

Implementing Privacy and Security Standards In Electronic Health Information Exchange

Patricia Gray, J.D., LL.M.

UNIVERSITY of **HOUSTON** | LAW CENTER
Health Law & Policy Institute

Prepared for the Texas Health and Human Services Commission and the
Texas Health Services Authority with support from the State Health
Information Exchange Cooperative Agreement Program

August 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY	3
INTRODUCTION	4
THE SECURITY RULE.....	5
SECURITY RULE STANDARDS AND IMPLEMENTATION SPECIFICATIONS	8
Administrative Safeguards	8
Physical Safeguards.....	9
Technical Safeguards	10
Organizational Requirements.....	11
HIPAA PRIVACY RULE AND PATIENT RIGHTS	12
Individual Rights and the Privacy Rule.....	12
Access, Disclosure, and Authorization	13
Patient Access and Right to Amend.....	14
Limiting Disclosure to Health Plans	15
Accounting for Disclosures and Access.....	15
Breach Notification	18
TEXAS LAW.....	20
82 nd Texas Legislature Update	21
OTHER FEDERAL PROVISIONS.....	24
Clinical Laboratory Improvements Amendments of 1988 (CLIA).....	25
Red Flags Rule	25
Family Educational Rights and Privacy Act (FERPA).....	25
Patient Safety and Quality Improvement Act Rules (42 CFR Part 3 Subpart C).....	26

Federally Funded Substance Abuse Treatment (42 C.F.R. Part 2)	27
Veterans Health Administration Health Information Privacy Requirements.....	28
KEY POLICY QUESTIONS.....	29
CONCLUSION.....	31

EXECUTIVE SUMMARY

Ensuring the privacy and security of patient health information requires a clear understanding of the concerns of various stakeholders as well as development of enforceable guidance that is feasible to implement and monitor. The HIPAA Privacy and Security Rules provide direction for policy makers to follow in working with those charged with the technical implementation of data security. The Privacy Rule addresses an individual's right to control use and disclosure of his or her protected health information (PHI); the Security Rule addresses the safeguards necessary to protect PHI from unauthorized access, use or disclosure.

The Security Rule only applies to PHI that is created, received, maintained or transmitted by a covered entity or its business associates in an electronic format. With the adoption of the HITECH amendments to HIPAA, it is now clear that HIEs may be considered business associates of covered entities under HIPAA. A major goal of the Security Rule is to protect the privacy of patient health information while simultaneously giving covered entities the flexibility to implement the policies and procedures that are appropriate to address patient privacy. The Security Rule addresses the confidentiality, integrity and availability of a patient's health information through implementation of administrative, physical and technical safeguards. The Security Rule safeguards are further defined by standards and implementation specifications. Individual rights to control access and use of their PHI include, with limited exceptions, the right to authorize such access and disclosure, the right to access and amend their own medical information, the right to obtain an accounting of access to, use and disclosure of their PHI, and the right to receive notice if their PHI is breached.

Both state and federal laws and regulations implicate the security and privacy of PHI. As laws are amended, new laws passed, and regulations evolve, it will be necessary to carefully monitor the changes in order to ensure the ongoing privacy and security of health data for the benefit of both patients and providers.

INTRODUCTION

Key Points

- Patients, providers and payers share some concerns about privacy and security of patients' health data, but each also has unique concerns.
- Policymakers must address the concerns that patients, providers and payers have about both the privacy and the security of patients' health information.

Ensuring the privacy and security of patient data is one of the most important elements in achieving successful implementation of electronic health information exchange. Privacy refers to an individual's right to control the disclosures and uses of their individually identifiable protected health information (PHI). Security refers to the administrative, physical and technical safeguards used to protect PHI from unauthorized access, use or disclosure. Although patients, providers and payers share many privacy and security concerns, each has specific concerns that may not be of as much concern to the others.

Patients' concerns center on the misuse of their data for others' commercial gain; revelation of sensitive health data that may result in embarrassment, compromise their personal safety, or otherwise be used in a discriminatory fashion; incorrect information in their medical records and the difficulty of accessing such records to correct the information; and loss of data in electronic systems. Patients are also concerned about medical identity theft and the ability of organizations to notify them of issues related to use of their records.¹

Both providers and payers have concerns related to costs of implementing and maintaining health information systems, usability of systems and maintaining regulatory compliance to ensure the safety and integrity of data in the system.² However, providers have some unique concerns regarding the sometimes conflicting impact of state and federal privacy laws, specific privacy laws governing control of sensitive health information such as HIV and mental health treatment, and potential liability issues related both to protection of health information and quality of care. Providers are also concerned about their ability to identify and resolve problems with quality of and access to data, and maintaining security of that data.³

This paper will address the legal requirements for providing and maintaining the security of a patient's PHI by those who have access to it. These requirements are primarily

¹ KRISTYN S. APPLEBY & JOANNE TARVER, *MEDICAL RECORDS REVIEW* § 1.9 (Aspen 4th ed. 2010).

² *Id.*

³ *Id.*

found in the Health Insurance Portability and Accessibility Act (HIPAA) Privacy Rule and Security Rule, as amended by provisions of the Health Information Technology for Economic and Clinical Health Act (HITECH). The HITECH amendments to the Privacy and Security Rules incorporate application of the HIPAA Privacy and Security Rules to business associates and their subcontractors.⁴

THE SECURITY RULE

Key Points

- The Security Rule only applies to PHI that is created, received, maintained or transmitted in an electronic format (ePHI).
- A major goal of the Security Rule is to protect the privacy of patients' health data while giving covered entities the flexibility to implement the policies and procedures that are appropriate to address patient privacy.
- The key terms undergirding the Security Rule are confidentiality, integrity, and availability.
- The security safeguards are broadly categorized as administrative safeguards, physical safeguards, and technical safeguards.
- The security safeguards are supported by specific standards and implementation specifications.
- The security safeguard standards are defined as "addressable" or "required".
- Covered entities are not permitted to consider cost, probability or criticality of potential risks to ePHI when deciding whether to implement a safeguard.

The regulations defining security standards for protecting PHI are primarily found in the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 at 45 C. F. R. Part 160 and 45 C.F.R. Part 164 Subparts A and C. These regulations are commonly referred to as the Security Rule. The standards were developed in part to address the increasing use of electronic information systems in health care settings for conducting administrative functions and, more recently, to provide clinical decision support in the delivery of health care. The Security Rule only applies to PHI that is created, received, maintained or transmitted in an electronic format.

⁴ American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 123 Stat. 115, Health Information Technology for Economic and Clinical Health (HITECH Act, §13000, et seq. (Feb. 17, 2009)); Title XIII of Division A and Title IV of Division B are known as the "Health Information Technology for Economic and Clinical Health Act" (HITECH Act).

It does not apply to PHI that is transmitted orally or in writing.⁵ Thus, in the Security Rule, a patient's PHI is referred to as electronic protected health information, or ePHI.

The security standards require that covered entities and their business associates:⁶

- (1) Ensure the confidentiality, integrity, and availability of all ePHI a covered entity creates, receives, maintains or transmits.
- (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of [the HIPAA Privacy Rule].
- (4) Ensure compliance [with the security standards] by the entity's workforce.⁷

There are three important terms undergirding the Security Rule. The first term is "confidentiality." Confidentiality, as defined in the Security Rule, supports the Privacy Rule's prohibition against misuse of a patient's ePHI and means that the patient's ePHI is neither accessible by nor disclosable to unauthorized persons.⁸ The second term is "integrity," which the Security Rule defines as meaning that a patient's ePHI is not to be altered or destroyed in an unauthorized manner.⁹ Finally, "availability" means that a patient's ePHI is only accessible and usable as needed by someone authorized to access and use the patient's data.¹⁰

The Security Rule sets standards for more comprehensive protection than the safeguards required under the Privacy Rule.¹¹ The security safeguards are broadly categorized as:

- (1) Administrative safeguards,
- (2) Physical safeguards, and
- (3) Technical safeguards.

⁵ Summary of *HIPAA Security Rule*, U.S. DEPT OF HEALTH & HUMAN SERVS., available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html> (last visited June 21, 2011)

⁶ HITECH Act §13401(a), 42 U. S. C. §17931.

⁷ 45 C. F. R. 164.306(a)(1)-(4) (2010).

⁸ 45 C.F.R. 164.304 (2010).

⁹ *Id.*

¹⁰ *Id.*

¹¹ 45 C. F. R. §164.530(c) (2010).

Administrative safeguards are defined as the policies and procedures designed to manage the security process, including the conduct of the covered entity's workforce.¹² Physical safeguards are defined as the policies, procedures, and physical methods designed to protect electronically stored health information from unauthorized access and to protect such information from natural and environmental hazards.¹³ Technical safeguards involve the technology and the policies and procedures for its use that protect ePHI and control access to it.¹⁴

Covered entities must ensure that their business associate contracts and other arrangements specify that both the business associate and any subcontractors hired by the business associate will comply with the security requirements applicable to the covered entity.¹⁵ Covered entities and their business associates are also required to maintain written policies and procedures documenting implementation of the security standards, to document updates and changes to such policies and procedures,¹⁶ to retain such documentation for a minimum of six years from the date of its creation or the date when it was last in effect, whichever is later,¹⁷ and to make such documentation available to those persons responsible for implementing the procedures to which the documentation applies.¹⁸

Each of the broad safeguard categories -- administrative, physical and technical -- are supported by specific standards and implementation specifications. These specific standards are further defined as "addressable" or "required". Certain implementation specifications are required, but covered entities have the flexibility to address other specifications in ways the covered entity deems reasonable and appropriate, taking into account the size, complexity and capability of the covered entity and its technical infrastructure hardware, and software security measures.¹⁹ Addressable does not mean optional.²⁰ If a covered entity chooses not to implement an "addressable" specification based on its risk assessment, it must document the reason and, if reasonable and appropriate, it must implement an alternative measure.²¹

¹² 45 C. F. R. §164.308 (2010).

¹³ 45 C. F. R. §164.310 (2010).

¹⁴ 45 C. F. R. §164.312 (2010).

¹⁵ 45 C. F. R. §164.314 (2010).

¹⁶ 45 C. F. R. §164.316(a) and (b)(1)(i) and (ii) (2010).

¹⁷ 45 C. F. R. §164.316(b)(2) (2010).

¹⁸ 45 C. F. R. §164.316(b)(2)(iii) (2010).

¹⁹ 45 C. F. R. §164.306(b) (2010).

²⁰ *Implementation Specifications*, HIPAA SECURITY SERIES (U.S. Dep't of Health and Human Servs., Washington, D.C.), vol. 2, paper 1, at 5 available at

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html>.

²¹ 45 C.F.R. §164.306(d)(ii)(B)(2) (2010).

It is important to note that the HITECH amendments to the Security Rule prohibit covered entities from considering the costs of security measures or the probability and criticality of potential risks to ePHI in complying with the requirements of the Security Rule.²²

SECURITY RULE STANDARDS AND IMPLEMENTATION SPECIFICATIONS

Key Points

- Administrative, physical and technical safeguards are supported by a total of eighteen standards and thirty-six implementation specifications.
- Administrative safeguards encompass the policies and procedures to develop and maintain security measures to protect ePHI and to manage the conduct of workforce employees to protect ePHI.
- The Security Management Standard of the Administrative Safeguards is the foundation on which every covered entity's security activities are built.
- Physical safeguards are the measures, policies and procedures to protect electronic information systems from hazards and unauthorized intrusion.
- Technical safeguards are the policies and procedures to protect access to and control of ePHI.

Administrative Safeguards

Administrative Safeguards are defined as the “administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect [ePHI] and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.”²³ There are nine standards and twenty-one implementation specifications addressed in the Administrative Safeguards. The first standard, the Security Management Standard,²⁴ and its associated required implementation specifications, are the foundation on which every covered entity's security activities are built. The required risk analysis, risk management, and system activity review processes are supported by the requirement that the entity develop a mandatory sanction policy to ensure workforce members and business associates comply with the security policies and procedures. Other required security standards specify that each covered entity must:

²² 45 C.F.R. §164.306(b)(2) (2010).

²³ 45 C.F.R. §164.304 (2010).

²⁴ 45 C.F.R. §164.308(a)(1) (2010).

(1) Identify a specific person “...who is responsible for the development and implementation of the policies and procedures required by [the Security Rule]”;²⁵

(2) “Implement policies and procedures to address security incidents”;²⁶

(3) “Establish (and implement as needed) [a contingency plan] for responding to an emergency or other occurrence...that damages systems that contain [ePHI]”;²⁷

(4) “Perform...periodic technical and nontechnical evaluations...that establish...the extent to which an entity’s security policies and procedures meet the requirements [of the Security Rule]”;²⁸ and

(5) “...Obtain satisfactory assurances...that business associates will appropriately safeguard [patient data]”.²⁹

The contingency plan implementation standards require that a covered entity have a data backup plan, a disaster recovery plan, and an emergency mode operation plan.³⁰ In addition, covered entities must develop and implement policies and procedures for authorizing access to ePHI,³¹ specifically isolating clearinghouse functions of any entity that is part of a larger hybrid organization.³²

Implementing Administrative Safeguards also includes a number of standards for which a covered entity may develop policies and procedures in accordance with its analysis under the factors set forth above. These standards and implementation specifications address such issues as workforce security,³³ security awareness and training,³⁴ and information access management.³⁵

Physical Safeguards

The Security Rule defines Physical Safeguards as “physical measures, policies and procedures to protect a covered entity’s or business associate’s electronic information systems and related buildings and equipment from natural and environmental hazards,

²⁵ 45 C.F.R. §164.308(a)(2) (2010).

²⁶ 45 C.F.R. §164.308(a)(6) (2010).

²⁷ 45 C.F.R. §164.308(a)(7) (2010).

²⁸ 45 C.F.R. §164.308(a)(8) (2010).

²⁹ 45 C.F.R. §164.308(b)(1) (2010).

³⁰ 45 C.F.R. §164.308(a)(7) (2010).

³¹ 45 C.F.R. §164.308(a)(4) (2010).

³² 45 C.F.R. §164.308(a)(4)(ii)(A) (2010).

³³ 45 C.F.R. §164.308(a)(3) (2010).

³⁴ 45 C.F.R. §164.308(a)(5) (2010).

³⁵ 45 C.F.R. §164.308(a)(4) (2010).

and unauthorized intrusion.”³⁶ The four standards that must be addressed under Physical Safeguards encompass facility access controls,³⁷ workstation use,³⁸ workforce security,³⁹ and device and media controls.⁴⁰ Covered entities have flexibility in developing the policies and procedures for Physical Safeguards with the exception of device and media controls. Implementation standards require that each covered entity ensure that any electronic device or media that contains ePHI be made unusable and/or inaccessible when finally disposing of the device. If a device or media is to be re-used, all ePHI must be removed from the media before it is reused.⁴¹ In addition, if the standards related to device and media disposal or re-use are implemented, a covered entity must also maintain a record of the movements of any such hardware and the person responsible for that movement.⁴²

Technical Safeguards

Technical Safeguards are defined in the Security Rule as “the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.”⁴³ Technical Safeguards encompass five standards: (1) access control,⁴⁴ (2) audit controls,⁴⁵ (3) integrity,⁴⁶ (4) person or entity authentication,⁴⁷ and (5) transmission security.⁴⁸

The term “access” has different meanings in the Privacy Rule and in the Security Rule. In the Privacy Rule, access refers to the uses and disclosures of PHI that are permitted or denied as set forth in provisions of Privacy Rule.⁴⁹ Access, for purposes of the Security Rule, refers to “the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.”⁵⁰ To ensure that only authorized users have access to a patient’s ePHI, the Security Rule requires that a covered entity or its business associates “assign a unique name and/or number for identifying and

³⁶ 45 C.F.R. §164.304 (2010).

³⁷ 45 C.F.R. §164.310(a)(1) (2010).

³⁸ 45 C.F.R. §164.310(b) (2010).

³⁹ 45 C.F.R. §164.310(c) (2010).

⁴⁰ 45 C.F.R. §164.310(d)(1) (2010).

⁴¹ 45 C.F.R. §164.310(d)(2)(i) and (ii) (2010).

⁴² 45 C.F.R. §164.310(d)(2)(iii) (2010).

⁴³ 45 C.F.R. §164.304 (2010).

⁴⁴ 45 C.F.R. §164.312(a)(1) (2010).

⁴⁵ 45 C.F.R. §164.312(b) (2010).

⁴⁶ 45 C.F.R. §164.312(c)(1) (2010).

⁴⁷ 45 C.F.R. §164.312(d) (2010).

⁴⁸ 45 C.F.R. §164.312(e)(1) (2010).

⁴⁹ *See generally* 45 C.F.R. Part 164 subpt E. Access as used in the Privacy Rule is discussed in more detail in HIPAA PRIVACY RULE AND PATIENT RIGHTS. *See infra*, p. 12.

⁵⁰ 45 C.F.R. §164.304 (2010).

tracking user identity.”⁵¹ The Security Rule also requires that covered entities and their business associates “establish...procedures for obtaining necessary electronic protected health information during an emergency.”⁵² Wherever feasible, covered entities must also implement automatic log-off terminating electronic sessions after a predetermined time of inactivity⁵³ and encryption and decryption of health data.⁵⁴ Covered entities and their business associates must also be able to track activity in information systems that contain or use ePHI⁵⁵ for purposes of complying with the audit requirements of the Privacy Rule, protecting ePHI from improper alteration or destruction,⁵⁶ ensuring the security of data transmission,⁵⁷ and being able to authenticate that the person or entity seeking access to ePHI is the person or entity as claimed.⁵⁸

Organizational Requirements

Some HIEs may operate only within a covered entity. Others may function independently providing exchange services to more than one covered entity. Although HIEs are not, themselves, defined as covered entities under the Privacy Rule, Section 13408 of HITECH extends the definition of business associate to include HIEs and e-prescribing systems, effective February 17, 2010. The requirements of the Security Rule also extend to all subcontractors for business associates of covered entities.⁵⁹ The current regulations implementing the Security Rule require that covered entities secure assurances from their business associates that the business associates will comply with the requirements of the Security Rule.

⁵¹ 45 C.F.R. §164.312(a)(2)(i) (2010).

⁵² 45 C.F.R. §164.312(a)(2)(ii) (2010).

⁵³ 45 C.F.R. §164.312(a)(2)(iii) (2010).

⁵⁴ 45 C.F.R. §164.312(a)(2)(iv) (2010).

⁵⁵ 45 C.F.R. §164.312(b) (2010).

⁵⁶ 45 C.F.R. §164.312(c)(1) (2010).

⁵⁷ 45 C.F.R. §164.312(e)(1) (2010).

⁵⁸ 45 C.F.R. §164.312(d) (2010).

⁵⁹ HITECH Act §13401(a); 42 U. S. C. §17931.

HIPAA PRIVACY RULE AND PATIENT RIGHTS

Key Points

- The Privacy Rule also implicates security of PHI in HIEs for patients' rights.
- The Privacy Rule encompasses all PHI whether it is being conveyed orally, in writing, or electronically.
- The Privacy Rule defines an individual's rights in relation to protection of his or her PHI.
- With limited exceptions, individuals have the right to access their own PHI, limit access to and disclosure of their data, obtain an accounting of the uses and disclosures of their data, and receive notice of a breach of access to their data.

In addition to the Security Rule, HIPAA's Privacy Rule also implicates security of health data in HIEs as the security of PHI is necessary to ensure certain patient rights in relation to their health information. The Privacy Rule standards are primarily found at 45 C. F. R. Part 160 and Part 164 Subpart E. The Privacy Rule encompasses all PHI and provides that covered entities are required to implement safeguards against any intentional or unintentional use or disclosure of PHI,⁶⁰ whether the PHI is being conveyed in oral, written (paper) or electronic form. For purposes of this section, the focus will remain on PHI compiled, maintained or transmitted in electronic form (ePHI).

There is considerable interplay between the Privacy Rule and the Security Rule. The Security Rule lays out the specific standards and implementation requirements necessary to provide for the security of a patient's data. The Privacy Rule lays out the policies applicable to individuals' rights in relation to protection of their health data.

Individual Rights and the Privacy Rule

Under the provisions of the Privacy Rule, individuals have the right to:

- (1) Authorize access by and disclosure to others of ePHI data in certain circumstances;
- (2) Access and amend their own medical information, except for psychotherapy notes;
- (3) Limit disclosure to a health plan of ePHI paid for solely by the patient;⁶¹

⁶⁰ 45 C.F.R. § 164.530(c)(1) and (2)(i) and (ii) (2010).

⁶¹ HITECH Act §13405(a); 42 U. S. C. §17935.

(4) Obtain an accounting of uses and disclosures of their ePHI; and

(5) Receive notice of a breach in access to their ePHI.

Access, Disclosure, and Authorization

This section focuses on disclosure of an individual's ePHI to others and the patient's rights in relation to those disclosures. Covered entities and their business associates are bound by the provisions of the Privacy Rule.⁶² In general, covered entities and their business associates may use or disclose ePHI without specific authorization from a patient for treatment, payment, and health care operations,⁶³ and for certain other purposes related to public health activities,⁶⁴ law enforcement and legal proceedings,⁶⁵ required health care oversight activities,⁶⁶ and some research activities.⁶⁷ This list is not exhaustive, but it is illustrative of the kinds of activities that do not trigger the need for specific patient authorization. Certain activities, even if they do not trigger a requirement for specific patient authorization, may still require notice to a patient, such as reports related to public health actions and reports to law enforcement officials, with certain exceptions to the notice requirement for abuse and neglect reports.⁶⁸ In addition, even where prior authorization is not required under the Privacy Rule for certain purposes, the Privacy Rule does not supersede more restrictive state or federal law which may require specific patient consent or authorization for certain disclosures. Finally, use of ePHI that does not require specific authorization must be limited to the "minimum necessary" amount of information required to carry out the purpose of the disclosure.⁶⁹ The HITECH amendments specify that a covered entity or its business associate disclosing ePHI must make the "minimum necessary" determination and may not rely on the requesting party to make that determination.⁷⁰

Covered entities and their business associates may also use and disclose certain de-identified data⁷¹ and create a mechanism to allow patients to be re-identified so long as the mechanism for re-identification would not otherwise disclose the identity of a

⁶² See 45 C.F.R. Part 164, Subpt E (2010).

⁶³ 45 C.F.R. §164.502(a)(1)(ii) and 45 C.F.R. §164.506 (2010).

⁶⁴ 45 C.F.R. §164.512(b) and (j) (2010).

⁶⁵ 45 C.F.R. §164.512(e) and (f) (2010).

⁶⁶ 45 C.F.R. §164.512(d) (2010).

⁶⁷ 45 C.F.R. §164.512(i) (2010).

⁶⁸ 45 C.F.R. §164.512(c) (2010).

⁶⁹ 45 C.F.R. §164.502(b) (2010).

⁷⁰ HITECH Act §13405(b)(2); 42 U.S.C. §17935(b)(2).

⁷¹ 45 C.F.R. §164.514(a) and (b) (2010).

particular patient.⁷² The mechanism may include a unique code or other means of record identification, but may not include specific patient identifiers such as gender or age.⁷³

Finally, covered entities and their business associates may use and disclose certain individually identifiable patient data in limited data sets, provided such data is subject to a data use agreement that limits disclosure only for the purpose created in the agreement.⁷⁴ The most common example of use of a limited data set is for research.

Patients must give specific authorization for use or disclosure of their ePHI found in psychotherapy notes⁷⁵ and for certain marketing activities related to the use of their data.⁷⁶

Each of these kinds of use or disclosure trigger the need to ensure that both the person authorizing the disclosure and the person or entity seeking the information is properly identified and their identity authenticated as set forth in the requirements of the Security Rule.

Patient Access and Right to Amend

The Privacy Rule currently requires covered entities to allow an individual the right to access, inspect, and to obtain a copy of PHI about the individual in a designated record set in a ... “form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form...as agreed to by the [parties].”⁷⁷ The exceptions to this requirement are psychotherapy notes where the provider feels that access may be harmful to the patient (subject to peer review), information compiled in anticipation of legal proceedings, and PHI that may be exempt under the Clinical Laboratory Improvements Amendments of 1988⁷⁸ which prohibit release of data to anyone, even the patient, unless specifically authorized.

The Privacy Rule requires that a covered entity must act on an individual’s request for a copy of his or her PHI maintained in a designated record set within 30 days,⁷⁹ though Texas state law, as adopted in HB 300 (82R - 2011), limits the time frame to 15 days.

⁷² 45 C.F.R. §164.514(c) (2010).

⁷³ See 45 C. F. R. §164.502(d)(2)(2010). “Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of [PHI].”

⁷⁴ 45 C.F.R. §164.514(e) (2010).

⁷⁵ 45 C.F.R. §164.508(a)(2) (2010).

⁷⁶ 45 C.F.R. §164.508(a)(3) and (4) (2010).

⁷⁷ 45 C.F.R. 164.524 (2010).

⁷⁸ *Id.*

⁷⁹ 45 C.F.R. 164.524(b) (2010).

The HITECH amendments to this section of the Privacy Rule require that individuals also have the right to access their PHI that is maintained in an electronic health record by securing a copy of the record in the “form or format requested by the individual.” This language is also adopted in state law via HB 300.

Limiting Disclosure to Health Plans

The HITECH amendments also give a patient the right to restrict disclosure to his or her health plan of any PHI that relates to items or services paid for in full by a person or the patient to the covered entity. Covered entities must comply with such requests from individuals.⁸⁰ The current rules implementing this right do not resolve all issues related to exercise of the right. For example, a patient may wish to restrict disclosure of treatment to his health plan. The provider may agree, but then send the required prescription request electronically, with the request being automatically submitted to the health plan for verification of coverage. Questions remain relating to how HIEs will manage all potential downstream requests under this limitation.⁸¹

Accounting for Disclosures and Access

Covered entities are required to track disclosures of ePHI except in special circumstances set forth in the Privacy Rule,⁸² and to provide an accounting of such disclosures to individuals upon request. The HITECH Act added a provision requiring accounting for disclosures made for treatment, payment and health care operations as those terms are defined in the Privacy Rule *if* the disclosures are made through an electronic health record⁸³ as that term is defined in HITECH.⁸⁴ Disclosures are defined as “the release, transfer, provision of access to, or divulging in any other manner of information *outside* the entity holding the information.”⁸⁵ [*Emphasis added*] In addition, the Security Rule requires that covered entities maintain and periodically review reports of who has accessed ePHI, but, currently, these logs do not have to be provided to individuals.⁸⁶

Inclusion of a new requirement for disclosures for treatment, payment and health care operations provoked considerable resistance from covered entities and enforcement is being deferred until the final rules governing implementation of the HITECH disclosure provisions are approved. On May 31, 2011, the federal HHS Office of Civil Rights

⁸⁰ HITECH Act §13405(a)(2); 42 U. S. C. §17935.

⁸¹ 75 Fed. Reg. 40899 (July 14, 2010).

⁸² See 45 C.F.R. §§164.502; 164.506-514 and 164.521.

⁸³ HITECH Act §13405(c); 42 U. S. C. §17935.

⁸⁴ Section 13400 of the HITECH Act defines an electronic health record as “an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.”

⁸⁵ 45 C.F.R. §160.103 (2010).

⁸⁶ 45 C.F.R. §164.308 and §164.312 (2010).

published its proposed rule on disclosures of electronic medical data in the Federal Register.⁸⁷

The proposed rule makes significant changes to the current Privacy Rule requirements governing disclosures of electronic medical data. At the time this paper is written, the 60-day comment period on the proposed rule has just begun. It is anticipated that the disclosure rule will be finalized later in 2011. In anticipation that much of what is proposed in the rule will survive, this paper will incorporate the proposed changes, designating them as proposed where appropriate.

The proposed rule will divide §164.528 of the Privacy Rule,⁸⁸ clarifying an individual's right to an accounting of disclosures and creating a right to receive an access report. "...The intent of the access report is to allow individuals to learn if specific persons have accessed their electronic designated record set information... the intent of the accounting of disclosures is to provide more detailed information ...for certain disclosures that are most likely to impact the individual."⁸⁹ Access reports will be limited to electronic access to patient data maintained in an electronically maintained designated record set.⁹⁰ The disclosure accounting will encompass disclosures of both paper and electronic records,⁹¹ though it will also be limited only to PHI in a designated record set as that term is defined in the Privacy Rule.⁹²

Under the proposed rule, each time information in an electronic designated record set is accessed, an access log will be created to include the date and time of the access, the identity of the person accessing the information, and, if available, a description of the information that was accessed and the actions taken in connection with that access (i.e. view, print, modify, etc.). Access reports will include access for treatment, payment and health care operations.⁹³

Commentary accompanying the proposed rule states that, based on past experience, most requests are about "who" accessed patient PHI, not "why" the access was made. Under the proposal for access reports, individuals will be able to determine who has accessed their ePHI, including members of a covered entity's workforce, which should be

⁸⁷ 76 Fed. Reg. 31426 (May 31, 2011).

⁸⁸ 76 Fed. Reg. 31428-31429 (May 31, 2011).

⁸⁹ 76 Fed. Reg. 31429 (May 31, 2011).

⁹⁰ *Id.*

⁹¹ *Id.*

⁹² See 45 C.F.R. §164.501 (2010). A designated record set is a group of records maintained by or for a covered entity from which information is retrieved and which is used by the covered entity to make decisions about the individual.

⁹³ 76 Fed. Reg. 31448 (May 31, 2011).

relatively straightforward because almost all of the information required to satisfy the requirements of an access report is already currently required under the Security Rule.⁹⁴

Currently, covered entities must be able to provide disclosure information for the six years preceding the request. The proposed rule reduces this requirement to three years,⁹⁵ though the responsive reports themselves and the data supporting the response must be kept for six years from the date of response.⁹⁶ This requirement applies to both disclosure accounting and access reports as set forth in the proposed rule.

A critical question is whether the HIE or the entity creating the record will be responsible for the disclosure accounting. Under the proposed rule, HIEs, for now, will be specifically excluded from having to provide either an access log or an accounting for disclosures within an electronic health information exchange. The commentary in the proposed rule sounds a cautionary note, however, that as electronic health information exchange expands and standards for such exchanges are approved, this exemption will be re-visited.⁹⁷

The proposed rule does provide that individuals will still have a right to learn of disclosures of their PHI through an HIE if such disclosures are made for one of the permissible exceptions to the requirement to obtain authorization for disclosures laid out in the Privacy Rule.⁹⁸ In addition, each time an electronic designated record set is accessed for purposes of exchange through an HIE, that information will be captured in an access report that can be made available to the individual.⁹⁹ This section of the proposed rule leaves unanswered questions about the applicability of provisions related to requirements of business associates. Thus, an HIE that is a business associate as that term is defined in HITECH or in state law will likely need to develop policies and procedures for responding to requests for accountings, including determining who will process the request.¹⁰⁰

In order to ensure that an accurate accounting can be made of disclosures of an individual's ePHI, covered entities and their business associates must have in place the

⁹⁴ *Id.*

⁹⁵ See 45 C.F.R. §164.308(a)(1)(ii)(D) and §164.312(b) (2010).

⁹⁶ 76 Fed. Reg. 31440 (May 31, 2011).

⁹⁷ 76 Fed. Reg. 31440-31441 (May 31, 2011).

⁹⁸ Under the Privacy Rule, covered entities are allowed to grant access to a patient's health data for a number of approved activities without obtaining specific authorization from the patient. These include reporting data for public health purposes, for certain law enforcement investigations, for judicial and administrative proceedings, for benefit eligibility determination, and for workers' compensation.

⁹⁹ *Id.*

¹⁰⁰ 45 C.F.R. §164.530(a)(1) (2010).

ability to monitor whether access to the entity's electronic health information system has been appropriate. Although neither the Privacy Rule nor the Security Rule specifically identify the data that should be gathered in order to address the requirements for audit controls, the Security Rule does specify that a covered entity or its business associate must implement "hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."¹⁰¹

Breach Notification

The HITECH Act creates a new breach reporting requirement for covered entities and their business associates.¹⁰² At the present time, the interim final rule for breach notification that was published on August 24, 2009 governs implementation of the HIPAA breach notification requirements. However, the U.S. Department of Health and Human Services is continuing to review this rule and anticipates publishing a new final rule in the future. As outlined in the interim rule, the breach reporting requirements create some potential land mines for an HIE implementing privacy and security requirements.¹⁰³

HITECH defines a reportable breach as ... "the unauthorized acquisition, access, use, or disclosure of protected information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."¹⁰⁴ Unintentional acquisition, access or use by an employee or individual acting under the authority of a covered entity or business associate is also not considered a reportable breach if the unintentional access was made in good faith and was within the course and scope of the professional relationship between the individual and the entity, and the information was not further accessed, used, or disclosed to anyone else.¹⁰⁵ Similarly, an incident in which an individual who is otherwise authorized to access an individual's ePHI inadvertently discloses the ePHI and the individual or entity that receives the inadvertent disclosure does not further disclose such information is not considered a reportable breach.¹⁰⁶ Kristen Rosati, a private attorney who has worked with a number of states on HIE legal issues, suggests that the exceptions to the HITECH breach provisions would be applicable to an HIE "because the purpose of the exceptions appears to be avoiding the

¹⁰¹ 45 C.F.R. 164.312(b)(2010).

¹⁰² HITECH Act § 13402; 42 U. S. C. § 17932.

¹⁰³ *Breach Notification Final Rule Update*, U. S. DEP'T. OF HEALTH & HUMAN SERVS. *available at* <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/finalruleupdate.html>. (last visited June 21, 2011).

¹⁰⁴ HITECH Act § 13400; 42 U. S. C. § 17930.

¹⁰⁵ *Id.*

¹⁰⁶ *Id.*

burden of reporting where access to an individual's information is provided by mistake by someone who is otherwise authorized to see health information and no further use or disclosure is made of the information.”¹⁰⁷

The Interim Final Rule clarifies that limited data sets that exclude the specific direct identifiers listed in 45 C.F.R. §164.512(e) (2) are also excluded from the application of the HITECH breach notification requirements. The Interim Rule also clarifies that certain other research or public health activities that use limited data sets that are subject to a data use agreement may include birth year *or* certain zip code information ¹⁰⁸ and still be exempt from the breach notification requirements. In order to be exempt, the covered entity or business associate must conduct a risk analysis to determine whether the potential risk of re-identification poses a significant risk of harm to an individual.¹⁰⁹ Although HIEs are exempt from accounting for disclosures under the notice of proposed rulemaking issued on May 31, 2011,¹¹⁰ it is unclear how they will know whether covered entities have completed an adequate risk analysis, if required.

Whether an intentional breach is reportable depends, at the present time, on two main factors. The first is whether the data is secured or unsecured. HITECH defines unsecured PHI as data that is not secured through the use of a technology or methodology that (1) renders PHI “...unusable...to unauthorized individual(s) and (2) “is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.”¹¹¹ The second factor is whether the use or disclosure of the individual's PHI could compromise the security or privacy of the PHI itself by creating a significant risk of financial, reputational, or other harm to the individual due to the breach.

In the event that a breach of an individual's unsecured ePHI is reportable, the covered entity is required to notify affected individuals in written form by first class mail or, alternatively, by e-mail if the individual has agreed to accept such notices electronically. If the covered entity has insufficient information to contact ten or more affected individuals, the covered entity must post a notice on the homepage of its website or provide notice through print or broadcast media where the individuals reside. If the breach affects fewer than ten individuals for whom the covered entity has insufficient contact information, the covered entity may provide notice by telephone or other means.

¹⁰⁷ Memorandum from Kristen Rosati, Esq. (Apr. 1, 2009) (on file with the author).

¹⁰⁸ 45 C.F.R. §164.514 (2010).

¹⁰⁹ 74 Fed. Reg. 42746 (August 24, 2009).

¹¹⁰ 76 Fed. Reg. 31426 (May 31, 2011).

¹¹¹ HITECH Act, §13402(h); 42 U. S.C. §17932(h).

If the breach affects 500 or more individuals, the covered entity must also notify the Secretary of HHS. If the breach occurs at or by a business associate, the business associate must notify the covered entity of the breach without unreasonable delay, and no later than 60 days from discovery of the breach, and, further, must cooperate with the affected covered entity to provide notice to affected individuals.¹¹²

TEXAS LAW

Key Points

- Some Texas state laws governing medical information privacy are more stringent than HIPAA.
- Texas state law does not contain a statutory equivalent to the HIPAA Security Rule.
- In 2011, the Texas Legislature passed HB 300, addressing complaint processes, sale of PHI, and requirements for patient permission before disclosing PHI.

In addition to the federal law described above, many states' laws also contain provisions that address the privacy of a patient's personal health information, many of which are more stringent than the requirements of the Privacy Rule. Except in limited circumstances, where state law is more stringent than the Privacy Rule, state law prevails.¹¹³ Texas state laws governing the privacy of medical information are primarily found in the Occupations Code (Texas Medical Practices Act)¹¹⁴ and the Health & Safety Code (Texas Medical Records Privacy Act).¹¹⁵ In addition, Title 7 of the Texas Health & Safety Code addresses issues of consent and disclosure of information for persons with intellectual disabilities (still currently statutorily referred to as "mental retardation"). With limited exceptions, under state law, sensitive information, such as HIV test results,¹¹⁶ records of sexually transmitted disease,¹¹⁷ and sexual assault information obtained as a result of confidential information communication between the assault

¹¹² *Breach Notification Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS. available at <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html> (last visited June 21, 2011).

¹¹³ See generally Cynthia Marietta & Patricia Gray, MEDICAL INFORMATION PRIVACY IN TEXAS, available at http://www.thsa.org/media/1812/primer_medical_information_privacy_protections_in_texas.pdf.

¹¹⁴ TEX. OCC. CODE ANN. §159.001 *et seq.* (West, 2009).

¹¹⁵ TEX HEALTH & SAFETY CODE ANN. §§181.001-181.205 (West, 2009).

¹¹⁶ TEX. HEALTH & SAFETY CODE ANN. §81.103 (West, 2009).

¹¹⁷ TEX. HEALTH & SAFETY CODE ANN. §81.046 (West, 2009).

victim and an advocate¹¹⁸ may not be disclosed without the express authorization of the patient.

Texas state law does not have a separate set of security standards equivalent to those found in the HIPAA Security Rule. Instead, the state incorporates federal standards required for electronic information transactions related to federally funded health programs administered in the state by adoption of uniform acts such as National Electronic Data Interchange Standards for Health Care Information¹¹⁹ and electronic transactions in the state Medicaid Program.¹²⁰ In addition, Texas has adopted the Uniform Electronic Transactions Act, which supports the electronic maintenance of records and recognizes the validity of electronic signatures.¹²¹

82nd Texas Legislature Update

The 82nd Texas Legislature (2011) adopted three bills with implications for electronic health information exchange.

HB 300 amends Chapter 181 of the Texas Health and Safety Code to require that:

- All covered entities, as that term is defined in both state law and in the federal HIPAA Privacy Rule, must comply with the Privacy Rule regarding access to and use of PHI.
- The Texas Health Services Authority (THSA) is required to develop privacy and security standards for the electronic sharing of PHI and submit them to the Texas Health and Human Services Commission (HHSC) for ratification.
- Covered entities must provide training regarding state and federal law concerning PHI to new employees not later than 60 days after the employee is hired by the covered entity. Such training must be provided again at least once every two years thereafter.
- Patients are entitled to receive a copy of their electronic health record in a form acceptable to the patient not later than 15 days after the patient's written request.

¹¹⁸ TEX. GOV. CODE ANN. §420.071(c) (West, 2009).

¹¹⁹ TEX. GOV. CODE ANN. §531.0315 (West, 2009).

¹²⁰ TEX. HEALTH & SAFETY CODE ANN. §12.0124 (West, 2009).

¹²¹ TEX. BUS. & COM. CODE ANN. §322.001 *et. seq.* (West, 2009).

- The attorney general must maintain an Internet website providing information about patients' privacy rights, a list of state agencies that regulate covered entities and the complaint process for each agency.
- Covered entities may not disclose an individual's PHI to any other person in exchange for any direct or indirect remuneration. Exceptions are granted for disclosures required for treatment, payment, health care operations and performance of certain insurance or health maintenance organizations services performed for the covered entity. With respect to the exception for insurance services, there are 28 functions listed in the Texas Insurance Code that are excepted.¹²² Any remuneration received by a covered entity is limited to the cost of preparing or transmitting the PHI.
- Covered entities must provide notice to patients if the covered entity either creates or receives PHI and the PHI is subject to electronic disclosure. The covered entity may provide a general notice by posting a written notice in the covered entity's place of business, posting a notice on the covered entity's Internet website, or by posting a notice in any other place affected individuals are likely to see it.
- Covered entities may not electronically disclose a patient's PHI to any person without a separate authorization from the patient or the patient's legally authorized representative for each disclosure. The authorization may be oral, but must be documented in the patient's record. Exceptions are provided for treatment, payment, health care operations and performance of certain insurance or health maintenance organization services performed for the covered entity.
- Covered entities may disclose a patient's PHI as otherwise authorized or required by either state or federal law.
- The attorney general is directed, by January 1, 2013, to adopt a standardized authorization form for covered entities to use. The form must comply with HIPAA privacy requirements and the provisions of HB 300. The language of

¹²² These exceptions cover activities ranging from fraud investigation and data base security to underwriting, issuance of policies, and ratemaking functions, to disease management and utilization review. Some of the exceptions may contradict other privacy requirements. For example, sensitive health information may be protected from disclosure for issuance of policies, but the exceptions in the insurance code indicate that such information could be disclosed for purposes of utilization review of patient services or disease management programs.

HB300 does not reference any other authorization requirements such as those referenced in 42 C.F.R. Part 2.

- Administrative penalties for wrongful disclosure may be limited if a court finds that disclosure was made only to another covered entity and only for a permitted purpose as set out above and, further, that 1) the recipient did not use or release the PHI; 2) the PHI was encrypted; or 3) that at the time of the disclosure the covered entity implemented and maintained security policies, including the education and training of employees responsible for the security of PHI.
- Factors that a court may consider in determining the amount of administrative penalties include the nature of the covered entities compliance history, the nature, circumstances, extent and gravity of the disclosure, the potential risk of financial, reputational or other harm to the individual whose PHI was disclosed, the covered entity's effort to correct to violation, the amount necessary to deter a future violation, and whether, at the time of the disclosure, the entity was certified by the THSA as having complied in the past with the privacy and security standards promulgated by the HHSC in consultation with the THSA.
- Administrative penalties may also be imposed for failure to notify an individual whose sensitive personal information may have been acquired by an authorized person.
- Administrative penalties may include both monetary penalties and enforcement actions such as revocation of a covered entity's license.
- Criminal penalties apply if wrongful access to a patient's PHI results in identity theft.¹²³

SB 156 creates an Institutional Review Board (IRB) within the Department of State Health Services (DSHS) to assist with disposition of data collected by the former Health Care Information Council and allows DSHS to disclose any data collected by the former entity, and not included in public use data, to any program within DSHS if reviewed and approved by the IRB. The bill also authorizes DSHS to disclose such data to any Health and Human Services agency as defined in SEC. 531.001(4) of the Texas Government Code, provided confidentiality of data can be maintained. Any data currently classified as confidential maintains its confidential status.¹²⁴

¹²³ HB 300, 82nd Reg. Sess. (Tex. 2011).

¹²⁴ HB 156, 82nd Reg. Sess. (Texas, 2011).

HB 411 addresses concerns with Texas' newborn screening program. Specific provisions added this session include a requirement that the newborn's parents consent to any disclosure of de-identified data screening test results for public health research purposes. In addition, such disclosures must be approved by both the Commissioner and an Institutional Review Board or privacy board of DSHS. Parents may revoke their authorization at any time, and the child may revoke consent after attaining the age of majority.¹²⁵

OTHER FEDERAL PROVISIONS

Key Points

In addition to HIPAA and HITECH, other federal laws and regulations such as those addressing clinical labs, educational facilities, federally funded substance abuse treatment, patient safety organizations and veterans also implicate the privacy and security of medical information.

- The Clinical Laboratory Improvements Amendments of 1988 (CLIA) limit release of clinical laboratory reports to specifically authorized persons.
- The Red Flags Rule requires that entities protect patients against identity theft.
- The Federal Educational rights and Privacy Act (FERPA) implicates the privacy of student health records maintained in public elementary and secondary schools.
- The Patient Safety and Quality Improvement Act authorizes review of both individual and aggregated patient data to improve patient safety.
- Federally funded substance abuse treatment programs have special requirements for accessing patient health information.
- The Veterans Health Administration requires written authorization from patients to release health information to non-VHA facilities.

¹²⁵ H.B. 411, 82nd Reg. Sess. (Texas, 2011)

There are other federal laws and regulations that impact privacy considerations for HIEs. Although a full discussion of every federal law that specifies privacy protection for personal health information is beyond the scope of this paper, certain provisions do deserve mention as they either raise unique policy questions or may require segmentation from access or disclosure without specific patient authorization.

Clinical Laboratory Improvements Amendments of 1988 (CLIA)

CLIA regulations and interpretative guidance, together with state law and the Privacy Rule, regulate clinical laboratories. In general, the Privacy Rule exempts clinical laboratories from patient right of access to information.¹²⁶ CLIA allows release of information only to an “authorized person,” such as the person who ordered the test, or to an “individual responsible for using the test results,” but not directly to the patient¹²⁷ CLIA allows states to expand the definition of authorized person,¹²⁸ but Texas follows the definition in the CLIA.¹²⁹

Red Flags Rule

The Red Flags Rule, drafted by the Federal Trade Commission to fight fraud and identity theft, requires all businesses that bill for services to establish programs to detect red flags in their operations that might lead to identity theft and to establish procedures to address and correct any identified red flags.¹³⁰ Although health care providers are exempt from enforcement under the Red Flags Rule, familiarity with its guidance is useful because medical identity theft is a concern for patients even if the percentage of patients affected is small.¹³¹

Family Educational Rights and Privacy Act (FERPA)

FERPA is a federal law that protects the privacy of students’ education records. It applies to all educational agencies and institutions that receive federal funds for programs administered under the U.S. Department of Education. It generally does not cover educational records of students who attend private or religious elementary and secondary schools. The term “education records” is broadly defined. At the elementary and secondary school level, a student’s health records, such as immunization records that are

¹²⁶ 45 C.F.R. §164.524(a)(1)(iii)(A) (2010)

¹²⁷ 42 C.F.R. §493.1291 (2010).

¹²⁸ 42 C.F.R. 493.2 (2010).

¹²⁹ *TMA Practice E-tips* available at <http://www.texmed.org/templateprint.aspx?id=1691>

¹³⁰ See generally 72 Fed. Reg. 63771 (Nov. 9, 2007); 16 C.F.R. §681 (2007) available at <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

¹³¹ Ponemon Institute *Second Annual Survey on Medical Identity Theft* (Mar. 2011) available at http://www.protectmyid.com/images/education_center/pdf/050TypesofFraud/1_types%20of%20fraud_medical%20study.pdf.

maintained by the school, as well as any records maintained by the school nurse, are education records subject to FERPA (unless the school based clinic itself qualifies as a covered entity). At the post-secondary level, medical and psychological treatment records of eligible students are excluded from the definition of education records to the extent that they are created and used only in connection with treatment of a student. Education records are generally excluded from coverage under the Privacy Rule.¹³² Records subject to FERPA protection, which may include student health records, generally may not be shared with third parties without written parental consent, but they may be shared with teachers and other school officials without written consent if these officials have “legitimate educational interests” as defined by school policy. In addition, education records may also be disclosed, without parental authorization, to “appropriate parties” in connection with an emergency, if knowledge of the information is necessary to protect the health or safety of a student. The HITECH amendments appear to limit disclosure of health information without specific written authorization from a parent or guardian only to immunization data required for school enrollment. However, the amendments leave open a number of questions, such as whether oral authorization must be documented and whether pre-school and post-secondary facilities that require immunization history for enrollment are covered.¹³³ The policy question for an HIE is whether to disclose PHI in response to inquiries from school based health providers whose potential redisclosure of the information is not covered under the Privacy Rule.¹³⁴

Patient Safety and Quality Improvement Act Rules (42 CFR Part 3 Subpart C)

The Patient Safety and Quality Improvement Act (PSQIA) was passed to assist in sharing information about adverse patient safety events among providers and patient safety organizations (PSO) in order to improve patient safety and quality of care. To achieve that objective, the rules for Part C of the Act provide that patient safety work product is privileged and confidential except in very limited circumstances. Covered entities may have a PSO as part of their internal health care operations for quality assurance purposes or they may contract with an external PSO to receive and analyze reports about patient safety issues. If the covered entity contracts with an external PSO, it must do so with a business associate agreement. In most instances, those providing information under the PSQIA will be covered entities subject to the provisions of HIPAA. Disclosures may include individually identifiable PHI or a PSO may aggregate patient data for analysis of

¹³² 45 C.F.R. 160.103 (2)(i) and (ii) (2002).

¹³³ See 75 Fed. Reg. 40896 (July 14, 2010).

¹³⁴ U.S. Dep’t. of Health & Human Serv., Joint Guidance on the Application of the *Family Educational Rights and Privacy Act (FERPA)* and the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* to Student Health Records (Nov. 2008), available at <http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveridentities/hipaaferpajointguide.pdf>.

patient safety events. Patients and providers are not required under the PSQIA to furnish information to a PSO. However, if a provider authorizes access to PHI as part of its health care operations, patients are entitled to know that their health information has been accessed by a PSO.

Federally Funded Substance Abuse Treatment (42 C.F.R. Part 2)

The federal regulations governing disclosure of federally funded substance abuse treatment impose limitations on disclosure and use of any information, including information about referral and intake, obtained in relation to the treatment of patients for both alcohol and other substance abuse. They cover not only programs in designated substance abuse treatment facilities, but also out-patient rehabilitation programs, programs within general hospitals, and services provided by individual providers.¹³⁵ Physicians who simply prescribe certain controlled substances, if prescribed to assist patients with maintenance of their treatment, are subject to the provisions of the Part 2 regulations.¹³⁶ Substance abuse patient records may only be released without the patient's consent (authorization) for stringently limited research purposes, to protect the patient in a medical emergency, or for certain audit and evaluation activities.¹³⁷ Absent these narrow exceptions, no patient information may be released without the patient's express consent, which must include all of the following elements to be valid:

- (1) The specific name or general designation of the program or person permitted to make the disclosure;
- (2) The name or title of the individual or the name of the organization to which the disclosure is to be made;
- (3) The name of the patient;
- (4) The purpose of the disclosure;
- (5) How much and what kind of information is to be disclosed;
- (6) The signature of the patient and, when required for a patient who is a minor, the signature of a person authorized to give consent; or, when required for a patient who is incompetent or deceased, the signature of person authorized to sign...in lieu of the patient;

¹³⁵ 42 C.F.R. §2.12(e) (2009).

¹³⁶ Substance Abuse and Mental Health Servs. Admn., *Frequently Asked Questions: Applying the Substance Abuse Confidentiality Regulations to Health Information Exchange (HIE)* available at <http://www.samhsa.gov/Health/Privacy/docs/EHR-FAQs.pdf> (last visited June 21, 2011).

¹³⁷ 42 C.F.R. Pt 2, Subpt. D (2010).

(7) The date on which the consent is signed;

(8) A statement that the consent is subject to revocation at any time except to the extent that the program or person who is to make the disclosure has already acted in reliance on it. Acting in reliance includes the provision of treatment services in reliance on a valid consent to disclose information to a third party payer; and

(9) The date, event, or condition upon which the consent will expire if not revoked before. This date, event or condition must insure that the consent will last no longer than reasonably necessary to serve the purpose for which it was given.¹³⁸

Records may not be disclosed for purposes of making criminal charges or investigating patients without a court order.¹³⁹ A court, in determining the extent to which disclosure is required, shall impose appropriate safeguards against unauthorized disclosure.¹⁴⁰ This prohibition against disclosure does not apply to reporting required under state law for incidents of suspected child abuse and neglect to appropriate authorities.¹⁴¹ Strict compliance with the statute is required.¹⁴²

Exchange of substance abuse data through an electronic HIE requires that the HIE enter into a Qualified Service Organization Agreement (QSOA) with a qualified provider covered under Part 2 in order to receive a patient's substance abuse treatment records. This requirement also applies to accepting such records for treatment, payment and health care operations.¹⁴³

Veterans Health Administration Health Information Privacy Requirements

The Veterans Health Administration (VA) has extensive policies governing the privacy of health information for its beneficiaries within its facilities. The most relevant section for HIEs in Texas will likely be provisions related to disclosure of individually identifiable health information between the VA and non-VA health care providers for the purpose of having the Veterans Administration pay for the services. In general, all such disclosures require prior written authorization from the individual to whom the information pertains. There are two primary exceptions to the requirement for written authorization:

¹³⁸ 42 C.F.R. §2.31 (2002).

¹³⁹ 42 U. S. C. §290ee-3(2)(C) (2010).

¹⁴⁰ *Id.*

¹⁴¹ 42U.S.C. §290ee-3 (2010).

¹⁴² 42 C.F.R. §2.13(b) (2010).

¹⁴³ Frequently Asked Questions, *supra* note 137 at p. 6.

(1) When the non-VA health care provider referred the individual to a VA health care facility and the individual intends to return to the same non-VA health care provider for follow-up care; and

(2) Under “emergent conditions to the non-VA health care provider caring for the individual.” If disclosure of Veterans Health Administration records is required in a medical emergency, a notice of disclosure must be sent to the patient at the patient’s last known address.¹⁴⁴

KEY POLICY QUESTIONS

The federal HIPAA Security Rule is designed to protect the privacy of ePHI while giving covered entities flexibility in implementing policies and procedures appropriate to carry out the requirements of the Security Rule.¹⁴⁵ In addition, individuals have certain rights under the Privacy Rule to oversee and ensure the accuracy of their health data, as well as certain rights to know who has seen their health data and, in most instances, for what purposes their data was accessed. HIEs are also a potentially important tool for cost effective and efficient delivery of health care as well as beneficial population based research.

Implementing the Privacy and Security Rules

- What actions will demonstrate that covered entities have adequately complied with addressable standards for implementing the Security Rule?
- How will actions of business associates of covered entities be monitored and enforced for compliance with both the Security Rule and the Privacy Rule?
- How will HIEs ensure that patients and providers, as well as others who may have a role in the development of HIEs, understand and comply with the rights of patients?
- How will HIEs monitor the work of technical support workforce staff to ensure the privacy and security of patient health information?

¹⁴⁴ Dep’t. of Veterans Affairs, VHA Handbook 1605:1 §24 (Dec. 31, 2002) available at http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1423

¹⁴⁵ *Summary of HIPAA Security Rule*, supra note 5.

Authenticating patient and user identification:

- What entity will be responsible for authenticating health care providers? Health care plans? Health care clearinghouses?
- How will HIEs determine what limits, if any, should be placed on authenticated providers to access patient data?
- How will HIEs determine responsibility for maintaining audit trails?
- How will patient identification be verified? How will authenticated identification be maintained?

Ensuring accountability

- What policies are needed to manage requests for access to patient data?
 - Research requests: How will HIEs manage requests for access to limited data sets that may include some patients' individually identifiable information? What steps to secure Institutional Review Board (IRB) approval will be required? How will risk assessments be reviewed?
 - Emergency response: Under what circumstances will an HIE recognize a request from a disaster response coordinator such as the Red Cross? If a disaster declaration is required, may it be from the state or a local jurisdiction, or must it be a federal declaration?

Managing sensitive information:

- What information will be classified as sensitive information?
- Will HIEs segment sensitive information? If so, what entity will be responsible for creating an electronic lockbox for securing sensitive information?
- How will HIEs secure "downstream" use of sensitive information if e-prescribing is used?

Consent and special populations:

- How will HIEs manage consent and authorization issues related to those with diminished mental capacity or minors who have the right to accept or refuse certain treatment?

- How will HIEs extend minors’ privacy rights as they relate to who can and cannot access their PHI, including an accounting for disclosure?
- How will HIEs manage access to sensitive information that a patient may wish to keep private, especially to the extent that such sensitive information may carry with it additional consent or authorization requirements?

Breach notification:

- The rules related to breach notification focus on notice to the patient. However, other parties in an HIE network may also be impacted. How will breach notification be provided to other potentially affected parties in an HIE network?

Other

Although Texas has a more expansive definition of covered entity than does HIPAA, an HIE could receive requests from entities that do not recognize Texas’ definition. In addition, HIEs must manage requests from technical support organizations.

- How will HIEs respond to requests for access to patient health data by organizations and individuals who do not meet the definition of “covered entity” in order to ensure patients that their health data is both private and secure?
- What policies are needed to address requests from non-covered entities?
- Should HIEs be required to furnish their own notice of privacy practice?

CONCLUSION

As Texas develops support for electronic health information exchange (HIE), patients, providers and payers will need assurance that the confidentiality, integrity and availability of patients’ protected health information (PHI) is maintained. Covered entities, their business associates and subcontractors must understand and adhere to the requirements of the Security Rule in order to guarantee the rights of patients under the Privacy Rule. Ongoing review of privacy and security practices is necessary as the rulemaking process continues and implements changes in both state and federal law. Close communication and coordination between those who develop privacy and security policies and those who develop the technical implementation of those policies is critical to ensure that the operation of HIEs in Texas is able to engender stakeholder trust.