, thereby, assess and ensure compliance.

Healthcare organizations must comply with applicable legal and regulatory requirements for maintaining and managing health information and other types of organizational information. Laws governing privacy and confidentiality, fraud, and abuse are particularly important to healthcare organizations. The health IS professional should understand the federal and state laws and regulations governing health information, which include retention/destruction laws, privacy and security laws and regulations, reimbursement regulations (e.g., meaningful use), risk management (both clinical and business-related), and litigation/e-discovery processes (i.e., release of information and legal holds).

In Section 6.1, I focus on the legal issues that make information governance critical for the healthcare organization. In particular, when healthcare organizations are involved in a lawsuit, they might need to provide data to the opposing side to facilitate trial preparation. This duty raises requirements about how organizations manage data and the subsequent information governance policy. As such, in Sections 6.2 to 6.3, I discuss e-discovery, the legal duty to preserve healthcare data, retention policies, and a defensible destruction policy. These are all critical components of information governance for the healthcare organization.

6.1 E-discovery

In the legal context, discovery refers to those devices and tools that one side of a lawsuit uses to obtain facts and information about the case from the other side to prepare for trial (McWay, 2010). E-discovery refers to when a party seeks electronically stored information (ESI) through discovery.

6.1.1 Challenges

For the healthcare organization, ESI raises significant challenges not present with conventional, paper-based records. These challenges include the format in which organizations must produce ESI so that one can search and read it easily, the potential undue burden in terms of time and expense in carrying out the discovery process, the existence of potentially hidden metadata, and the need to preserve ESI and not

destroy nor delete it inadvertently. Organizations may also be concerned that producing ESI will result in waiving the attorney-client privilege, which protects and keeps confidential certain information shared between the attorney and the client. Table 1 elaborates on the different ways in which ESI differs from paper information.

Table 1. How ESI Differs from Paper Information (McWay, 2010)

Volume	Use of electronic programs, databases, and devices results in a large number of potentially relevant documents to review.
Variety of sources	One electronic document may reside in multiple places.
Dynamic quality	The ability to change or mutate data.
Hidden information	Metadata and embedded data.
Reliance on systems	Complex ESI may only be comprehensible and usable if not separated from the system that created it.
Deletion	ESI may be recovered from multiple sources even if deleted from the medium in which it was originally stored.

Producing ESI may also result in waiving the attorney work-product privilege. The attorney work-product privilege dictates that an opposing party generally may not discover or compel one to disclose written or oral materials prepared by or for an attorney in the course of legal representation.

Record retention also raises concerns about e-discovery costs, which increase with the size and complexity of data repositories. Electronic health records are advantageous because they do not require as much physical storage space as paper records. Thus, healthcare providers often retain ESI longer than statute or regulation requires. This approach can result in massive amounts of information that healthcare providers must search and produce in response to discovery requests. Thus, organizations should cautiously retain health records beyond the required periods based on their medical and administrative needs and their fiscal, technological, and storage constraints.

6.1.2 Legal Duty to Preserve Data

The healthcare organization has a legal duty to preserve ESI within the legally required retention periods even though it might be costly. However, preserving ESI is difficult in practice. ESI by its nature is dynamic and changeable. Routine computer operations may require parties to overwrite data, delete emails, and recycle backup tapes as a part of an organization's regular business practices. Thus, organizations need to balance the need to preserve ESI against the need to continue critical, routine computer operations.

In the event of a lawsuit, parties attempt to preserve ESI by either issuing a litigation hold or obtaining a preservation order (McWay, 2010). A litigation hold refers to the actions of a party who possesses data to make efforts to prevent routine destruction and preserve the ESI that may be discoverable even before a lawsuit has been filed. This duty arises when a party becomes aware that they may have evidence that could be relevant to potential litigation. The opposing party may trigger an adversary's duty to issue a litigation hold by advising them of their intent to file a lawsuit or by sending a notice of preservation. A notice of preservation is a letter notifying an adversary that it needs to preserve relevant electronic evidence. A court may also order a party to preserve electronic and other evidence by issuing a preservation order.

Spoliation is another pertinent e-discovery issue. Spoliation refers to wrongfully destroying or altering evidence or failing to preserve property or data for another's use as evidence in pending or reasonably foreseeable litigation. The central question that determines spoliation is whether the party who destroyed or altered the information had reason to know not to do so. Spoliation is a discovery violation and subject to sanctions. For example, in *Zubake v. UBS Warburg, LLC*, the court found Warburg's actions in deleting relevant emails and not preserving backup tapes to be discovery violations. The court awarded Zubake US$29.2 million in damages.

Courts deal considerably in managing e-discovery requests. Parties often dispute many areas of e-discovery including its scope, parties' obligations to preserve information, whether certain information is privileged, and how information should be produced. Courts often need to resolve these e-discovery disputes.

6.2 Retention Requirements

The unavailability of a health record can result in lawsuits for the negligent loss of records or spoliation if they are destroyed and not available within state and federal record retention requirements. Thus, healthcare organizations need to develop retention policies to facilitate compliance with legal, regulatory, tax and business requirements. No single framework dictates how an organization should design its retention policy. Myriad laws, regulations, and accreditation and professional guidelines provide guidance to the healthcare organization on how to develop appropriate retention policies. For instance, at the federal level, the HIPAA privacy rule does not include medical record retention requirements (U.S. Department of Health and Human Services, 2009). Nonetheless, the HIPAA privacy rule does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other PHI for whatever period they maintain such information. The HIPAA privacy rule also requires that covered entities protect healthcare records when disposing and destroying such records. The Centers for Medicare and Medicaid Services (CMS) requires that organizations retain patient records for Medicare beneficiaries for a five-year period (Center for Medicare & Medicaid Services, HHS, 2008). Medicaid requirements may also vary by state. HIPAA also requires that organizations retain records showing HIPAA compliance for six years.

Each state may have unique medical record-retention laws that vary by setting or type of record. In addition, payers and regulatory or accrediting agencies may have regulations governing record retention. Organizations should know all applicable regulations and abide by the most stringent. Professional organizations often offer guidance on record-retention policies. For instance, AHIMA recommends a ten-year retention period for adult patient records (measured from the date of the patient's last healthcare encounter).

The healthcare organization might be tempted to retain data forever to guard against spoliation. However, others can use data retained for excessive periods as evidence against the organization in the event of a lawsuit. Therefore, it might not be best to keep data beyond its retention period. As a result, the healthcare organization must create effective record-retention policies. These policies determine the length of time the healthcare provider should maintain health records. The organization must develop a record retention schedule to detail what data it will retained, the retention period, and the manner in which it will store the data.

Though not a healthcare case, a well-known example of record disposition that caused unintended consequences is the famous Arthur Andersen/Enron case (Kinsler, 2008). The courts convicted the accounting firm, Arthur Andersen, for obstructing justice based on the destruction of Enron-related documents between October 16 and November 9, 2001. During that time, Arthur Andersen's in-house lawyer acknowledged that a Securities Exchange Commission (SEC) investigation was "highly probable", but she nevertheless advised Andersen's personnel to shred Enron's documents. Although the Supreme Court subsequently reversed Andersen's conviction, the impact of the scandal and the findings of criminal complicity destroyed the firm.

Thus, the healthcare organization must protect itself from liability from a spoliation suit by developing a defensible destruction policy. The defensible destruction policy aims to ensure that the organization properly and legally disposes information the organization no longer needs.

6.3 Defensible Destruction Policy

An organization may destroy medical records in the ordinary course of business or due to a provider's closure. However, if a healthcare organization destroys data that it may need in the future for legal reasons, they may face legal action for spoliation. The best defense against a spoliation suit is a defensible destruction policy. Defensible deletion refers to the process of disposing information that an organization no longer needs for business or legal reasons in the framework of its overall information-governance strategy. Record-destruction policies should address the controlling statutes or regulations that may specify or recommend the destruction method such as shredding, burning, or recycling. Some laws may require the healthcare organization to create an abstract of patient data before destroying the patient record. State laws may require the facility to notify the patient or the licensing authority before destroying the patient record.

The HIPAA security rule also establishes policies for destroying PHI. As a general rule, one may destroy data only after the retention period has expired using only those methods specified in an information

governance or security policy. The organization may destroy PHI internally or use a commercial contractor. The paramount concern, however, is keeping the contents of the record confidential when destroying the data in compliance with the HIPAA privacy rule. Also, the healthcare organization should retain a certificate of destruction that shows what data and records it destroyed, who specifically destroyed these data, and the destruction method. Failure to retain a certificate of destruction opens up the organization to claims that it destroyed an individual record for suspicious reasons such as to obtain an advantage in a lawsuit.

The following federal court decision provides a good example of how a company can defensibly delete data that it no longer needed. The *In Re Pradaxa (Dabigatran Etexilate) Products Liability Litigation* (2013) case was a class action product liability claim against the defendant, Boehringer Ingelheim, for the widely prescribed blood-thinner Pradaxa. The plaintiffs alleged that Pradaxa caused potentially fatal internal bleeding. During the case, the plaintiffs filed a motion to compel the defendant to produce emails and documents that the former vice president of marketing prepared about the litigation. The plaintiffs sought an adverse inference jury instruction for spoliation and alleged that the defendant had destroyed those emails and documents. When a judge issues an adverse inference instruction to the jury, the judge informs the jury that someone did not produce evidence or that someone spoiled the evidence so that it could not be brought to court to hurt their case. The defendant, Boehringer Ingelheim Pharmaceuticals (BIPI), explained that it had destroyed the requested documents in accordance with the company's record-retention policies and no longer had the documents. The trial court concluded that BIPI destroyed the former vice president's documents according to its document retention policies and that BIPI was not under a duty to preserve these documents when BIPI acted in conformance with its retention policies. In the end, the court held that BIPI did not spoliate evidence and that the plaintiffs were not entitled to an adverse inference instruction.

As such, we can see that health IS professionals must ensure that they establish policies and procedures that govern the discovery of paper and electronic materials in concert with IS professionals, legal counsel, risk management staff, and senior management. In turn, these policies and procedures should be communicated to all members of the healthcare organization who possess responsibility for e-discovery.

To prepare an organization for e-discovery, the health IS professional must realize that no one scheme exists that addresses all of the issues. Organizations must carefully review and apply the legal and quasi-legal requirements including those that accrediting and institutional standards and professional guidelines require to one's specific context. Organizations should then integrate these legal and quasi-legal requirements into an information-governance policy that balances the organization's ability to maintain adequate information for the organization to function; comply with laws, regulations, and professional and accreditation guidelines; and manage storage constraints and costs.

In Section 7, I summarize the legal and regulatory implications for designing and implementing IS and highlights the main research issues.

7 Legal & Regulatory Requirements for Health IT

Health IT legislation and regulation impose several requirements on the healthcare organization for designing, implementing, and managing healthcare IS. These requirements center on privacy, security standards, and information governance. Several organizations have developed privacy and security standards and frameworks for the U.S. healthcare industry. For example, many organizations in the U.S. healthcare industry adopted the Health Information Trust Alliance's (HITRUST) common security framework (CSF). Developed in collaboration with healthcare and information security professionals, the CSF integrates healthcare regulations and standards into a single security framework. Table 2 summarizes the security requirements, and Table 3 summarizes the privacy requirements that HITRUST recommends for healthcare organizations (HITRUST Alliance, 2015).

Many research avenues emerge as a result of these legal and regulatory requirements. For instance, cybersecurity breaches affect the healthcare industry significantly. IS researchers could determine the socio-technical factors that make healthcare more vulnerable to cybercrime than any other industry. One could explore the security risks inherent in EHRs, HIEs, mobile, and wearable technology. One could also assess the institutional factors contributing to the healthcare industry's readiness to prevent data breaches and to comply with HIPAA's Breach notification rule.

IS researchers could also conduct research on patient-consent systems. Research issues include developing and examining approaches for designing meaningful patient-consent procedures and mechanisms for recording patients' consent preferences, designing systems to educate and engage the cognitively impaired and illiterate patient, and designing systems to implement restrictions on disclosures of protected health information.

Table 2. Legal and Regulatory Requirements for Designing, Implementing, and Managing Health IS—Security (HITRUST Alliance, 2015)

Information security management program	Document an information security management program that addresses the organization's overall security program including monitoring, maintenance, and improvement.
Access and audit controls	Implement an access-control policy to control access to information, information assets, and business processes, including access HIEs provide to employees of all connecting organizations. Secure PHI through data encryption and use firewalls to filter traffic and restrict access to systems. Implement auditing and monitoring capabilities.
Human resources	Define security roles and responsibilities of employees, contractors, and third party users. Carry out relevant background checks. Terms and conditions of employment shall include responsibilities for information security. Employees should undergo information security awareness, education, and training. Institute a formal disciplinary process for employees who have violated security policies and procedures. Implement employee termination procedures to terminate access rights and return the organization's information assets.
Risk management	Develop and implement a risk management program that addresses risk assessments, risk mitigation, and risk evaluations. Consider actions to take when a breach of PHI occurs.
Security policy	Develop, publish, disseminate, and continuously review the information security policy in line with business objectives and relevant laws and regulations, including a strategic plan and a security program with well-defined roles and responsibilities.
Organization of information security	Implement an internal information security organization and provide the resources needed for information security. Appoint a senior level information security official, ensure that the organization's information security processes and structures are in place, and ensure that representatives from different parts of the organization with relevant roles and job functions coordinate information security activities. Implement an identity theft-prevention program and requirements for confidentiality agreements. Facilitate an independent review of information security.
Compliance	Ensure that the design, operation, use, and management of IS adheres to applicable laws; statutory, regulatory, or contractual obligations; and security requirements.
Asset management	Clearly identify all information assets, document the importance of these assets, and maintain an inventory. Maintain all information on assets needed to recover from a disaster.
Physical and environmental security	Prevent unauthorized physical access, damage, and interference to the organization's premises and information.
Communications and operations management	Document, maintain, and make available operating procedures to all users who need them and secure them against unauthorized access.
Information systems acquisition, development, and maintenance	Ensure that security is an integral part of new IS and business requirements for new information systems, enhancements, and software packages. Address information security and privacy in all phases of the project management methodology.
Information security incident management	Handle information security events and weaknesses associated with IS in a manner that allows the organization to take timely corrective action.
Business continuity management	Implement strategies and plans to counteract business interruptions, protect critical business processes from information systems failures, and ensure their timely resumption. Test and update business continuity plans.

Developing a theoretical perspective of the behavioral issues underlying the use of patient consent-management systems such as users' trust and distrust and patient's privacy beliefs are also important research issues. Further, health IT developers should consider how to build data segmentation functionality into their products to facilitate e-consent. In turn, IS researchers need to evaluate the effectiveness of these approaches and how organizations use them.

Table 3. Legal and Regulatory Requirements for Designing, Implementing, and Managing Health IS—Privacy (HITRUST Alliance, 2015)

Privacy organization	Appoint a senior privacy officer. Implement technical and physical safeguards to prevent staff from intentionally or unintentionally using or disclosing PHI. Assure individuals' privacy and security through appropriate contracts, monitoring, and other means to report and mitigate non-adherence and breaches. Implement breach-notification procedures. Assess adherence to the privacy rule.
De-identification	De-identify data as required when using PHI for research, policy assessment, statistical endeavors, and other uses outside of treatment, payment, and healthcare operations.
Authorization & disclosure of PHI	Create openness and transparency about policies, procedures, and technologies that directly affect individuals and their identifiable health information including notice of privacy practices, managing and documenting the use and disclosure of patient authorization, and requests for restriction of the use and disclosure of patient PHI. Develop patient consent management systems and meaningful patient consent procedures and mechanisms. Develop policies to respond to legal and other requests to disclose PHI. Institute auditing and monitoring capabilities.

Table 4 summarizes the key factors healthcare organizations should consider when implementing information governance. Overall, information governance programs are less prevalent and less mature in healthcare organizations than needed (Knight & Stainbrook, 2014). Most healthcare organizations have not yet established a comprehensive strategy for information governance. Similarly, the IS research community has conducted little research on information governance in the healthcare industry. We need theoretically grounded studies that explore how organizations implement information governance frameworks. We also need to carry out studies that explain the business value of information governance, organizational change, and risk management as organizations implement information governance policies. Studies that identify the drivers and inhibitors of legal and regulatory compliance will provide valuable lessons for IS researchers and practitioners.

Researchers could also study the predictive disposition of healthcare records, which includes automated methods for healthcare record management. Software solutions that manage record retention and legal hold policies do exist. To automatically dispose medical records in a defensible manner, record-management applications must have the ability to understand the meaning in unstructured content so that it classifies content to meet the organization's retention policies appropriately. Thus, such research could develop IS management practices and solutions that move organizations away from manual, employee-based information governance to automated methods that automatically apply retention policies, protect content on litigation hold, and dispose of content according to a defensible destruction policy. However, the sensitivity and confidentiality of an organization's legal affairs may make such studies difficult to execute.

The U.S. Government's health IT initiative, which motivated the wide-scale implementation of EHRs and HIEs, is one of the most complex and transformative suite of IS projects to engage an entire nation. Empirical studies that examine the process of implementing the meaningful use of health IT and national HIEs and the effectiveness of the organizational structures, governance and project management processes that support this initiative will provide useful lessons for researchers and practitioners in and outside the health IS community. We also need to understand the barriers and drivers of HIE interoperability. Assessments of whether the U.S. government achieved the health IT policy goals set out in its legislation, and the unintended consequences, are fruitful avenues of research. We also need to understand the role of health IT legislation in facilitating a nation's health IT transformation.

Table 4. Legal and Regulatory Requirements for Designing, Implementing, and Managing Health IS—Information Governance

Information governance organization	Form a multi-disciplinary team to oversee the information governance function and to develop the legal health record policy. Implement employee, business associate, and third party confidentiality agreements to protect patients PHI. Train the workforce on how to handle PHI.
Legal health record policy	Develop the legal health record policy to determine the healthcare organizations' legal health records and to ensure integrity for legal and business purposes. Define the legal health record and HIPAA's designated record set.

Table 4. Legal and Regulatory Requirements for Designing, Implementing, and Managing Health IS—Information Governance

Sharing information and health records	Develop policies and procedures to address the sharing, acceptance, and retention of electronic and paper information received from external facilities including via health information exchanges.
Record completion/ lockdown	Develop policy to determine when the health record is completed and should be locked to prevent further editing and amendment.
Amendments & corrections	Policies should address when and how amendments and corrections to the health record should be made. Retractions should also be addressed.
Authentication	Systems should automatically record the name and credentials of the person documenting patient care and the date and time. Accommodations should be made for situations where multiple persons document the entry. The systems should accommodate electronic signatures for documents, including transcribed documents and scanned images. Develop a policy for documents requiring co-signatures. Put auditing and monitoring capabilities in place.
Versions	Develop a policy to manage document versions and decide whether all versions or just the final document will be kept. There are significant legal implications if changes are made to a document and the original version is unavailable.
Metadata	Be aware of and document metadata and develop policy on retention period for metadata.
Record retention and destruction	Develop defensible record destruction policy to protect the organization against spoliation lawsuits. Categorize organization records and determine retention periods in accordance with statutory requirements. Develop policies for outsourcing and destroying records to protect the privacy of individuals and to protect the organization against lawsuits for spoliation. Maintain certificates of destruction that identify the records destroyed and the dates and times of record destruction. Put auditing capabilities in place. Develop policies to place litigation holds on organizational records and to respond to third-party notices and orders of preservation to preserve organizational records.
e-Discovery	Establish and communicate policies and procedures that govern the discovery of paper and electronic materials to members of the healthcare organization who possess responsibility for e-discovery.

8 Conclusion

This paper explores the legal issues that impact the design, implementation, and use of health IT. Motivated by the legal and regulatory issues that impact health IT, the paper also suggests research issues for the IS research community to consider. Health IT legislation will continue to transform health IT. As organizations comply with health IT legislation and as health IT evolves, we need to empirically understand the impacts and develop new IS tools and IS-management practices. I hope this paper will entice health IS researchers to approach health IS research through a legal and regulatory lens to address some of these issues.

References

AHIMA. (2011). Fundamentals of the legal health record and designated record set. *Journal of AHIMA, 82*(2). Retrieved from http://library.ahima.org/doc?oid=104008#.V2rUi1fp5g8

AHIMA. (2014). Information governance: Principles for health care. Retrieved from http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx

Brodnik, M. S., Rinehart-Thompson, L. A., & Reynolds, R. B. (2012). *Fundamentals of law for health informatics and information mangement* (2nd ed.). Chicago, Illinois: American Health Information Management Association.

Centers for Medicare & Medicaid Services, HHS. (2008). *Condition of participation: Medical record services.* 42 CFR § 482.24 (c)(2)(v).

Dullabh, P., Adler-Milstein, J., Hovey, L., & Jha, A. K. (2014). *Key challenges to enabling health information exchange and how states can help.* Chicago, IL: NORC.

Experian. (2015). *2015 second annual data breach industry forecast.*

Gabriel, M., Charles, D., Henry, J., & Lee-Wikins, T. (2015). *State and national trends of two-factor authentication for non-federal acute care hospitals*. *HealthIT.gov.* Retrieved from http://dashboard.healthit.gov/evaluations/data-briefs/hospital-two-factor-authentication.php

Gartner. (2015). *IT glossary.* Retrieved from http://www.gartner.com/it-glossary/?s=information+governance

Goldstein, M., Rein, A., Heesters, M. M., Hughes, P. P., & Williams, B. (2010). *Data segmentation in electronic health information exchange: Policy considerations and analysis*. Washington, DC: U.S. Department of Health and Human Services.

Harmonizing State Privacy Law Collaborative. (2009). *Health information security and privacy collaboration.* Retrieved from https://www.healthit.gov/sites/default/files/hspl_1_final_rpt.pdf

HITRUST Alliance. (2015). *HITRUST common security framework.* Retrieved from https://hitrustalliance.net/content/uploads/2014/07/HITRUST-2014-CSF-v6.1-v1.pdf

Identity Theft Resource Center. (2015). *Identity Theft Resource Center breach report hits near record high in 2015.* Retrieved from http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html

In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation, no. 3: 12-md-02385-drh-scw (s.d. ill. aug. 9, 2013).

Kinsler, J. S. (2008). Arthur Andersen and the temple of doom. *Southwestern University Law Review, 37*, 97-134.

Knight, K., & Stainbrook, C. (2014). *Benchmarking white paper: Information governance in health care*. Minneappolis, MD: Cohasset Associates.

McWay, D. C. (2010). *Legal and ethical aspects of health information management* (3rd ed.) New York, NY: Cengage.

National Alliance for Health Information Technology. (2008). *Defining key health information technology terms.* Retrieved from https://www.nachc.com/client/Key%20HIT%20Terms%20Definitions%20Final_April_2008.pdf

Office of the National Coordinator for Health Information Technology. (2011a). *Customizing EHR implementation to capture patient and clinical information for quality measurement and reporting*. Retrieved from https://www.healthit.gov/providers-professionals/multnomah-county-health-department-case-study

Office of the National Coordinator for Health Information Technology. (2011b). *Rural health clinic exchanges information with hospitals and physicians for improved coordination of care*. Retrieved from https://www.healthit.gov/providers-professionals/rural-health-clinic-exchanges-information-hospitals-and-physicians-improved-

Office of the National Coordinator for Health Information Technology. (2011c). *Solo family practitioner demonstrates care coordination with referring physicians.* Retrieved from https://www.healthit.gov/providers-professionals/brull-case-study

Office of the National Coordinator for Health Information Technology. (2012a). *Florida physician uses EHR for practice improvement effort*. Retrieved from https://www.healthit.gov/providers-professionals/florida-physician-uses-ehr-practice-improvement-effort

Office of the National Coordinator for Health Information Technology. (2012b). *No digital divide in this rural Kentucky practice.* Retrieved from https://www.healthit.gov/providers-professionals/no-digital-divide-rural-kentucky-practice

Office of the National Coordinator for Health Information Technology. (2013a). *Health information security & privacy collaboration (HISPC)*. Retrieved from https://www.healthit.gov/policy-researchers-implementers/health-information-security-privacy-collaboration-hispc

Office of the National Coordinator for Health Information Technology. (2013b). *How to attain meaningful use*. Retrieved from https://www.healthit.gov/providers-professionals/how-attain-meaningful-use

Office of the National Coordinator for Health Information Technology. (2014a). *eConsent toolkit*. Retrieved from https://www.healthit.gov/providers-professionals/econsent-toolkit

Office of the National Coordinator for Health Information Technology. (2014b). *Enabling privacy: Data segmentation*. Retrieved from https://www.healthit.gov/providers-professionals/data-segmentation-overview

Office of the National Coordinator for Health Information Technology. (2014c). *Health information exchange: Standards & interoperability.* Retrieved from http://healthit.gov/providers-professionals/standards-interoperability

Office of the National Coordinator for Health Information Technology. (2014d). *Health information exchange: What is a health information exchange?* Retrieved from http://healthit.gov/providers-professionals/health-information-exchange/what-hie

Office of the National Coordinator for Health Information Technology. (2014e). *State health information exchange cooperative agreement program.* Retrieved from https://www.healthit.gov/policy-researchers-implementers/state-health-information-exchange

Office of the National Coordinator for Health Information Technology. (2014f). *Enabling privacy: Data Segmentation.* Retrieved from https://www.healthit.gov/providers-professionals/data-segmentation-overview

Office of the National Coordinator for Health Information Technology. (2015a). *Hospitals participating in the CMS EHR incentive programs.* Retrieved from http://dashboard.healthit.gov/quickstats/pages/FIG-Hospitals-EHR-Incentive-Programs.php

Office of the National Coordinator for Health Information Technology. (2015b). *Meaningful use definitions & objectives.* Retrieved from https://www.healthit.gov/providers-professionals/meaningful-use-definition-objectives

Sweeney, L., & Yoo, J. S. (2015). *De-anonymizing South Korean resident registration numbers shared in prescription data*. *Technology Science*.

Texas Health Services Authority. (2012). *Texas consent management services whitepaper*. Retrieved from http://hietexas.org/component/docman/doc_download/387-thsa-consent-management-services-white-paper

The American Telemedicine Association. (2012). *What is telemedicine*. Retrieved from http://www.americantelemed.org/about-telemedicine/what-is-telemedicine

U.S. Department of Health & Human Services. (2003a*). Summary of the HIPAA privacy rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/p rivacysummary.pdf

U.S. Department of Health & Human Services. (2003b). *Summary of the HIPAA security rule*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummar y.html

U.S. Department of Health and Human Services. (2002). *Minimum necessary requirement*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.html

U.S. Department of Health and Human Services. (2009). *The HIPAA privacy and security rules: Frequently asked questions about the disposal of protected health information*. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/disposalfaqs.pdf

U.S. Department of Health and Human Services. (2012). *Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule*. Retrieved from http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

Washington, L. (2010). From custodian to steward: Evolving roles in the E-HIM transition. *Journal of AHIMA, 81*(5), 42-43.

Glossary

Attorney-client privilege: a rule that protects certain information shared between the attorney and the client and keeps that information confidential.

Attorney work-product privilege: a rule that an opposing party generally may not discover or compel disclosure of written or oral materials prepared by or for an attorney in the course of legal representation, especially in preparation for litigation.

Business associate: a person or entity that a covered entity engages to perform certain functions or activities that involve using or disclosing protected health information on behalf of the covered entity. A member of the covered entity's workforce is not a business associate. A covered healthcare provider, health plan, or healthcare clearinghouse can be a business associate of another covered entity.

Clinical decision support: health IT functionality that builds on the foundation of an EHR to provide persons involved in care processes with general and person-specific information intelligently filtered and organized at appropriate times to enhance health and healthcare.

Conflict of laws: where the statutes of different states do not agree on the same legal issue, a conflict of laws arises.

Consumer mediated exchange: has the ability for patients to aggregate and control the use of their health information among providers.

Covered entities: covered entities include health plans, healthcare clearinghouses, and any healthcare provider who transmits health information in electronic form in connection with transactions for which the secretary of HHS has adopted standards under HIPAA.

De-identified health information: information that neither identifies nor provides a reasonable basis to identify an individual.

Designated record set: a group of records maintained by or for a covered entity that may include patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

Directed exchange: the ability to send and receive secure information electronically between healthcare providers to support coordinated care.

Electronic health record: an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that authorized clinicians and staff across more than one healthcare organization can create, gather, manage, and consult.

Electronic medical record: an electronic record of health-related information on an individual that authorized clinicians and staff in one healthcare organization can create, gather, manage, and consult.

Healthcare operations: includes any of the following activities: a) quality assessment and improvement activities, including case management and care coordination; b) competency-assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; e) business planning, development, management, and administration; and f) business management and general administrative activities of the entity, including but not limited to de-identifying PHI, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Healthcare providers: every healthcare provider (regardless of size) who electronically transmits health information in connection with certain transactions is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA transactions rule. Using electronic technology, such as email, does not mean a healthcare provider is a covered entity; the transmission must be in connection with a standard transaction. The privacy rule covers a healthcare provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Healthcare providers include all providers of services (e.g., institutional providers such as hospitals) and providers of medical or health services (e.g., non-institutional providers such as physicians, dentists and other

practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for healthcare.

Health information exchange (HIE): a regional collaboration among independent healthcare organizations for sharing clinical information. Often, administrative information is shared as well.

Health plans: group plans that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations (HMOs), Medicare, Medicaid, Medicare Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. Two types of government-funded programs are not health plans: 1) those whose principal purpose is not providing or paying the cost of healthcare, such as the food stamps program; and 2) those programs whose principal activity is directly providing healthcare, such as a community health center, or the making of grants to fund the direct provision of healthcare. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance.

Hybrid health record: a record that contains both paper and electronic records and media such as film, video, or imaging systems and uses both manual and electronic processes. It is collected from multiple sources and used for a wide variety of purposes.

Incidental use and disclosure: the unavoidable use and disclosure that may occur pursuant to the permitted or required use or disclosure of the PHI.

Information governance: the specification of decision rights and an accountability framework to ensure appropriate behavior in valuating, creating, storing, using, archiving, and deleting information. It includes the processes, roles and policies, standards and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

Information technology (IT) governance: the processes that ensure the effective and efficient use of IT in enabling an organization to achieve its goals. Demand-side IT governance (what IT should work on) is the process by which organizations ensure they effectively evaluate, select, prioritize, and fund competing IT investments; oversee their implementation; and extract measurable business benefits. Demand-side IT governance is a business investment, decision making and oversight process, and it is a business management responsibility. Supply-side IT governance (how IT should do what it does) is concerned with ensuring that the IT organization operates in an effective, efficient, and compliant fashion, and it is primarily a CIO responsibility.

Legal health record: the legal health record is generated at or for a healthcare organization as its business record and is the record that would be released upon request. The legal health record is the documentation of healthcare services provided to an individual during any aspect of healthcare delivery in any type of healthcare organization.

Litigation hold: refers to the actions of a party who possesses data to make efforts to prevent routine destruction and preserve the electronically stored information (ESI) that may be discoverable even before a lawsuit has been filed. This duty is independent of whether the party has had a lawsuit filed against it and arises when a party becomes aware that they may have evidence that could be relevant to potential litigation.

Notice of preservation: a letter notifying an adversary of the need to preserve relevant electronic evidence even if paper copies are available.

Order of preservation: temporary court order to preserve electronic and other evidence.

Payment: encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for healthcare delivered to an individual. Also includes the activities of a healthcare provider to obtain payment or be reimbursed for providing healthcare to an individual.

Personal health record: the personal health record is an electronic record of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

Preemption: when for certain matters of national importance, federal law takes precedence or preempts state law.

Query-based exchange: the ability for providers to find and/or request information on a patient from other providers; often used for unplanned care.

Spoliation: the wrongful destruction or material alteration of evidence or the failure to preserve property or data for another's use as evidence in pending or reasonably foreseeable litigation. The central question of spoliation is whether the party who destroyed or altered the information had reason to know not to do so.

Treatment: the provision, coordination, or management of healthcare and related services for an individual by one or more healthcare providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.

About the Authors

Karlene C. Cousins is Associate Professor of Information Systems and Business Analytics in the College of Business at the Florida International University. Her research agenda is focused on (1) the examination of the effects of mobile computing environments on organizations and society; and (2) the legal and regulatory issues impacting the use and innovation of information systems. A licensed attorney, she has worked with IT companies on regulatory, data privacy and intellectual property issues. In academia, she is most known for her work in the empirical examinations of evolving work practices as a result of the capability of mobile technology to accommodate both work and life activities. She published articles in journals such as the *European Journal of Information Systems*, *Communications of the ACM*, *Decision Sciences* and *Journal of the AIS*.