HITRUST
Health Information Trust Alliance

Texas House Bill 300: Compliance through HITRUST

How HITRUST is addressing the new Texas law relating to the privacy of protected health information, and providing administrative, civil, and criminal penalties.

December 2012

HITRUST
Health Information Trust Alliance

Contents

HITRUST
Health Information Trust Alliance

Understanding HB 300

Overview

In June of 2011, Texas House Bill ("HB") 300 was passed unanimously by both houses of the State Legislature. The new law is effective as of September 1, 2012, and amends Texas Health Code, Chapters 181 and 182; Texas Business and Commerce Code, Sections 521 and 522; Texas Government Code, Chapter 531; and Texas Insurance Code, Chapter 602. The State law is designed to better ensure the security and privacy of protected health information (PHI) that is exchanged via electronic means for residents in the State of Texas. The law also grants new enforcement authority to a variety of state agencies, establishes standards for the use of electronic health records, and increases penalties for the wrongful electronic disclosure of PHI, including creating a new felony for wrongfully accessing or reading electronic health records (EHRs) via electronic means.

Applicability

HB 300 builds upon the Federal Health Insurance Portability and Accountability Act (HIPAA), requiring that all "covered entities" as defined by 45 C.F.R. 160.103 comply both with HIPAA and the requirements specified in the new State law. As defined by 45 C.F.R. 160.103, a covered entity is any health plan, health care clearinghouse, or health care provider who transmits any health information electronically. HB 300 expands the definition of a covered entity to apply to any entity that stores, processes, or transmits PHI in a commercial or professional capacity; any entity that comes into possession of PHI; or is an employee, agent, or contractor of an entity as described above. Explicitly, in addition to the entities listed by HIPAA, this definition of covered entity effectively extends the term to include business associates, governmental units, information or computer management entities, schools, health researchers, or a person who maintains an Internet site.

Training

Under section 181.101 of the amended Texas Health Code, all covered entities are required to provide a training program for employees regarding the State and Federal laws relating to PHI. Specifically, the training program must be tailored to the course of business of the covered entity and to the roles and responsibilities of its employees. The training program must be provided within 60 days from the date any employee is hired, and again to all employees at least every two years. Further, the covered entity must ensure each employee signs a statement acknowledging that the employee has attended and completed the training program.

Consumer Access

For covered entities, specifically health care providers, using an EHRs system , the entity must provide an individual's record electronically within 15 business days following a written request from the individual.

Consumer Information Website

The State Attorney General is required to maintain an informational website relating to consumer and patient privacy in Texas. Specifically the website shall:

- Provide information regarding privacy rights as it relates to PHI under State and Federal law
- List the State agencies that regulate covered entities in the State
- Detail information regarding each agency's complaint process
- Provide contact information for each agency

The State Attorney General's website for consumer protection is accessible at https://www.oag.state.tx.us/consumer/.

Consumer Complaint Report

The State Attorney General is required to submit a report to the legislature annually that addresses the number and types of complaints received as it relates to consumer privacy of PHI, and the enforcement action taken for each compliant. In turn, each State agency that receives consumer complaints is required to submit to the Attorney General information about the complaints the agency has received and any enforcement or response taken to address the complaint. In order to maintain privacy, the Attorney General is responsible for de-identifying any PHI that may be present in the complaint or response prior to filing his/her report to the legislature.

Sale of PHI

A covered entity may not disclose PHI for direct or indirect payment except as follows:

- To another covered entity for treatment, payment, health care operations, or for performing an insurance or health maintenance organization function
- If otherwise required by State or Federal law

The payment requested to disclose the information must not exceed the reasonable costs of preparing and transmitting the information.

Notice of Authorization for Electronic Disclosure

A covered entity must provide general notice to the individuals for whom it creates or receives PHI by:

- Posting a written notice in the entity's business;
- Posting an electronic notice on the entity's website; or
- Posting a notice in a conspicuous location where it is likely to be noticed by the individuals whose PHI is being disclosed

The electronic disclosure of PHI is prohibited without a separate authorization from each individual for each disclosure. The authorization must be made in electronic or written form, or documented in writing by the covered entity if authorization was provided in oral form. Authorization is not required for disclosures listed in the prior section.

The State Attorney General is required to provide a standard authorization form, though as of the date of this report, one does not appear to be available.

Penalties and Enforcement

The State Attorney General is authorized to enact civil monetary penalties against any covered entity that violates the requirements of the Texas Health Code, Chapter 181, as amended by HB 300. The following table lists the tiers of penalties, including the maximum amount and under what circumstances the penalty may be applied:

Penalty Amount	Penalty Conditions
$5,000	Violations committed with **negligence** in one year, regardless of how long the violation continues during that year.
$25,000	Violations committed **knowingly or intentionally** in one year, regardless of how long the violation continues during that year.
$250,000	Violations committed knowingly or intentionally where PHI was used for **financial gain**.

The penalties are capped at $250,000 annually, but only if the disclosure was to another covered entity and for treatment, payment, health care operations, or otherwise required by law; and the information was encrypted, the recipient did not use or release the PHI, and the covered entity that disclosed the information has adequate privacy and security policies in place including employee training. If the violations are found to have occurred frequently, constituting a pattern of non-compliance, penalties may be assessed not to exceed $1.5 million annually. The State Attorney General is authorized to retain a portion of the penalties to cover the costs of enforcement.

In addition to penalties, if the investigation finds a pattern of non-compliance, a covered entity that is licensed by the State may have its license revoked.

Audits

The Texas Health and Human Services Commission may request that the United States secretary of health and human services conduct an audit of a covered entity to determine the entity's compliance with HIPAA. Following a violation that is found to be a pattern of non-compliance, the Commission may request the covered entity to submit the results of a risk analysis conducted by the covered entity or request the licensing agency to conduct the audit if applicable.

Standards for the Electronic Sharing of PHI

The Texas Health and Human Services Commission is responsible for reviewing and adopting privacy and security standards for the electronic sharing of PHI. The standards adopted must comply with HIPAA and other applicable State and Federal laws relating to the confidentiality and security of PHI. Further, the standards must ensure the secure maintenance and disclosure of PHI, include procedures for securely disclosing PHI, and support interoperability. These standards are listed and discussed further in the following sections.

The Texas Health Services Authority (THSA) is also established as a public-private collaborative to develop a seamless electronic health information infrastructure to support the health care system in the State and to improve patient safety and quality of care. Subsequently, THSA plans to offer statewide

health information exchange (HIE) capacity through a network called HIETexas that will enable the sharing of patient information between providers across the state via HIEs and their participants. As part of this program, THSA has established draft model security policies that local HIEs should adopt and tailor to their environment and operations. These policies are listed and discussed further in the following sections.

Standards for the Electronic Exchange of Health Information

As required by HB 300, the Texas Health and Human Services Commission is responsible for reviewing and adopting privacy and security standards relating to the electronic exchange of health information. On September 13, 2012, THSA had developed the standards and submitted them to the Commission for adoption by rule.

The proposed new rules apply to covered entities that electronically exchange, use, or disclose PHI. The rules identify statutory and regulatory requirements that covered entities must follow to be in compliance with the law. The standards proposed include:

- The HIPAA Privacy, Security, and Breach Notification Rules
- The Texas Medical Records Act, Chapter 181 of the Texas Health and Safety Code
- The Texas Identity Theft Act, Chapter 521 of the Texas Business and Commerce Code
- Other applicable State and Federal laws or regulations as they relate to the confidentiality of information

The proposed standards that any covered entity that electronically exchanges, uses, or discloses PHI must comply with, as applicable, are listed in the table in Appendix A of this document.

THSA Model Security Policies

In 2010, the Department of Health and Human Services (HHS), through the Office of the National Coordinator (ONC) for Health Information Technology, approved Texas' Strategic and Operational Plan for a Statewide HIE, under which the State received grant funding to further certain health information exchange goals. As part of this program, which is being administered by the Texas Health and Human Services Commission with contractual support from the THSA, the Commission helped to fund 12 regional HIE networks, the Local HIEs. These Local HIEs cover approximately 90% of the State's physicians and hospitals eligible for the program. The purpose of the model security policy is to help the Local HIEs comply with State and Federal law requirements by providing a guide as to some common policies and procedures that may be applicable to the HIEs. It is important to note that each Local HIE has the freedom and flexibility to implement its own unique privacy and security measures as appropriate and in compliance with State and Federal law (i.e., these policies are meant to be a guide, not a mandate).

The THSA Model Security Policies implement the requirements of the HIPAA Security Rule very closely. This includes:

- **164.308, Administrative Safeguards** – Administrative safeguards are administrative actions, policies, and procedures that manage the selection, development, implementation, and maintenance of security measures to protect EPHI and to manage the conduct of Users, some of which apply to HIE Users and/or Participant Users, in relation to the protection of such EPHI.
- **164.310, Physical Safeguards** – Physical safeguards are physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion.
- **164.312, Technical Safeguards** – A Technical Safeguard is the technology and the policy and procedures for its use that protect EPHI and control access to it.

164.314, Organizational Safeguards, which addresses specific implementation specifications for Business Associate contracts and other written agreements, and 164.316, Policies, Procedures and Documentation Safeguards, which addresses requirements for storing, maintaining and retaining documentation and an overarching standard for developing security policies and procedures, are not explicitly addressed or referenced within the policies. While 164.308(b)(1) through (b)(4) address the concept of Business Associate agreements, and each sub-section generally specifies the policies and procedures necessary, it is recommended that Local HIEs adopting this model security policy review and supplement the guidance with the limited requirements from these omitted sections of the HIPAA Security Rule.

It is important to note that since the THSA model security policy implements HIPAA, a Federal law, any Texas State law that provides for greater protections over HIPAA supersedes the associated HIPAA requirement. Thus, it is important for organizations adopting the model security policies to also closely review and consider the Texas standards relating to the confidentiality of information, as described in the prior section.

The table in Appendix B of this document maps the THSA model security policy to the HITRUST Common Security Framework (CSF). Since the THSA model security policy is based on the HIPAA Security Rule, an authoritative source already integrated into the CSF, little change to the CSF was necessary to account for the policies and procedures in this model security policy. Instead, HITRUST's objectives were to provide an accurate and simple mapping between the CSF and the THSA model security policy.

How HITRUST Supports Compliance with HB 300

HITRUST, in its effort to ensure it continues to provide relevant solutions to address information security and compliance in the healthcare industry, has mapped the requirements of HB 300 to the CSF. Since the CSF is not a new standard but rather a framework of security controls that incorporates and references existing standards and regulations applicable to healthcare organizations, HB 300 becomes a new authoritative source within the CSF.

It is important to note that at this time the CSF only addresses security controls and requirements. Many of the other requirements HB 300 are of a business or privacy nature, or specify requirements for State

agencies within Texas. Subsequently these requirements are not mapped to the CSF because they are outside its scope.

Regardless, a full breakdown of the requirements from HB 300 is provided in the table below. Where applicable, the requirement is mapped to the CSF, denoted by the CSF control reference and implementation level, along with any updates or changes that are necessary to fully align with HB 300. Integrating this State regulation into the CSF in this way allows organizations that have, are in process, or are planning to adopt the CSF, to gain confidence that their efforts can address the State's requirements while aligning with other applicable State and Federal regulations, industry standards, and third party business requirements.

TX HB 300	Authoritative Source Reference	Requirements	CSF xRef	CSF Changes
Section 2. Subchapter A	181.004	APPLICABILITY OF STATE AND FEDERAL LAW.	N/A	N/A
	181.004(a)	A covered entity, as that term is defined by 45 C.F.R. Section 160.103, shall comply with the Health Insurance Portability and Accountability Act and Privacy Standards.	All HIPAA xRefs in the CSF.	None noted.
	181.004(b)	Subject to Section 181.051, a covered entity, as that term is defined by Section 181.001, shall comply with this chapter.	N/A	N/A
Section 3.	181.005	DUTIES OF THE EXECUTIVE COMMISSIONER.	N/A	N/A
	181.005(a)	The executive commissioner shall administer this chapter and may adopt rules consistent with the Health Insurance Portability and Accountability Act and Privacy Standards to administer this chapter.	N/A	N/A
	181.005(b)	The executive commissioner shall review amendments to the definitions in 45 C.F.R. Parts 160 and 164 that occur after September 1, 2011, and determine whether it is in the best interest of the state to adopt the amended federal regulations. If the executive commissioner determines that it is in the best interest of the state to adopt the amended federal regulations, the amended regulations shall apply as required by this chapter.	N/A	N/A
	181.005(c)	In making a determination under this section, the executive commissioner must consider, in addition to other factors affecting the public interest, the beneficial and adverse effects the amendments would have on:	N/A	N/A
	181.005(c)(1)	the lives of individuals in this state and their expectations of privacy; and	N/A	N/A

	181.005(c)(2)	governmental entities, institutions of higher education, state-owned teaching hospitals, private businesses, and commerce in this state.	N/A	N/A
	181.005(d)	The executive commissioner shall prepare a report of the executive commissioner's determination made under this section and shall file the report with the presiding officer of each house of the legislature before the 30th day after the date the determination is made. The report must include an explanation of the reasons for the determination.	N/A	N/A
Section 4.	181.006	PROTECTED HEALTH INFORMATION NOT PUBLIC Notwithstanding Sections 181.004 and 181.051, for a covered entity that is a governmental unit, an individual's protected health information: includes any information that reflects that an individual received health care from the covered entity; and; is not public information and is not subject to disclosure under Chapter 552, Government Code.	N/A	N/A
Section 5. Subchapter B	181.059	CRIME VICTIM COMPENSATION This chapter does not apply to any person or entity in connection with providing, administering, supporting, or coordinating any of the benefits regarding compensation to victims of crime as provided by Subchapter B, Chapter 56, Code of Criminal Procedure.	N/A	N/A
Section 6. Subchapter C	181.101	TRAINING REQUIRED	N/A	N/A
	181.101(a)	Each covered entity shall provide a training program to employees of the covered entity regarding the state and federal law concerning protected health information as it relates to:	02.e, Level 1	Awareness training shall commence with a formal induction process designed to introduce the organization's security policies, state and

				federal laws, and expectations before access to information or services is granted.
	181.101(a)(1)	the covered entity's particular course of business; and	02.e, Level 1	None noted.
	181.101(a)(2)	each employee's scope of employment.	02.e, Level 3	None noted.
	181.101(b)	An employee of a covered entity must complete training described by Subsection (a) not later than the 60th day after the date the employee is hired by the covered entity.	02.e, Level 1	Awareness training shall commence with a formal induction process designed to introduce the organization's security policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired.
	181.101(c)	An employee of a covered entity shall receive training described by Subsection (a) at least once every two years.	02.e, Level 2	None noted.
	181.101(d)	A covered entity shall require an employee of the entity who attends a training program described by Subsection (a) to sign, electronically or in writing, a statement verifying the employee's attendance at the training program. The covered entity shall maintain the signed statement.	02.e, Level 2 - employee signoff 02.e, Level 3 - maintenance of records	None noted.
	181.102	CONSUMER ACCESS TO ELECTRONIC HEALTH RECORDS	N/A	N/A

	181.102(a)	Except as provided by Subsection (b), if a health care provider is using an electronic health records system that is capable of fulfilling the request, the health care provider, not later than the 15th business day after the date the health care provider receives a written request from a person for the person's electronic health record, shall provide the requested record to the person in electronic form unless the person agrees to accept the record in another form.	N/A	N/A
	181.102(b)	A health care provider is not required to provide access to a person's protected health information that is excepted from access, or to which access may be denied, under 45 C.F.R. Section 164.524.	N/A	N/A
	181.102(c)	For purposes of Subsection (a), the executive commissioner, in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, by rule may recommend a standard electronic format for the release of requested health records. The standard electronic format recommended under this section must be consistent, if feasible, with federal law regarding the release of electronic health records.	N/A	N/A

	181.103	CONSUMER INFORMATION WEBSITE The attorney general shall maintain an Internet website that provides: information concerning a consumer's privacy rights regarding protected health information under federal and state law; a list of the state agencies, including the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, that regulate covered entities in this state and the types of entities each agency regulates; detailed information regarding each agency's complaint enforcement process; and contact information, including the address of the agency's Internet website, for each agency listed under Subdivision (2) for reporting a violation of this chapter.	N/A	N/A
	181.104	CONSUMER COMPLAINT REPORT BY ATTORNEY GENERAL.	N/A	N/A
	181.104(a)	The attorney general annually shall submit to the legislature a report describing:	N/A	N/A
	181.104(a)(1)	the number and types of complaints received by the attorney general and by the state agencies receiving consumer complaints under Section 181.103; and	N/A	N/A
	181.104(a)(2)	the enforcement action taken in response to each complaint reported under Subdivision (1).	N/A	N/A
	181.104(b)	Each state agency that receives consumer complaints under Section 181.103 shall submit to the attorney general, in the form required by the attorney general, the information the attorney general requires to compile the report required by Subsection (a).	N/A	N/A

	181.104(c)	The attorney general shall de-identify protected health information from the individual to whom the information pertains before including the information in the report required by Subsection (a).	N/A	N/A
Section 7. Subchapter D	181.153	SALE OF PROTECTED HEALTH INFORMATION PROHIBITED; EXCEPTIONS	N/A	N/A
	181.153(a)	A covered entity may not disclose an individual's protected health information to any other person in exchange for direct or indirect remuneration, except that a covered entity may disclose an individual's protected health information:	N/A	N/A
	181.153(a)(1)	to another covered entity, as that term is defined by Section 181.001, or to a covered entity, as that term is defined by Section 602.001, Insurance Code, for the purpose of:	N/A	N/A
	181.153(a)(1)(A)	treatment;	N/A	N/A
	181.153(a)(1)(B)	payment;	N/A	N/A
	181.153(a)(1)(C)	health care operations; or	N/A	N/A
	181.153(a)(1)(D)	performing an insurance or health maintenance organization function described by Section 602.053, Insurance Code; or	N/A	N/A
	181.153(a)(2)	as otherwise authorized or required by state or federal law.	N/A	N/A
	181.153(b)	The direct or indirect remuneration a covered entity receives for making a disclosure of protected health information authorized by Subsection (a)(1)(D) may not exceed the covered entity's reasonable costs of preparing or transmitting the protected health information.	N/A	N/A

	181.154	NOTICE AND AUTHORIZATION REQUIRED FOR ELECTRONIC DISCLOSURE OF PROTECTED HEALTH INFORMATION; EXCEPTIONS		N/A
	181.154(a)	A covered entity shall provide notice to an individual for whom the covered entity creates or receives protected health information if the individual's protected health information is subject to electronic disclosure. A covered entity may provide general notice by:	N/A	N/A
	181.154(a)(1)	posting a written notice in the covered entity's place of business;	N/A	N/A
	181.154(a)(2)	posting a notice on the covered entity's Internet website; or	N/A	N/A
	181.154(a)(3)	posting a notice in any other place where individuals whose protected health information is subject to electronic disclosure are likely to see the notice.	N/A	N/A
	181.154(b)	Except as provided by Subsection (c), a covered entity may not electronically disclose an individual's protected health information to any person without a separate authorization from the individual or the individual's legally authorized representative for each disclosure. An authorization for disclosure under this subsection may be made in written or electronic form or in oral form if it is documented in writing by the covered entity.	N/A	N/A
	181.154(c)	The authorization for electronic disclosure of protected health information described by Subsection (b) is not required if the disclosure is made:	N/A	N/A

	181.154(c)(1)	to another covered entity, as that term is defined by Section 181.001, or to a covered entity, as that term is defined by Section 602.001, Insurance Code, for the purpose of:	N/A	N/A
	181.154(c)(1)(A)	treatment;	N/A	N/A
	181.154(c)(1)(B)	payment;	N/A	N/A
	181.154(c)(1)(C)	health care operations; or	N/A	N/A
	181.154(c)(1)(D)	performing an insurance or health maintenance organization function described by Section 602.053, Insurance Code; or	N/A	N/A
	181.154(c)(2)	as otherwise authorized or required by state or federal law.	N/A	N/A
	181.154(d)	The attorney general shall adopt a standard authorization form for use in complying with this section. The form must comply with the Health Insurance Portability and Accountability Act and Privacy Standards and this chapter.	N/A	N/A
	181.154(e)	This section does not apply to a covered entity, as defined by Section 602.001, Insurance Code, if that entity is not a covered entity as defined by 45 C.F.R. Section 160.103.	N/A	N/A
Section 8.	181.201	N/A	N/A	N/A
	181.201(b)	In addition to the injunctive relief provided by Subsection (a), the attorney general may institute an action for civil penalties against a covered entity for a violation of this chapter. A civil penalty assessed under this section may not exceed:	N/A	N/A
	181.201(b)(1)	$5,000 for each violation that occurs in one year, regardless of how long the violation continues during that year, committed negligently;	N/A	N/A

	181.201(b)(2)	$25,000 for each violation that occurs in one year, regardless of how long the violation continues during that year, committed knowingly or intentionally; or	N/A	N/A
	181.201(b)(3)	$250,000 for each violation in which the covered entity knowingly or intentionally used protected health information for financial gain.	N/A	N/A
	181.201(b-1)	The total amount of a penalty assessed against a covered entity under Subsection (b) in relation to a violation or violations of Section 181.154 may not exceed $250,000 annually if the court finds that the disclosure was made only to another covered entity and only for a purpose described by Section 181.154(c) and the court finds that:	N/A	N/A
	181.201(b-1)(1)	the protected health information disclosed was encrypted or transmitted using encryption technology designed to protect against improper disclosure;	N/A	N/A
	181.201(b-1)(2)	the recipient of the protected health information did not use or release the protected health information; or	N/A	N/A
	181.201(b-1)(3)	at the time of the disclosure of the protected health information, the covered entity had developed, implemented, and maintained security policies, including the education and training of employees responsible for the security of protected health information.	N/A	N/A
	181.201(c)	If the court in which an action under Subsection (b) is pending finds that the violations have occurred with a frequency as to constitute a pattern or practice, the court may assess a civil penalty not to exceed $1.5 million annually	N/A	N/A
	181.201(d)	In determining the amount of a penalty imposed under Subsection (b), the court shall consider:	N/A	N/A

	181.201(d)(1)	the seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure;	N/A	N/A
	181.201(d)(2)	the covered entity's compliance history;	N/A	N/A
	181.201(d)(3)	whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose protected health information is involved in the violation;	N/A	N/A
	181.201(d)(4)	whether the covered entity was certified at the time of the violation as described by Section 182.108;	N/A	N/A
	181.201(d)(5)	the amount necessary to deter a future violation; and	N/A	N/A
	181.201(d)(6)	the covered entity's efforts to correct the violation.	N/A	N/A
	181.201(e)	The attorney general may institute an action against a covered entity that is licensed by a licensing agency of this state for a civil penalty under this section only if the licensing agency refers the violation to the attorney general under Section 181.202(2).	N/A	N/A
	181.201(f)	The office of the attorney general may retain a reasonable portion of a civil penalty recovered under this section, not to exceed amounts specified in the General Appropriations Act, for the enforcement of this subchapter.	N/A	N/A

Section 9.	181.202	DISCIPLINARY ACTION In addition to the penalties prescribed by this chapter, a violation of this chapter by a covered entity that is licensed by an agency of this state is subject to investigation and disciplinary proceedings, including probation or suspension by the licensing agency. If there is evidence that the violations of this chapter are egregious and constitute a pattern or practice, the agency may: revoke the covered entity's license; or refer the covered entity's case to the attorney general for the institution of an action for civil penalties under Section 181.201(b).	N/A	N/A
Section 10.	181.205	N/A	N/A	N/A
	181.205(b)	In determining the amount of a penalty imposed under other law in accordance with Section 181.202, a court or state agency shall consider the following factors:	N/A	N/A
	181.205(b)(1)	the seriousness of the violation, including the nature, circumstances, extent, and gravity of the disclosure;	N/A	N/A
	181.205(b)(2)	the covered entity's compliance history;	N/A	N/A
	181.205(b)(3)	whether the violation poses a significant risk of financial, reputational, or other harm to an individual whose protected health information is involved in the violation;	N/A	N/A
	181.205(b)(4)	whether the covered entity was certified at the time of the violation as described by Section 182.108;	N/A	N/A
	181.205(b)(5)	the amount necessary to deter a future violation; and	N/A	N/A
	181.205(b)(6)	the covered entity's efforts to correct the violation.	N/A	N/A

	181.205(c)	On receipt of evidence under Subsections (a) and (b), a court or state agency shall consider the evidence and mitigate imposition of an administrative penalty or assessment of a civil penalty accordingly.	N/A	N/A
Section 11.	181.206	AUDITS OF COVERED ENTITIES	N/A	N/A
	181.206(a)	The commission, in coordination with the attorney general, the Texas Health Services Authority, and the Texas Department of Insurance:	N/A	N/A
	181.206(a)(1)	may request that the United States secretary of health and human services conduct an audit of a covered entity, as that term is defined by 45 C.F.R. Section 160.103, in this state to determine compliance with the Health Insurance Portability and Accountability Act and Privacy Standards; and	N/A	N/A
	181.206(a)(2)	shall periodically monitor and review the results of audits of covered entities in this state conducted by the United States secretary of health and human services.	N/A	N/A
	181.206(b)	If the commission has evidence that a covered entity has committed violations of this chapter that are egregious and constitute a pattern or practice, the commission may:	N/A	N/A
	181.206(b)(1)	require the covered entity to submit to the commission the results of a risk analysis conducted by the covered entity if required by 45 C.F.R. Section 164.308(a)(1)(ii)(A); or	N/A	N/A
	181.206(b)(2)	if the covered entity is licensed by a licensing agency of this state, request that the licensing agency conduct an audit of the covered entity's system to determine compliance with the provisions of this chapter.	N/A	N/A

	181.206(c)	The commission annually shall submit to the appropriate standing committees of the senate and the house of representatives a report regarding the number of federal audits of covered entities in this state and the number of audits required under Subsection (b).	N/A	N/A
	181.207	FUNDING The commission and the Texas Department of Insurance, in consultation with the Texas Health Services Authority, shall apply for and actively pursue available federal funding for enforcement of this chapter.	N/A	N/A
Section 12.	182.002			N/A
	182.002(2-a)	"Covered entity" has the meaning assigned by Section 181.001.	N/A	N/A
	182.002(3-a)	"Disclose" has the meaning assigned by Section 181.001.	N/A	N/A
	182.002(3-b)	"Health Insurance Portability and Accountability Act and Privacy Standards" has the meaning assigned by Section 181.001.	N/A	N/A
Section 13. Subchapter C	182.108	STANDARDS FOR ELECTRONIC SHARING OF PROTECTED HEALTH INFORMATION; COVERED ENTITY CERTIFICATION	N/A	N/A
	182.108(a)	The corporation shall develop and submit to the commission for ratification privacy and security standards for the electronic sharing of protected health information.	N/A	N/A
	182.108(b)	The commission shall review and by rule adopt acceptable standards submitted for ratification under Subsection (a).	N/A	N/A
	182.108(c)	Standards adopted under Subsection (b) must be designed to:	N/A	N/A

	182.108(c)(1)	comply with the Health Insurance Portability and Accountability Act and Privacy Standards and Chapter 181;	N/A	N/A
	182.108(c)(2)	comply with any other state and federal law relating to the security and confidentiality of information electronically maintained or disclosed by a covered entity;	N/A	N/A
	182.108(c)(3)	ensure the secure maintenance and disclosure of personally identifiable health information;	N/A	N/A
	182.108(c)(4)	include strategies and procedures for disclosing personally identifiable health information; and	N/A	N/A
	182.108(c)(5)	support a level of system interoperability with existing health record databases in this state that is consistent with emerging standards.	N/A	N/A
	182.108(d)	The corporation shall establish a process by which a covered entity may apply for certification by the corporation of a covered entity's past compliance with standards adopted under Subsection (b).	N/A	N/A
	182.108(e)	The corporation shall publish the standards adopted under Subsection (b) on the corporation's Internet website.	N/A	N/A
Section 14.	521.053(b)	A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security, after discovering or receiving notification of the breach, to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made as quickly as possible, except as provided by Subsection (d) or as necessary to determine the scope of the breach and restore the reasonable integrity of the data	11.a, Level 1	None noted.

		system.		
	521.053(b-1)	Notwithstanding Subsection (b), the requirements of Subsection (b) apply only if the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of this state or another state that does not require a person described by Subsection (b) to notify the individual of a breach of system security. If the individual is a resident of a state that requires a person described by Subsection (b) to provide notice of a breach of system security, the notice of the breach of system security provided under that state's law satisfies the requirements of Subsection (b).	11.a, Level 1	None noted.
Section 15.	521.151(a-1)	In addition to penalties assessed under Subsection (a), a person who fails to take reasonable action to comply with Section 521.053(b) is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due under that subsection for each consecutive day that the person fails to take reasonable action to comply with that subsection. Civil penalties under this section may not exceed $250,000 for all individuals to whom notification is due after a single breach. The attorney general may bring an action to recover the civil penalties imposed under this subsection.	N/A	N/A

Section 16.	522.002(b)	An offense under this section is a Class B misdemeanor, except that the offense is a state jail felony if the information accessed, read, scanned, stored, or transferred was protected health information as defined by the Health Insurance Portability and Accountability Act and Privacy Standards, as defined by Section 181.001, Health and Safety Code.	N/A	N/A
Section 17. Subchapter B	531.0994	STUDY; ANNUAL REPORT		
	531.0994(a)	The commission, in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, shall explore and evaluate new developments in safeguarding protected health information.	N/A	N/A
	531.0994(b)	Not later than December 1 each year, the commission shall report to the legislature on new developments in safeguarding protected health information and recommendations for the implementation of safeguards within the commission.	N/A	N/A
Section 18. Subchapter B	602.054	COMPLIANCE WITH OTHER LAW A covered entity shall comply with: Subchapter D, Chapter 181, Health and Safety Code, except as otherwise provided by that subchapter; and the standards adopted under Section 182.108, Health and Safety Code.	Privacy reqs. N/A	N/A

Green text within the proposed changes column denotes additions that will be made to the 2013 version of the CSF in support of compliance with the requirement.

HITRUST
Health Information Trust Alliance

Appendix A – Detailed Listing of the Standards Required for the Secure Electronic Exchange of Health Information

The table includes the name of the standard, a summary of the standard, the Federal or State scope of the standard, the applicability of the standard, and a link to more information (i.e., the source text of the standard).

390.2 Standards	Summary	Scope	Applicability	More Info
HIPAA Privacy, Security and Breach Notification Regulations	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or Standards for Privacy of Individually Identifiable Health Information, establishes national standards for the protection of certain health information. The Security Standards for the Protection of Electronic Protected Health Information (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronic protected health information" (e-PHI). Within HHS, the Office for Civil Rights (OCR) has responsibility for enforcing the Privacy and Security Rules with voluntary compliance	Federal	The Privacy, Security and Breach Notification Rules, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities"). The HITECH Act of 2009 expanded the responsibilities of business associates under the Privacy, Security and Breach Notification Rules.	http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

	activities and civil money penalties.			
Texas Medical Records Act, Chapter 181 of the Texas Health and Safety Code	The Act sets limits on who gets to see a patient's personal information, how medical providers can use personal information, requires providers to disclose to whom personal health information has been given, and review and correct information in medical records upon request.	State: Texas	Entities that for commercial, financial, or professional gain, monetary fees, or dues, or on a cooperative, nonprofit, or pro bono basis, engages, in whole or in part, and with real or constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information. The term includes a business associate, health care payer, governmental unit, information or computer management entity, school, health researcher, health care facility, clinic, health care provider, or person who maintains an Internet site.	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.181.htm
Texas Identity Theft Act, Chapter 521 of the Texas Business and Commerce Code	The Act states that businesses have a legal duty to protect and safeguard sensitive personal information. The Act requires businesses that collect or maintain sensitive personal information in the regular course of business to implement and maintain reasonable procedures and corrective measures to protect and safeguard that information from unlawful disclosure or use.	State: Texas	Businesses that collect or maintain sensitive personal information of Texas residents.	http://www.statutes.legis.state.tx.us/Docs/BC/htm/BC.521.htm

Texas Health and Safety Code §82.008	Grants the Texas Board of Health (the "board") the authority to establish a Texas Cancer Registry ("registry") and specifically allows the board to request and obtain a copy of a health care facility's master patient index so that it may determine if all cancer cases were correctly identified and reported to the registry.	State: Texas	Cancer data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.82.htm#82.008
Texas Health and Safety Code §82.009	Pursuant to Texas Health and Safety Code, Chapter 82, §82.008, Chapter 82, §82.009 specifies that reports, records, and information obtained by the board for the registry are for the confidential use of the Texas Department of Health and the persons or public or private entities that the department determines are necessary to carry out the intent of this chapter.	State: Texas	Cancer data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.82.htm#82.009
Title 25 Texas Administrative Code (TAC) §91.9	Pursuant to Texas Health and Safety Code, Chapter 82, §82.009, Texas Administrative Code §91.9 specifies that all data obtained is for the confidential use of the department and the persons or entities, public or private, that the department determines are necessary to carry out the intent of the Act.	State: Texas	Cancer data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=91&rl=9
Texas Health and Safety Code §81.103	Specifies that a test result, specifically related to HIV and AIDS tests, is confidential and that a person that possesses or has knowledge of a test result may not release or disclose the test result or allow the test result to become known. Certain exceptions are listed.	State: Texas	HIV/AIDS data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.81.htm

Title 40 TAC §8.288 (relating to Confidentiality of Test Results)	Specifies that the results of HIV tests are confidential by law. Specifically reports, records, and information may not be released or made public except as provided by the Texas Health and Safety Code, §§81.103, 81.104, and §85.115, which sets forth strict penalties for violations.	State: Texas	HIV/AIDS data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=40&pt=1&ch=8&rl=288
Genetic Information Nondiscrimination Act of 2008 (GINA) Pub. L. No. 110-233 (including applicable regulations promulgated under that act)	The Act prohibits the discrimination of individuals on the basis of genetic information with respect to health insurance and employment. This Act modifies the Employee Retirement Income Security Act of 1974, the Public Health Service Act, Internal Revenue Code of 1986, and title XVIII of the Social Security Act relating to Medigap. As it relates to the HIPAA Privacy Rule, genetic information shall be treated as protected health information.	Federal	Genetic data	http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf
Texas Insurance Code, Chapter 546, Subchapter C;	Specifies that genetic information is confidential and privileged regardless of the source of the information, and a person or entity that holds genetic information about an individual may not disclose or be compelled to disclose, by subpoena or otherwise, that information unless the disclosure is to the individual, a physician designated by the individual, or otherwise authorized by the individual as provided by Section 546.104.	State: Texas	Genetic data	http://www.statutes.legis.state.tx.us/Docs/IN/htm/IN.546.htm

Texas Labor Code §21.403	Specifies that genetic information is confidential and privileged regardless of the source of the information, and a person or entity that holds genetic information about an individual may not disclose or be compelled to disclose, by subpoena or otherwise, that information unless the disclosure is to the individual, a physician designated by the individual, or otherwise authorized by the individual as provided by Section 21.4032.	State: Texas	Genetic data	http://www.statutes.legis.state.tx.us/Docs/LA/htm/LA.21.htm
Texas Labor Code §21.404	Specifies that an individual who submits to a genetic test has the right to know the results of the test. On the written request by the individual, the entity that performed the test shall disclose the test results to the individual or a physician designated by the individual.	State: Texas	Genetic data	http://www.statutes.legis.state.tx.us/Docs/LA/htm/LA.21.htm
Texas Occupations Code, Chapter 58	Specifies that licensing authorities may not deny an application for an occupational license, suspend, revoke, or refuse to renew an occupational license, or take any other disciplinary action against a license holder based on the refusal of the license applicant or license holder to submit to genetic testing or disclose the results of any testing performed in the past. Further specifies that an individual who submits to a genetic test has the right to know the results of the test (see Texas Labor Code §21.404), and genetic information is confidential and privileged (see Texas Labor Code §21.403).	State: Texas	Genetic data	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.58.htm

Texas Health and Safety Code, Chapter 44, Subchapter C	Specifies that a record of the identity, personal history, or background information of a survivor or information and communications concerning the victimization of a survivor of sexual assault that is created by or provided to an advocate or maintained by a sexual assault program is confidential and may not be disclosed, with select exceptions noted.	State: Texas	Sexual assault data	http://law.justia.com/codes/texas/2005/hs/002.00.000044.00.html
Texas Health and Safety Code §81.046	Specifies that reports, records, and information relating to cases or suspected cases of diseases or health conditions are confidential and not public information and may not be released or made public on subpoena or otherwise except as provided by Subsections of this Chapter.	State: Texas	Communicable diseases data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.81.htm
Title 25 TAC §97.10 (relating to Confidential Nature of Case Reporting and Records)	Specifies that all individual morbidity case reports received by the health authority or the Department of State Health Services (department) are confidential records and not public records.	State: Texas	Communicable diseases data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=97&rl=10
Texas Health and Safety Code, Chapter 611, Mental Health Records / Substance Abuse Records	Specifies that communications between a patient and a professional for diagnosis, evaluation, or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction, and records of the identity, diagnosis, evaluation, or treatment of a patient that are created or maintained by a professional, are confidential. Exceptions permitting the disclosure in select instance are provided by Sections 611.004 or 611.0045.	State: Texas	Mental health data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.611.htm

42 CFR Part 2, Confidentiality of Alcohol and Drug Abuse Patient Records	Under the statutory provisions quoted in §§ 2.1 and 2.2, these regulations impose restrictions upon the disclosure and use of alcohol and drug abuse patient records which are maintained in connection with the performance of any federally assisted alcohol and drug abuse program. The regulations specify: (1) Definitions, applicability, and general restrictions in subpart B (definitions applicable to § 2.34 only appear in that section); (2) Disclosures which may be made with written patient consent and the form of the written consent in subpart C; (3) Disclosures which may be made without written patient consent or an authorizing court order in subpart D; and (4) Disclosures and uses of patient records which may be made with an authorizing court order and the procedures and criteria for the entry and scope of those orders in subpart E.	Federal	Substance abuse or substance use disorder data	http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl
Texas Health and Safety Code, Chapter 611, Mental Health Records/ Substance Abuse Records	Specifies that communications between a patient and a professional for diagnosis, evaluation, or treatment of any mental or emotional condition or disorder, including alcoholism or drug addiction, and records of the identity, diagnosis, evaluation, or treatment of a patient that are created or maintained by a professional, are confidential. Exceptions permitting the disclosure in select instance are	State: Texas	Substance abuse or substance use disorder data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.611.htm

	provided by Sections 611.004 or 611.0045.			
Texas Health and Safety Code §161.0073	Specifies that, except as provided by Sections 161.00705 and 161.00735, information that individually identifies an individual that is received by the department for the immunization registry is confidential and may be used by the department for registry purposes only.	State: Texas	Immunizations data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.161.htm
Texas Health and Safety Code §161.009	Specifies penalties for the unauthorized disclosure of immunization registry information received by the department.	State: Texas	Immunizations data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.161.htm
Title 25 TAC §100.2 (relating to Confidentiality)	Specifies that, except as provided by Health and Safety Code, Chapter 161, Subchapter A, §161.00705, information that individually identifies a child or other individual, and is received by the department for the immunization registry, is confidential and may be used by the department for registry purposes only.	State: Texas	Immunizations data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=T&app=9&p_dir=N&p_rloc=137401&p_tloc=&p_ploc=1&pg=8&p_tac=&ti=25&pt=1&ch=100&rl=1
Texas Government Code §552.115	Specifies when birth and death records are made publicly available (after the 75th anniversary and 25th anniversary respectively) and that until public the information is labeled confidential and maintained securely by the Bureau of Vital Statistics of the Texas Department of Health.	State: Texas	Bureau of Vital Statistics data	http://codes.lp.findlaw.com/txstatutes/GV/5/A/552/C/552.115

Texas Health and Safety Code Chapters 192 and 193, §195.005	Specifies that the section of the birth certificate entitled "For Medical and Health Use Only" is not part of the legal birth certificate and that information held under that section is confidential. Further specifies that an individual who knowingly discloses that information, causes another to disclose the information, or otherwise fails to comply with the rule commits an offense that is classified as a Class A misdemeanor.	State: Texas	Bureau of Vital Statistics data	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.195.htm
Title 25 TAC Chapter 181 (relating to Vital Statistics)	As it relates to Vital Statistics, specifies that copies of birth records are available to the public for searching or inspection on or after the 75th anniversary of the date of birth as shown on the record filed with the bureau or the local registration official.	State: Texas	Bureau of Vital Statistics data	http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=5&ti=25&pt=1&ch=181&sch=A&rl=Y
Texas Human Resources Code, Chapter 48, Report of Abuse or Neglect of Elderly or Disabled Persons	The purpose of this chapter is to provide for the authority to investigate the abuse, neglect, or exploitation of an elderly or disabled person and to provide protective services to that person. With exceptions provided, all files, reports, records, communications, and working papers used or developed in an investigation made under this chapter or in providing services as a result of an investigation are considered confidential.	State: Texas	Reports of abuse or neglect	http://www.statutes.legis.state.tx.us/Docs/HR/htm/HR.48.htm

Texas Health and Safety Code §161.132	Specifies that any person, including an employee, volunteer, or other person associated with an inpatient mental health facility, a treatment facility, or a hospital that provides comprehensive medical rehabilitation services, who reasonably believes or who knows of information that would reasonably cause a person to believe that the physical or mental health or welfare of a patient or client of the facility who is receiving chemical dependency, mental health, or rehabilitation services has been, is, or will be adversely affected by abuse or neglect caused by any person shall as soon as possible report the information supporting the belief to the agency that licenses the facility or to the appropriate state health care regulatory agency.	State: Texas	Data related to reports of abuse or neglect	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.161.htm#161.132
Family Code Chapter 261, Reports of Child Abuse	With exceptions provided, the files, reports, records, communications, audiotapes, videotapes, and working papers used or developed in an investigation of the adverse effect of a child's physical or mental health or welfare due to abuse or neglect or in providing services as a result of an investigation are confidential.	Federal	Data related to reports of child abuse or neglect	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.261.htm
Internal Revenue Code, Title 26, 26 U.S.C. §6103	Tax returns and return information shall be confidential, and except as authorized by this title, no individual shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section.	Federal	Federal tax information data	http://www.gpo.gov/fdsys/pkg/USCODE-2011-title26/html/USCODE-2011-title26-subtitleF-chap61-subchapB-sec6103.htm

IRS Publication 1075	This publication provides guidance in ensuring that the policies, practices, controls, and safeguards employed by recipient agencies or agents and contractors adequately protect the confidentiality of the information they receive from the IRS. Enterprise security policies shall address the purpose, scope, responsibilities, and management commitment to implement all applicable security controls including managerial, operational, and technical security controls.	Federal	Federal tax information data	http://www.irs.gov/pub/irs-pdf/p1075.pdf
42 U.S.C. §1306, 20 CFR Part 401	Specifies that, except as permitted by the Privacy Act and the regulations in this part, or when required by the Freedom of Information Act, the Social Security Administration will not disclose personal records without the individual's written consent.	Federal	Social Security Administration data	http://www.law.cornell.edu/cfr/text/20/401/subpart-C
Texas Health and Safety Code §84.006	Specifies that all information and records relating to reportable conditions are confidential. The information may not be released or made public on subpoena or otherwise, with exceptions noted. Further specifies that the board shall adopt rules establishing procedures to ensure that all information and records maintained by the department under this chapter are kept confidential and protected from release to unauthorized persons.	State: Texas	Occupational diseases data	http://www.weblaws.org/texas/laws/tex._health_and_safety_code_section_84.006_confidentiality

25 TAC §99.1 (relating to General Provisions)	Authorizes the Executive Commissioner of the Health and Human Services Commission to adopt rules concerning the reporting and control of occupational conditions. Specifies that all case reports received by the local health authority or the Department of State Health Services are confidential records and not public records. These records will be held in a secure location and accessed only by authorized personnel.	State: Texas	Occupational diseases data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=99&rl=1
25 TAC §56.11 (relating to Confidentiality)	Specifies that providers shall safeguard client family planning information. Clients must provide written authorization prior to the release of any personally identifying information except reports of child abuse required by Texas Family Code, Chapter 261, and as required or authorized by other law.	State: Texas	Family planning data	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=56&rl=11
7 CFR §272 (SNAP)	Specifies that the use or disclosure of information obtained from food stamp applicant or recipient households shall be restricted to authorized individuals listed.	Federal	Recipients of government benefits data	http://www.law.cornell.edu/cfr/text/7/272.1
45 CFR §205.50 (TANF)	Specifies that a state plan for financial assistance under title IV-A of the Social Security Act, must provide that the use or disclosure of information concerning applicants and recipients will be limited to authorized purposes.	Federal	Recipients of government benefits data	http://www.gpo.gov/fdsys/pkg/CFR-2008-title45-vol2/xml/CFR-2008-title45-vol2-sec205-50.xml

42 CFR §431.300 et. seq. (Medicaid)	Specifies that a State plan must provide safeguards that restrict the use or disclosure of information concerning applicants and recipients to purposes directly connected with the administration of the plan. This subpart specifies State plan requirements, the types of information to be safeguarded, the conditions for release of safeguarded information, and restrictions on the distribution of other information.	Federal	Recipients of government benefits data	http://www.law.cornell.edu/cfr/text/42/431.300
42 CFR §457.1110 (CHIP)	Specifies that the state must ensure that, for individual medical records and any other health and enrollment information maintained with respect to enrollees, that identifies particular enrollees (in any form), the state establishes and implements procedures to abide by all applicable Federal and State laws regarding confidentiality and disclosure, including those laws addressing the confidentiality of information about minors and the privacy of minors, and privacy of individually identifiable health information.	Federal	Recipients of government benefits data	http://www.gpo.gov/fdsys/pkg/CFR-2009-title42-vol4/xml/CFR-2009-title42-vol4-sec457-1110.xml
Texas Health and Safety Code, Chapter 241, Subchapter G, Hospital Disclosures of Health Care Information	Specifies that except as authorized by Section 241.153, a hospital or an agent or employee of a hospital may not disclose health care information about a patient to any person other than the patient or the patient's legally authorized representative without the written authorization of the patient or the patient's legally authorized representative.	State: Texas	Hospitals	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.241.htm

25 TAC §133.42 (relating to Patient Rights)	Specifies that a hospital shall adopt, implement, and enforce a policy to ensure patients' rights. The written policy shall include, among other items, the right of the patient, within the limits of law, to personal privacy and confidentiality of information;	State: Texas	Hospitals	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=133&rl=42
Texas Health and Safety Code, Chapter 242, §242.134 and §242.501(8), Nursing Home Resident Rights	Specifies that the department by rule shall adopt a statement of the rights of a resident. This includes having information about the resident in the possession of the institution maintained as confidential.	State: Texas	Nursing facilities	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.242.htm
40 TAC §19.407 (relating to Privacy and Confidentiality)	Specifies that the resident has the right to personal privacy and confidentiality of his personal and clinical records. Personal privacy includes accommodations, medical treatment, written and telephone communications, personal care, visits, and meetings of family and resident groups, but this does not require the facility to provide a private room for each resident.	State: Texas	Nursing facilities	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=40&pt=1&ch=19&rl=407
Texas Health and Safety Code, Chapter 252, §252.126	Specifies that a report, record, or working paper used or developed in an investigation made under this subchapter is confidential and may be disclosed only as provided by Chapter 48, Human Resources Code, Chapter 261, Family Code, or this section.	State: Texas	Intermediate care facilities for persons with an intellectual disability or related conditions (ICF/IID)	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.252.htm
Texas Health and Safety Code, Chapter 252, §252.134	Specifies that a facility licensed under this chapter shall submit a report to the department concerning the death of a resident or former resident. Further specifies that the reports are confidential and not subject to the	State: Texas	Intermediate care facilities for persons with an intellectual disability or related conditions (ICF/IID)	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.252.htm

	provisions of Chapter 552, Government Code.			
Texas Health and Safety Code Chapter 254	Specifies the requirements to establish or operate a freestanding emergency medical care facility in the state of Texas.	State: Texas	Freestanding emergency medical care facilities	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.254.htm
25 TAC §131.53 (relating to Medical Records)	Specifies that the facility shall develop and maintain a system for the collection, processing, maintenance, storage, retrieval, authentication, and distribution of patient medical records. Further specifies that any record that contains clinical, social, financial, or other data on a patient shall be strictly confidential and shall be protected from loss, tampering, alteration, improper destruction, and unauthorized or inadvertent disclosure.	State: Texas	Freestanding emergency medical care facilities	http://info.sos.state.tx.us/pls/pub/regviewer$ext.RegPage?sl=R&app=1&p_dir=&p_rloc=219893&p_tloc=&p_ploc=&pg=1&p_reg=219893&ti=25&pt=1&ch=131&rl=53&issue=05/28/2010&z_chk=
Texas Health and Safety Code, Chapter 243, 25 TAC §135.5 (relating to Patient Rights)	Specifies that patients shall be provided appropriate privacy, and that patient records shall be treated confidentially and, except when authorized by law, patients shall be given the opportunity to approve or refuse their release.	State: Texas	Ambulatory surgical centers	http://info.sos.state.tx.us/pls/pub/regviewer$ext.RegPage?sl=R&app=1&p_dir=&p_rloc=199838&p_tloc=&p_ploc=&pg=1&p_reg=199838&ti=25&pt=1&ch=135&rl=5&issue=06/12/2009&z_chk=
Texas Health and Safety Code, Chapter 773, §§773.079-773.096	Specifies that a communication between certified emergency medical services personnel or a physician providing medical supervision and a patient, and records of the identity, evaluation, or treatment of a patient, that are made or created in the course of providing emergency medical services to the patient is confidential and privileged and may not be disclosed except as provided by this chapter.	State: Texas	Emergency medical services	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.773.htm

25 TAC 157.11 (relating to Requirements for an EMS Provider License)	Specifies the requirements for issuing and maintaining an EMS Provider License issued by the Texas Health Services Department.	State: Texas	Emergency medical services	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=157&rl=11
Texas Occupations Code, Chapter 159, Physician-Patient Communication	Specifies that a communication between a physician and a patient, relative to or in connection with any professional services as a physician to the patient, is confidential and privileged and may not be disclosed except as provided by this chapter.	State: Texas	Physicians	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.159.htm
Texas Occupations Code §§201.402 - 201.405, Chiropractor-Patient Confidentiality	Specifies that a communication between a chiropractor and a patient, and records of the identity, evaluation, or treatment of a patient, relating to or in connection with any professional services provided by a chiropractor to the patient is confidential and privileged and may not be disclosed except as provided by this chapter.	State: Texas	Chiropractors	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.201.htm
Texas Occupations Code §258.051 et seq., Dental-Patient Confidentiality	Specifies that the records of a diagnosis made and treatment performed for and on a dental patient are the property of the dentist performing the dental service and that the dentist's records may not be sold, pledged as collateral, or transferred to any person other than the patient unless the transfer is made in compliance with Subchapter C and board rules.	State: Texas	Dentists	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.258.htm

Clinical Laboratory Improvement Amendments (CLIA) (1988)	Congress passed the Clinical Laboratory Improvement Amendments (CLIA) in 1988 establishing quality standards for all laboratory testing to ensure the accuracy, reliability and timeliness of patient test results regardless of where the test was performed. Specifically, the laboratory must ensure confidentiality of patient information throughout all phases of the total testing process that are under the laboratory's control.	Federal	Laboratories	http://wwwn.cdc.gov/clia/regs/toc.aspx
42 CFR §493.1291	Specifies that the laboratory must have an adequate manual or electronic system(s) in place to ensure test results and other patient-specific data are accurately and reliably sent from the point of data entry (whether interfaced or entered manually) to final report destination, in a timely manner.	Federal	Laboratories	http://www.gpo.gov/fdsys/pkg/CFR-2011-title42-vol5/xml/CFR-2011-title42-vol5-sec493-1291.xml
Texas Occupations Code, Chapter 562, §562.052, Confidential Records of Pharmacists	Specifies that a confidential record is privileged and a pharmacist may release a confidential record only to authorized individuals as listed.	State: Texas	Pharmacists	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.562.htm
Texas Occupations Code, Chapter 202, Subchapter I, §202.401 et seq., Podiatrist Privilege and Confidentiality	Specifies that communications that relates to or is in connection with professional services provided by a podiatrist for a patient, and records of the identity, diagnosis, evaluation, or treatment of a patient by a podiatrist that are created or maintained by a podiatrist, are confidential and privileged and may not be disclosed except as provided by this subchapter.	State: Texas	Podiatrists	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.202.htm

Health Breach Notification Rule for Vendors of Personal Health Records, 16 CFR Part 318	The Recovery Act requires ‘‘vendors of personal health records’’ and ‘‘PHR related entities,’’ as defined below, to notify their customers of any breach of unsecured, individually identifiable health information. Further, a third party service provider of such vendors or entities that experiences a breach must notify such vendors or entities of the breach, so that they can in turn notify their customers. The Act contains specific requirements governing the timing, method, and contents of the breach notice to consumers.	Federal	Personal health record vendors	http://www.ftc.gov/os/2009/08/R911002hbn.pdf
Texas Health and Safety Code §251.011	Specifies that except as provided by Section 251.012, a person may not operate an end stage renal disease facility without a license issued under this chapter.	State: Texas	End stage renal disease facilities	http://www.statutes.legis.state.tx.us/Docs/HS/pdf/HS.251.pdf
25 TAC §117.42 (relating to Patient Rights)	Specifies that each end stage renal disease facility shall adopt, implement, and enforce policies and procedures appropriate to the patient population served which ensure each patient is provided privacy and confidentiality, for the patient and the clinical record, among other requirements.	State: Texas	End stage renal disease facilities	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=117&rl=42
25 TAC §125.33 (relating to Resident Rights)	Specifies that each special care facility shall promote and protect the rights of all residents. Policies that ensure resident rights shall be adopted, implemented and enforced. This includes the right of the resident, within the limits of law, to personal privacy and confidentiality of information.	State: Texas	Special care facilities (AIDS)	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=125&rl=33
Texas Health and Safety Code §577.013	Specifies that the department may make investigations it considers necessary and proper to obtain compliance with this subtitle and the department's rules and standards.	State: Texas	Private psychiatric hospitals and crisis stabilization units	http://www.statutes.legis.state.tx.us/Docs/HS/htm/HS.577.htm

25 TAC Chapter 134 (relating to Private Psychiatric Hospitals and Crisis Stabilization Units)	The purpose of this chapter is to implement the Private Mental Hospitals and Other Mental Health Facilities licensing Act, Health and Safety Code, Chapter 577, which requires mental hospitals and mental health facilities that provide court-ordered mental health services to be licensed by the Texas Department of Health. This chapter provides definitions, and establishes licensing procedures, operational requirements, standards for voluntary agreements, enforcement procedures, fire prevention and safety requirements, and physical plant and construction requirements for private psychiatric hospitals and crisis stabilization units.	State: Texas	Private psychiatric hospitals and crisis stabilization units	http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=4&ti=25&pt=1&ch=134
25 TAC §137.53 (relating to Clinical Records)	Specifies that birthing centers must adopt, implement, enforce and maintain a clinical record system to assure that the care and services provided to each client is completely and accurately documented, and systematically organized to facilitate the compilation and retrieval of information. Specifically the centers shall ensure that each client's record is treated with confidentiality, safeguarded against loss and unofficial use, and is maintained according to professional standards of practice.	State: Texas	Birthing centers	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=137&rl=53
Texas Occupations Code §504.251	Specifies the grounds for license, registration, or certification denial or disciplinary action.	State: Texas	Licensed chemical dependency counselors and treatment facilities	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.504.htm

25 TAC §140.424 (relating to Standards for Private Practice)	Specifies the standards and requirements for counseling records of a licensed chemical dependency counselor's private practice. Specifically the counselor shall comply with all applicable state and federal laws relating to confidentiality and any electronic services shall comply with applicable law and accepted security standards.	State: Texas	Licensed chemical dependency counselors and treatment facilities	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=140&rl=424
Texas Health and Safety Code, Chapter 464	Specifies that a person may not offer or purport to offer chemical dependency treatment without a license issued under this subchapter, unless the person is exempted under Subchapter C or is working for or providing counseling with a program exempted under Subchapter C.	State: Texas	Licensed chemical dependency counselors and treatment facilities	http://www.statutes.legis.state.tx.us/Docs/HS/pdf/HS.464.pdf
25 TAC Chapter 448 (relating to Standard of Care)	Specifies that the provider shall provide adequate and appropriate services consistent with best practices and industry standards. Specifically the provider shall protect the privacy of individuals served and shall not disclose confidential information without express written consent, except as permitted by law.	State: Texas	Licensed chemical dependency counselors and treatment facilities	http://info.sos.state.tx.us/pls/pub/readtac$ext.ViewTAC?tac_view=5&ti=25&pt=1&ch=448&sch=B&rl=Y
25 TAC §140.514 (relating to Disciplinary Actions)	Specifies that the department is authorized to take disciplinary actions for the violation of any provisions of the Medical Radiologic Technologist Certification Act (Act) or this chapter. Specifically that disciplinary action may be taken for disclosing confidential information concerning a patient or client except where required or allowed by law.	State: Texas	Medical radiologic technologists	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=140&rl=514
25 TAC §140.586 (relating to Code of Ethics, Duties	Specifies that a license holder shall comply with the requirements, as listed, in the provision of professional services.	State: Texas	Dyslexia therapists and dyslexia practitioners	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=

and Responsibilities of License Holders)				9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=140&rl=586
25 TAC §146.11 (relating to Professional and Ethical Standards)	Establishes the standards of professional and ethical conduct required of an instructor, training program, promotor(a) or community health worker pursuant to the Health and Safety Code, Chapter 48. Specifically that an instructor, promotor(a) or community health worker shall not violate any provision of any federal or state statute relating to confidentiality of patient/client communication and/or records.	State: Texas	Promotors or community health workers	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=146&rl=11
Texas Family Code §§32.003	Specifies that a child may consent to medical, dental, psychological, and surgical treatment for the child by a licensed physician or dentist and the circumstances under which this may occur.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.32.htm
Texas Family Code §§32.004	Specifies that a child may consent to counseling and the circumstances under which this may occur.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.32.htm
Texas Family Code §151.003	Specifies that a state agency may not adopt rules or policies or take any other action that violates the fundamental right and duty of a parent to direct the upbringing of the parent's child.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.151.htm
Texas Family Code §153.073	Specifies the rights of a parent appointed as a conservator of a child, unless limited by court order. This includes access to medical, dental, psychological, and educational records of the child.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.153.htm

Texas Family Code §153.074	Specifies the rights and duties of a parent appointed as a conservator of a child during the period that the parent has possession of the child.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.153.htm
Texas Family Code §153.132	Specifies the exclusive rights and duties of a parent appointed as sole managing conservator of a child.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/FA/htm/FA.153.htm
Texas Occupations Code §159.005	Specifies that consent for the release of confidential information must be in writing and signed by the patient, the parent or legal guardian of the patient, an attorney ad litem appointed for the patient, or a personal representative of the patient if the patient is deceased.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/OC/htm/OC.159.htm
Texas Civil Practice and Remedies Code §129.001	Specifies that the age of majority in the state of Texas is 18 years.	State: Texas	Minors	http://www.statutes.legis.state.tx.us/Docs/CP/htm/CP.129.htm
25 TAC §38.5 (relating to Rights and Responsibilities of a Client's Parents, Foster Parents, Guardian, or Managing Conservator, or an Adult Client)	Specifies the rights of a client's parents, foster parents, guardian, or managing conservator, or an adult client. This includes having all client files and other information maintained in a confidential manner to the extent authorized by law.	State: Texas	Children with Special Health Care Needs	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=38&rl=5

25 TAC §33.30 (relating to Confidentiality of Records).	Specifies that Federal and state laws and regulations prohibit the disclosure of information about Medicaid clients without effective consent by the client or on behalf of the client, except for purposes directly connected with the administration of the Medicaid program. Further specifies that entities with which the Texas Health and Human Services Commission or the department contracts to perform certain administrative functions, including contractors for outreach, informing, and transportation services, may receive confidential information without the client's consent, but only to the extent necessary to performance and administration of the contract. These contracted entities are bound by the same standards of confidentiality applicable to the Medicaid program, and they must provide effective safeguards to ensure confidentiality.	State: Texas	Early and Periodic Screening, Diagnosis, and Treatment	http://info.sos.state.tx.us/pls/pub/readtac$ext.TacPage?sl=R&app=9&p_dir=&p_rloc=&p_tloc=&p_ploc=&pg=1&p_tac=&ti=25&pt=1&ch=33&rl=30

Appendix B – THSA Model Security Policy Mapping to the HITRUST CSF

The table below lists the sections of the THSA model security policy, a description of the policy itself, citations to the HIPAA Security rule, the mapping to the CSF, and proposed changes to the 2013 version of the CSF (if applicable). Items in parenthesis in the CSF References column denotes the name of the HIPAA Security rule requirement the CSF control cross-references. For example, 10.d (Integrity Controls) means CSF control 10.d references 164.312(e)(2)(i) Integrity Controls. Instances where no references are provided are because there was only one HIPAA Security rule requirement directly referenced.

THSA Model Security Policies	Policy	HIPAA Citations	CSF Reference(s)	Proposed CSF Changes
Article I – Introduction	The Texas Health Services Authority (THSA) Health Information Model Policy Regarding Privacy and Security of Health Information is hereby adopted and approved by THSA, and it shall be effective as of the Effective Date. The Model Policy is comprised of two separate sets of policies: a set of Model Privacy Policies and a set of Model Security Policies. This document contains the Model Security Policies; the Model Privacy Policies are contained in an accompanying document. **THSA Model Security Policies.** These Model Security Policies are not intended to be exhaustive or one-size-fits-all, and Local HIEs are not required to adopt them verbatim; rather, the Model Security Policies are intended to serve as a model set of policies that Local HIEs can adopt or use as a resource to ensure the privacy and security of EPHI. THSA realizes that some Local HIEs may have robust policies already in place, while other Local HIEs may not, and that the degree and manner of access,	N/A	N/A	N/A

	disclosure, and use of EPHI by Local HIEs throughout the state varies considerably. Thus, while these Model Security Policies often contain detailed, specific procedures and protocols, each Local HIE has the freedom and flexibility to implement its own unique privacy and security measures as appropriate and in compliance with state and federal law. Both state and federal laws implicate the security and privacy of EPHI, and the Model Policy was developed to comply with applicable law and to implement best practices. Thus, Local HIEs may choose to adopt these Model Security Policies in their entirety, or to use them as a resource to facilitate development of their own privacy measures. However, the law in this area continues to evolve, and thus it will be important for Local HIEs to continually stay abreast of applicable law and industry standards.			
Article II – Definitions	N/A	N/A	N/A	N/A
Article III – Security Officer	HIE shall designate a Security Officer whose role shall be developing, implementing, maintaining, and monitoring HIE's adherence to the terms of its security policies.	45 C.F.R. § 164.308(a)(2) Authority and Responsibility for the Information Security Program	05.a 05.c	None noted

Article IV – Security Management Process	HIE shall ensure that information systems are properly secured and that EPHI is adequately protected. HIE shall implement procedures to prevent, detect, contain, and correct security violations. The components of this policy include: 1. Risk Analysis – HIE shall conduct an annual assessment of the potential risks and vulnerabilities to the Confidentiality, Integrity, and Availability of HIE's electronic information which includes, but may not be limited to EPHI. 2. Risk Management – HIE shall implement security measures sufficient to reduce risks and vulnerabilities to the Confidentiality, Integrity, and Availability of electronic information (including EPHI) to an appropriate and reasonable level as determined by HIE management. 3. Disciplinary Action – HIE shall take appropriate disciplinary actions against HIE Users who knowingly fail to comply with information security-related policies and procedures. 4. Review – HIE shall implement procedures to review records of information systems activity to gauge the effectiveness of Administrative, Physical, and Technical safeguards as well as identify possible breaches of information security.	45 C.F.R. § 164.308(a)(1) • Risk Analysis • Risk Management • Sanction Policy • Information System Activity Review	0.a (Security Mgmt Process; Risk Analysis; Risk Management) 02.f (Sanction Policy) 03.b (Risk Analysis) 03.c (Risk Management) 06.i (Risk Management) (supporting) 09.ab (Information System Activity Review) 09.ae (Information System Activity Review)	None noted

Article V – Workforce Security	HIE shall ensure that each HIE User has appropriate access to EPHI, based on his/her role within HIE and his/her need to access the data. Controls shall be implemented to prevent individuals who should not have access from obtaining such access. Specific features of HIE's Workforce Security Policy shall include: 1. Authorization and/or Supervision – All HIE Users shall be authorized to access systems and applications containing confidential information (including EPHI) prior to being granted access to those systems. Written records of authorization for systems and application access shall be maintained by the Security Officer for a period of not less than 6 years. 2. Workforce Clearance Procedures – An HIE User's access shall be reviewed [annually] (after initial authorization) to help ensure that such HIE User's continued access to EPHI is appropriate. 3. User Notification – HIE Users shall be notified in writing of their responsibilities related to maintaining the Confidentiality, Integrity, and Availability of EPHI and expected adherence to HIE's information security policies. 4. Termination Procedures – Upon termination of an HIE User, adequate steps shall be taken to help ensure the rapid removal of the HIE User's access to facilities and systems that contain EPHI.	45 C.F.R. § 164.308(a)(3) • Authorization and/or Supervision • Workforce Clearance Procedure • Termination Procedures	01.a (Workforce Security) 01.b (Workforce Security; Authorization and/or Supervision; Workforce Clearance; Termination Procedures) 01.c (Authorization and/or Supervision) 01.e (Workforce Clearance) 01.v (Workforce Security; Authorization and/or Supervision) 02.g (Termination Procedures) 02.h (Termination Procedures) 02.i (Termination Procedures)	None noted

Article VI – Information Access Management	HIE shall ensure that access to EPHI is authorized, correctly provided/modified, and removed timely for all Users. Access to EPHI shall be authorized to ensure the Confidentiality, Integrity, and Availability of the information. Specific features of HIE's Information Access Management Policy include: 1. Authorization – All Users shall be authorized to access systems/applications containing EPHI prior to being granted access. Written access authorization records shall be maintained for a minimum of 6 years. With respect to HIE Users, also see the Workforce Security Policy. 2. Access Establishment and Modification – Written (or electronic) documentation shall be maintained of each User's system access and authorization levels when such access or authorization is granted, reviewed, or modified. This documentation shall be maintained by the Security Officer for a period of not less than 6 years.	45 C.F.R. § 164.308(a)(4): • Isolating Health Care Clearinghouse Function (NOT APPLICABLE TO HIEs) • Access Authorization • Access Establishment and Modification	01.b (Information Access Mgmt; Access Authorization; Access Establishment and Modification) 01.c (Information Access Mgmt; Access Authorization) 01.e (Access Establishment and Modification) 01.v (Information Access Mgmt; Access Authorization)	None noted

Article VII – Security Awareness	HIE shall ensure that all HIE Users are educated on security risks and accountability regarding properly securing EPHI. HIE shall provide periodic security awareness and training to all HIE Users (including management). Specific features of the awareness and training policy shall include, but may not be limited to: 1. Security Reminders – Periodic communications on information security policies and procedures. 2. Protection from Malicious Software – Training on procedures to protect against, detect, and report malicious software such as viruses. 3. Login Monitoring – Training on how to identify (if possible) unauthorized use of access credentials by an unauthorized party. 4. Password Management – Training on how to create, change, and safeguard Passwords.	45 C.F.R. § 164.308(a)(5): • Security Reminders • Protection from Malicious Software • Login Monitoring • Password Management	01.d (Password Management) 01.f (Password Management) 01.r (Password Management) 02.e (Security Awareness Program; Security Reminders) 09.j (Protection from Malicious Software) 09.aa (Login Monitoring) 09.ab (Login Monitoring)	None noted

Article VIII – Security Incidents	HIE shall address attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. HIE shall maintain security procedures to preserve the confidentiality and Integrity of EPHI. HIE's policies shall contain provisions to help prevent detect, contain, and correct various security breaches/incidents. Response and Reporting – Procedures shall be maintained for individuals to report actual or suspected security incidents to the Security Official. The Security Official shall respond to the incident as appropriate and as directed by management in an effort to mitigate any harmful effects of the incident. The Security Official shall maintain documentation of all security incidents and outcomes for a period of 6 years or based on applicable regulatory requirements (whichever is greater).	45 C.F.R. § 164.308(a)(6): • Response and Reporting	11.a (Response and Reporting) 11.c (Security Incident Procedures) 11.d (Response and Reporting) 11.e (Response and Reporting)	None noted

Article IX – Contingency Planning	HIE shall ensure that information systems containing EPHI and related daily processing can be recovered following an unplanned event. HIE shall maintain policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, and natural disaster) that damages systems containing EPHI. The specific features of this Contingency Planning Policy include: 1. Applications and Data Criticality Analysis – Assessment of the relative criticality of specific applications and data in support of contingency plan components; 2. Data Backup Plan – Procedures to create and maintain retrievable exact copies of EPHI; 3. Disaster Recovery Plan – Procedures to restore any loss of data; 4. Emergency Mode Operations Plan – Procedures to enable continuation of critical business processes for the protection of the security of EPHI while operating in an emergency mode; and 5. Testing and Revision – Procedures for [periodic] testing and revision of contingency plans.	45 C.F.R. § 164.308(a)(7): • Data Backup Plan • Disaster Recovery Plan • Emergency Mode Operation Plan • Testing and Revision Procedure • Applications and Data Criticality Analysis	08.d (Contingency Plan) 09.l (Data Backup Plan) 12.a (Emergency Mode Operation Plan) 12.b (Applications and Data Criticality Analysis) 12.c (Data Backup Plan; Disaster Recovery Plan; Emergency Mode Operation Plan; Testing and Revision Procedure; Applications and Data Criticality Analysis) 12.d (Disaster Recovery Plan) 12.e (Testing and Revision Procedure)	None noted

Article X – Evaluation And Audit	HIE shall assure the Confidentiality, Availability, and Integrity of EPHI. HIE shall perform a periodic technical and nontechnical evaluation to ensure that HIE policies comply with laws, rules, and regulations. This periodic technical and nontechnical evaluation shall also respond to environmental or operational changes affecting the security of EPHI. The technical evaluation shall include testing and investigation of HIE's technical security procedures, including the algorithms or processes used for Encryption, Authentication, and Integrity. The nontechnical evaluation shall include testing and investigation of HIE's administrative and physical security policies. The Security Officer shall review the effectiveness of existing policies as well as HIE User's and Participant User's compliance with these policies.	45 C.F.R. § 164.308(a)(8) Security Audits	0.a 03.a 06.g 06.h	None noted
Article XI – Vendor Contracts And Agreements	HIE is a Business Associate of its Participant Users who are Covered Entities. As such, HIE must enter into a Business Associate Agreement with each of its Participant Users. HIE shall not receive any EPHI from a Participant User or Subcontractor until a fully executed Business Associate Agreement has been entered into between the parties. Additionally, HIE shall enter into a Business Associate Subcontractor Agreement with any entity that receives EPHI from HIE and performs a function on behalf of the HIE.	45 C.F.R. § 164.308(b)(1): • Written Contract or Other Arrangement	05.k (Business Associate Contracts and Other Arrangements; Written Contracts or Other Arrangements) 09.e (Written Contracts or Other Arrangements) 09.t (Written Contracts or Other Arrangements) 10.l (Written Contracts or Other Arrangements)	None noted

Article XII – HIE Facility Access Control	HIE shall establish physical access controls (i.e., keys, locks, and cards) to help prevent/detect intrusion/unauthorized access and to ensure that HIE Users have minimum necessary access to perform their daily job functions. Additionally, physical access controls are in place to protect physical computer systems and related buildings in the event of natural disasters and environmental hazards. HIE shall limit physical access to its electronic information systems and the facilities in which such systems are housed while ensuring that properly authorized access is allowed. The specific features of HIE's Access Control policy include: 1. Contingency Operations – Procedures shall allow for system access in support of restoration of lost data under the disaster recovery and emergency mode operations plans in an emergency. 2. HIE Facility Security Plan – Safeguards shall be in place to protect the system and the equipment therein from unauthorized physical access, tampering, and theft. 3. Access Control and Validation Procedures – Safeguards shall be in place to validate a person's access to facilities based on his or her role or function. 4. Maintenance Records – Documentation shall be maintained with respect to repairs and modifications to the physical components of the	45 C.F.R. § 164.310(a)(1): • Contingency Operations • Facility Security Plan • Access Control and Validation Procedures • Maintenance Records	08.a (Facility Access Controls) 08.b (Facility Access Controls; Access Control and Validation Procedures) 08.d (Facility Security Plan) 08.j (Maintenance Records) 12.c (Contingency Operations; Maintenance Records)	None noted

	systems that relate to security.			
Article XIII – Workstation Use And Security	HIE shall ensure that all HIE User workstations are properly secured to help mitigate the risk of unauthorized access to information. HIE shall implement, and shall educate Participant Users on implementing, procedures regarding physical safeguards over workstations, especially those located in less secure/public areas. HIE shall define acceptable uses for HIE User workstations. Additionally, HIE shall implement physical security controls to properly secure HIE User workstations.	45 C.F.R. § 164.310(b) 45 C.F.R. § 164.310(c)	08.g (Physical Workstation Safeguards)	Map the following (as a primary) to 45 C.F.R 164.310(b) • 01.g • 01.x • 06.e • 08.g

Article XIV – Device And Media Controls	HIE shall ensure that portable information systems are protected from unauthorized access and release. Unencrypted computing devices (e.g. PCs, laptops, PDAs, servers, smart phones, other mobile phones, tablets, digital e-readers, photo copiers, etc.) and electronic storage media (e.g. hard drives, solid state drives, floppy disks, CDs, DVDs, backup tapes, external removable storage devices, flash drives, SD cards, SIM cards, etc.) that contain EPHI or other confidential data shall be tracked as they move into and out of HIE's facilities. HIE shall maintain a log, for example, by using RFID technology and/or the device's location tracking applications, of all devices and media that come into contact with EPHI, that includes when the device or media first encountered EPHI, where the device is physically located, if it has been moved within the facility, and if and when the device or media has been thoroughly and appropriately cleaned of EPHI and/or transported outside of the HIEs control. HIE shall report the loss of any device or media potentially containing EPHI immediately to the covered entities with which they interact. HIE shall isolate EPHI-containing devices and media from non-EPHI-containing devices and media. HIE shall remove EPHI from devices and media in accordance with National Institute of Standards and Technology (NIST) standards.	45 C.F.R. § 164.310(d)(1): • Disposal • Media Re-use • Accountability • Data Backup and Storage	07.a (Accountability) 08.l (Disposal; Media Re-use) 09.l (Data Backup and Storage) 09.o (Device and Media Controls; Accountability) 09.p (Disposal) 09.u (Device and Media Controls)	None noted

Article XV – Technical Access Controls	HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. HIE shall implement Technical Safeguards for electronic information systems that maintain EPHI to allow access only to those programs and persons that have been granted access rights according to access control and authorization policies. The specific features of the Access Control Policy include: 1. Unique User Identification – Unique user IDs and Passwords shall be assigned to each User. 2. Emergency Access Procedures – Procedures shall ensure access to EPHI in an emergency. 3. Automatic Logoff – Unattended workstations/terminals shall be locked down following a period of inactivity. 4. Encryption/Decryption – Preference shall be given in system selection to applications and operating systems that allow for the encryption of User credentials and EPHI. Encryption, if used, shall be accomplished using standard (non-proprietary) algorithms.	45 C.F.R. § 164.312(a)(1): • Unique User Identification • Emergency Access Procedure • Automatic Logoff • Encryption and Decryption	01.a (Access Control; Emergency Access Procedure) 01.b (Access Control; Unique User Identification) 01.h (Unique User Identification) 01.q (Unique User Identification) 01.t (Automatic Logoff) 01.v (Access Control) 10.f (Encryption and Decryption) 10.g (Key Management) 12.c (Emergency Access Procedure)	None noted
Article XVI – Audit Controls	HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. Certain systems have the capability to produce audit trails (i.e., audit control mechanisms) to record and examine system, network, and/or application activity. Periodically, the Security Officer shall review audit trails to detect and research security breaches (including high-risk	45 C.F.R. § 164.312(b) Logging	06.i 09.aa 09.ab 09.ad	None noted

	patterns), to confirm/deny Users' compliance with HIE policies and procedures, and to identify potential weaknesses.			
Article XVII – Integrity Controls	HIE shall ensure that EPHI has not been changed/corrupted and to validate that data came from the original sender. Certain systems that process EPHI shall utilize controls to ensure the accuracy and Integrity of data at rest as well as in the processing cycle.	45 C.F.R. 164.312(c)(1): • Mechanism to Authenticate Electronic Protected Health Information	09.j (Mechanism to Authenticate ePHI) 10.c (Mechanism to Authenticate ePHI) 10.d (Mechanism to Authenticate ePHI) 10.g (Integrity)	None noted
Article XVIII – Authentication Controls	HIE shall ensure that access to information systems is properly controlled and restricted to authorized individuals. Authorization controls refer to the type of access that allow a User into HIE's systems. Such controls shall be restricted by role/function and/or individual User. HIE shall implement authentication controls that: (i) verify that the User is authorized and the one claimed; and (ii) deny access to unauthorized Users, programs, and/or processes. HIE has implemented procedures for ensuring that external users are properly authenticated to HIE's systems/network.	45 C.F.R. §164.312(d) Non-repudiation	01.b 01.q	None noted

Article XIX – Transmission Security	HIE shall take certain measures when EPHI is sent outside of HIE (e.g., via company network, e-mail, etc.) as well as establish the appropriate use of encryption to protect stored EPHI. Whenever EPHI is transmitted over an open network such as the Internet, technical controls, including Integrity controls and encryption, shall be implemented. 1. Integrity – When EPHI is transmitted outside of HIE or into HIE from another party, Integrity controls shall be implemented to ensure that data accuracy is maintained. 2. Encryption – HIE shall use encryption whenever EPHI is sent outside of HIE. In addition, encryption may be appropriate for other types of information including, but not limited to, e-mail containing other sensitive information and electronic files containing User credentials (e.g. usernames and Passwords) for systems that contain EPHI.	45 C.F.R. §164.312(e)(1): • Integrity Controls • Encryption	09.m (Transmission Security; Integrity Controls; Encryption) 09.n (Transmission Security; Integrity Controls; Encryption) 10.d (Integrity Controls) 10.f (Transmission Security; Policy on the Use of Cryptographic Controls)	None noted