



New Developments in Safeguarding Protected Health Information During 2014

Submitted to the House Public Health Committee
and the Senate Health and Human Services Committee
by the
Health and Human Services Commission

December 2014

INTRODUCTION

House Bill 300, 82nd Legislature, Regular Session, 2011, added a provision in Government Code Section 531.0994, requiring the Health and Human Services Commission (HHSC), in consultation with the Department of State Health Services, the Texas Medical Board, and the Texas Department of Insurance, to explore and evaluate new developments in safeguarding Protected Health Information (PHI). By December 1st of each year, HHSC must report to the legislature about new developments in safeguarding PHI and make recommendations for the implementation of PHI safeguards within HHSC.

This report is intended to meet the requirement of House Bill 300 (HB 300). The report documents HHSC efforts to explore and evaluate new developments in safeguarding PHI, in coordination with other agencies and entities, and makes recommendations for implementation of PHI safeguards within HHSC.

BACKGROUND

Numerous state and federal laws require safeguards over PHI. A Texas covered entity, as defined by the Texas Medical Records Privacy Act, Chapter 181, Health and Safety Code, that uses or discloses identifiable PHI, must comply, to the extent possible, with the following confidentiality standards and safeguard requirements.

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, as amended and regulated thereunder, in 45 Code of Federal Regulations Parts 160 and 164.
- Texas Medical Records Privacy Act, Texas Health and Safety Code, Chapter 181.
- Texas Identity Theft Enforcement and Protection Act, Texas Business and Commerce Code, Chapter 521.
- Laws and regulations governing specific types of information, individuals, facilities, and provider types, as summarized in Appendix A.

HHSC must also comply with other confidentiality requirements:

- Benefit program use, disclosure, and safeguard requirements, such as required by Medicaid.
- Federal data sharing agreements with the Social Security Administration and the Internal Revenue Service, which contain privacy and security requirements.
- State regulations over information security included in 1 Texas Administrative Code, Chapters 202 (Information Security) and 390 (Information Practices).

NEW DEVELOPMENTS IN SAFEGUARDING PHI

This following details new developments in safeguarding PHI during 2014, including changes in federal law and policy and changes in state law, regulations, and policy. It also includes information about recent HHSC accomplishments and initiatives to improve safeguard activities.

Changes in Federal Law and Policy

HIPAA

HIPAA covered entities continue to adjust to 2013 HIPAA Omnibus regulatory changes. Some of the activities include:

- Identifying and implementing industry best practices to respond to Omnibus breach notification standards and required breach risk assessments.
- Preparing for newly required U.S. Department of Health and Human Services, Office of Civil Rights (OCR) HIPAA audits. The OCR revised its audit protocols and held training webinars on those changes during 2014.
- Responding to OCR's second "Annual Report to Congress on Breaches of Unsecured Protected Health Information (PHI), for calendar years 2011 and 2012,"¹ issued in July 2014. The report made recommendations for HIPAA covered entities to mitigate and prevent breaches by taking the following actions:
 - Revise policies and procedures
 - Improve physical security, install new security systems, or relocate equipment or records to a more secure area
 - Train or retrain workforce who use or disclose PHI
 - Provide free credit monitoring following a breach
 - Adopt encryption technologies
 - Impose sanctions on workforce members found to be in violation of policies and procedures for PHI
 - Regularly change passwords
 - Perform new risk assessments
 - Revise business associate contracts to be more precise about PHI safeguards

FISMA

A pending federal bill, the Federal Information Security *Modernization* Act of 2014, would amend the Federal Information Security *Management* Act of 2002 (FISMA).² The bill, if passed,

¹ See, <http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachreport2011-2012.pdf>.

² Federal Information Security Modernization Act of 2014, 113th Congress (2013-2014), S.2521: <https://www.congress.gov/bill/113th-congress/senate-bill/2521>.

would modernize the 2002 federal information security requirements of FISMA to shift the focus away from agency self-assessments and checklist reporting, and toward continuous monitoring, data breach mitigation, and integrated security testing under the direction of the Office of Management and Budget (OMB). Under a modernized FISMA, OMB would be required to establish federal agency procedures for breach of personally identifiable information, including requirements for notice to affected individuals. Under the revised OMB security policy, Medicaid state agencies, such as HHSC, would be required, as a condition for receiving funding from federal agency partners such as the Social Security Administration and the Centers for Medicare and Medicaid Services, to comply with FISMA and the revised OMB security policy.

NIST

The National Institute of Standards and Technology (NIST), a federal agency, establishes information technology standards, policies, and guidance for federal agencies and state governments that receive federal funding. In 2014, NIST issued Draft Special Publication 800-53A, Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations."³ The publication is a companion guideline to NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," and provides guidance on building effective plans for, and how to analyze and manage the results of, privacy and security assessments. HHSC is aligning its controls with this guidance, as described below.

Changes in State Laws, Regulations, and Policy

No changes in Texas state law for safeguarding PHI become effective during 2014.

Department of Information Resources

The Department of Information Resources is planning significant regulatory changes to security standards required of state agencies in 1 Texas Administrative Code, Chapter 202, Information Security Standards.⁴ DIR does not plan to include privacy controls in its re-write of the regulations.

Texas Health Services Authority

The Texas Health Services Authority has now partnered with the Health Information Trust Alliance to begin a certification program, called "SECURETexas,"⁵ to permit HIPAA covered entities to demonstrate compliance with state and federal privacy and security laws. The Texas Health Services Authority also published program criteria for Texas Health Information

³ See, http://csrc.nist.gov/publications/drafts/800-53a/sp800_53a_r4_draft.pdf.

⁴ See, Texas Department of Information Resources, TAC 202 Overview Presentation: <http://www.dir.state.tx.us/SiteCollectionDocuments/Security/Texas%20CyberSecurity%20Framework/TAC202>

⁵ See, Texas Health Services Authority, Privacy and Security Certification, Secure Texas Certification Overview: <http://hietexas.org/privacy-and-security-certification/overview>.

Exchange Accreditation, including privacy and security criteria for PHI.⁶ The accreditation program is run in partnership with the Electronic Health Network Accreditation Commission.

HHSC Accomplishments and Initiatives to Improve Safeguard Activities

In 2014, HHSC made a number of improvements for safeguarding PHI through developments in its privacy and security programs, improvements in agency contracting standards, and changes in human resources policy.

Privacy Program

In 2014, HHSC restructured its privacy program and implemented or planned several activities to safeguard PHI and other agency confidential information.

- In March, 2014, HHSC formed a new Risk and Compliance and Management Division, with direct reporting to the Executive Commissioner, which oversees the HHSC Privacy Office.
- On August 1, 2014, HHSC appointed its first Chief Privacy Officer, restructured the Privacy Office, expanded staff resources for the Privacy Office, and is developing a privacy program for Health and Human Services agencies. The Privacy Officer has responsibility for most HB 300 compliance and reporting activities and oversight of agency compliance with HIPAA and other state and federal confidential information and privacy requirements. The Chief Privacy Officer leads HHSC and Health and Human Services joint agency Incident Response Teams assembled to address actual or suspected privacy breaches.
- HHSC is in the process of finalizing an internal document to establish and communicate policies regarding expectations, and roles and responsibilities of HHS employees for safeguarding PHI, privacy breach reporting, and support of HB 300 requirements. The document is expected to be finalized in early 2015.
- The HHSC Privacy Office is revising its workforce privacy policies and procedures and has drafted an Incident Response Plan to guide Health and Human Services agency responses to actual or suspected privacy breaches. Both are expected to be finalized in early 2015.
- The HHSC Privacy Office is revising HHSC workforce privacy training to include recent HIPAA Omnibus changes and best practices. The revised training is expected to be finalized in 2015.
- HHSC revised and published a new Notice of Privacy Practices, which includes an Organized Health Care Arrangement and shared privacy notice between HHSC, the Department of State Health Services, and the Department of Aging and Disability Services, the three HIPAA covered entities within the Health and Human Services agencies.

⁶ See, Texas Health Services Authority, HIE Accreditation, Health Information Exchange Accreditation Program. <http://hitrustalliance.net/texas/>.

- The HHSC Privacy Office launched a privacy awareness and education campaign, and is communicating privacy best practices and engaging in outreach and training directed to the HHSC workforce and to HHSC business partners.
- HHSC is revising its Business Continuity of Operations plan template to clarify privacy considerations during an emergency or disaster, such as risks to PHI and agency confidential information, compliance challenges, and the ability to safeguard PHI and agency confidential information.
- HHSC is developing a methodology and plan to implement performance of Privacy Impact Assessments on systems with PHI and agency confidential information to conform with federal requirements. A Privacy Impact Assessment is a decision making tool used to evaluate a system by (a) identifying what private information is collected, and how and why that information is used or disclosed, and (b) assessing the adequacy of efforts to identify and mitigate privacy risks at the beginning of and during the course of a program or system. Federal agencies are required to conduct Privacy Impact Assessments when developing new or revising existing programs or systems containing personally identifiable information.⁷
- HHSC is preparing for expected federal compliance audits, required by the American Recovery and Reinvestment Act of 2009 and HIPAA to be performed periodically on all HIPAA covered entities by the Department of Health and Human Services, Office of Civil Rights. HHSC will draft a Health and Human Services HIPAA Audit Response Plan and develop a Book of Evidence to permit HIPAA covered agencies to respond efficiently and effectively to the comprehensive federal audit compliance protocols.

Security Program

In 2014, HHSC strengthened its security program over PHI and other agency confidential information. HHSC IT Security:

- Revised or planned governance improvements:
 - Revised the Health and Human Services information security policy Circular to establish "Enterprise Information Security" objectives
 - Revised "Enterprise Information Security Policy" standards to incorporate guidance from NIST 800-53, Revision 4, framework, and to establish the "Enterprise Information Security Program" for Health and Human Services agencies, consistent with 1 Texas Administrative Code Chapter 202
 - Revised the standards and guidelines for minimum security controls to protect PHI and other information resources
 - Planned to develop guidelines for information owners and custodians.

⁷ For example, Privacy Impact Assessments are required by the E-Government Act and are subject to guidance issued by the Office of Management and Budget, Memorandum M-03-22.

- Improved HHSC's Data Loss Prevention (DLP) technology, which blocks and reports on unsecure transmissions of PHI or other agency confidential information from agency information resources, as follows:
 - Developed policy documentation for the threshold DLP settings
 - Increased settings for greater detection of activity
 - Extended the scope of coverage and monitoring environment to include endpoints, such as computers and printers
- Improved workforce security training:
 - Updated security awareness training, required annually, for agency workforce
 - Completed a pilot security awareness training using the SANS Institute's "Securing the Human"⁸ platform, and purchased licenses to provide the training to all workforce within Health and Human Services agencies.
- Continued to improve processes for managing mobile devices, including the use of Mobile Device Management technology for technical controls and compliance with security standards.

In addition, HHSC IT Security is:

- Developing a security exceptions policy, based on NIST 800-53, Revision 4, framework, and will centrally track exceptions using a risk register in HHSC's Governance, Risk and Compliance application technology, to rate risk according to likelihood and impact of vulnerabilities.
- Initiating required contractor self-assessments to self-report security controls, based on NIST 800-53, Revision 4, guidelines, for review by HHSC Security Assurance workforce.

Contracting Standards

In 2014, HHSC improved standards for contracts that involve PHI and agency confidential information by updating and improving its form Data Use Agreement (DUA). HHSC:

- Updated the current form DUA version with stronger controls and requirements, captured current best practices, clarified minimum standards for use or disclosure of PHI or other agency confidential information, and made the form more readily available to all Health and Human Services agencies.
- Published the form DUA on HHSC's website with plans to link the DUA within the procurement library for all future requests for proposals that involve the use or disclosure of PHI or other agency confidential information.
- Drafted a new more concise version of the DUA, expected to be published on HHSC's website in early fiscal year 2015.

⁸ The SANS Institute is a leading, international information security training and certification program. See, www.securingthehuman.org.

- Assembled a workgroup to:
 - Create a central repository for DUAs that involve the use or disclosure of PHI or other agency confidential information, for HIPAA compliance purposes
 - Improve methods to inventory, track, periodically review, and issue amendments or updates for outdated DUAs, in compliance with applicable laws and guidelines and consistent with best practices
 - Support HHSC's existing requirements to monitor contractor performance

Human Resources Policy

In 2014, HHSC updated its Human Resources policies to safeguard PHI with new workforce requirements. As a result, HHSC:

- Improved identification, tracking, and rebadging of agency staff augmentation contractors.
- Developed a draft Social Media Policy, addressing PHI and other security and privacy requirements.

RECOMMENDATIONS

The Texas Medical Records Privacy Act (the "Act"), Chapter 181, Health and Safety Code, could be revised to address inconsistencies with federal law with respect to the use of certain terminology and to the scope of certain safeguarding requirements. Revisions to the Act would strengthen and clarify requirements that would help ensure HHSC and other entities subject to the Act properly safeguard PHI. HHSC recommends the following revisions to the Act.

Security and Privacy Requirements

Issue - Electronic PHI Security

The Act has no electronic PHI security requirements similar to those included as part of 26 required or addressable security considerations in the HIPAA security regulations. While the Act adopts HIPAA privacy and administrative requirements, by reference to HIPAA as, 45 CFR Parts 160 and 164, *Subpart A (General Provisions)* and *Subpart E (Privacy of Individually Identifiable Information)*, it does not include Texas requirements consistent with federal and industry standards.

These standards provide for security controls over electronic PHI in the following categories:

- Administrative Security, such as policies and procedures for training, provision of access, termination, review of safeguards; incident management and disaster recovery plans, and contract provisions when sharing PHI with a third-party.
- Physical Security, such as locks, keys, physical access, physical storage and trash.

- Technical Security, such as system passwords, intrusion protections, audit logging and protections such as standards for encryption of PHI.

For HIPAA covered entities and their business associates that are subject to HIPAA security standards, the implication of the lack of security standards in the Act is the Act lacks an independent mechanism to enforce violations of security requirements by HIPAA covered entities under Texas law. Texas enforcement activities are currently limited to and subject to HIPAA regulatory oversight.⁹

For a non-HIPAA covered entity under the Act, there is no duty to have adequate electronic or physical, administrative, or technical security requirements over PHI, and the Act has no enforcement mechanism for such violations.

As a result, the lack of security controls limits the Act's effectiveness to protect PHI electronically maintained in Texas. Consequently, there is an increased risk of unauthorized use or disclosure of PHI, which often results in harm to the individual, such as harm due to financial or medical identity theft.

Recommendation

HHSC recommends the Legislature consider adding a provision to the Act that includes specific requirements for electronic PHI security for entities subject to the Act.

Issue - Privacy Requirements for Non-Covered Entities

Section 181.004(b) of the Act requires entities that are subject to the Act, but who are not subject to HIPAA, to comply with the Act only, not HIPAA; the Act makes HIPAA applicable to HIPAA covered entities. Privacy requirements for entities that are subject to the Act, but who are not subject to HIPAA, include (a) providing timely training for employees, (b) maintaining evidence of training for six years, and (c) not engaging in prohibited acts like unlawful sale or marketing of PHI. While the Act requires entities that are subject to the Act, but who are not subject to HIPAA, to comply with the Act's requirements and prohibitions, the Act does not require these entities to maintain PHI in compliance with other privacy safeguards, such as requirements for:

- Privacy policies applicable to the use or disclosure of PHI by the entity and its workforce.

⁹ Section 13410(e) of the Health Information Technology for Clinical and Economic Health Act in the American Recovery and Reinvestment Act of 2009, gave State Attorneys General the authority to bring civil actions on behalf of state residents for violations of the HIPAA Privacy and Security Rules. The HITECH Act permits State Attorneys General to obtain damages or to enjoin further violations of the HIPAA Privacy and Security Rules. However, this enforcement authority requires significant coordination between HIPAA regulators and the Office of Attorney General.

- Privacy notices, or statements about privacy practices on the entity websites with a contact for complaints about PHI.
- Adequate safeguards in agreements when sharing PHI with third-parties.
- Provision of individual rights to access or receive an accounting of certain uses or disclosures of PHI maintained by the entity, subject to appropriate Act exemptions.

Recommendation

HHSC recommends the Legislature consider adding a provision to the Act that expands the requirements for certain PHI privacy safeguards to entities that are subject to the Act, but who are not subject to HIPAA, such as requirements for policies, procedures, a privacy notice, contract safeguards, and individual rights.

Breach Notice Requirements

Issue - *PHI Breach Response and Notification Requirements*

The Act contains no specific PHI breach notification requirement, or adoption of other breach notice laws, rules, or regulations. The Act limits the definition of HIPAA by reference to HIPAA 45 CFR Part 164 and its Subsections A (general requirements) and E (privacy requirements):

'Health Insurance Portability and Accountability Act and Privacy Standards' means the *privacy* requirements in existence on September 1, 2011, of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) contained in 45 C.F.R. Part 160 and 45 C.F.R. Part 164, *Subparts A and E*.

Id. at Section 181.001, Definitions, (b)(3)(Emphasis supplied). This is further discussed below in HHSC's recommendations about the Act's definitions.

Of course, HIPAA covered entities would be subject to HIPAA's breach notice requirements, but because the applicability of the Act is limited to privacy requirements, the Act lacks an independent mechanism to enforce requirement for actual or suspected breaches of PHI by HIPAA covered entities under Texas law.

Likewise, entities that are subject to the Act, but who are not subject to HIPAA, have no duty under the Act to notify individuals, mitigate unsecure paper or electronic PHI, or cooperate in an investigation to mitigate a breach by HIPAA covered entities or public authorities. Although Texas has a general breach notice law in Business and Commerce Code, Chapter 521 ("Texas Breach Law"), it is limited to breaches of *electronic "sensitive personal information,"* including a name plus identifiable health information (PHI) or a Social Security Number, for example.

Not all PHI breaches include "sensitive personal information," or are breaches of electronic PHI. Below are some examples of breaches that could be caused by or that involve entities that are subject to the Act, but who are not subject to HIPAA, with no duty owed by the entity to notify individuals, further safeguard unsecure paper or electronic PHI, or cooperate in an investigation to mitigate a breach. In the examples, the PHI involved would not meet the definition of "sensitive personal information" to afford protection under the Texas Breach Law.

- A common carrier routinely transports paper medical records for a HIPAA covered entity; but common carriers are exempt from HIPAA, under the "mere conduit" exception. In the incident it is discovered that PHI paper records were transported with inadequate physical security and were compromised (lost, damaged, destroyed, or unlawful access). The common carrier had no legal duty to cooperate with the health care provider that shipped the records to investigate and mitigate a breach.
- A commercial lender forecloses on a medical facility or a storage facility with a health care provider tenant. The lender or property owner discovers PHI medical records were abandoned on the property by an "unsustainable covered entity."¹⁰ Either can decide to destroy the records in an unsecure manner, like dumping them or not providing individual access to retrieve records. Neither the lender nor the storage company is under a legal duty to cooperate in an investigation or to notify individuals of the breach. Failure to provide access to individual records or loss of PHI could be catastrophic to an individual (e.g. loss of scans, x-rays, records of or contraindications for treatment) or cause duplicative, unnecessary care for an individual.
- An Internet site that offers general technical support or services receives PHI inadvertently uploaded by a HIPAA covered entity, viewable publicly. The file does not contain names (which would have subjected the company to the Texas Breach Law), but does contain otherwise identifiable HIPAA PHI. The Internet site is under no legal duty to cooperate to investigate and mitigate the breach, such as remove the PHI from public view.

As a result, the lack of breach notice standards owed by the entities that are subject to the Act, but who are not subject to HIPAA, to (a) investigate a breach, (b) cooperate with investigation required by HIPAA covered-entities or legal authorities, or (c) notify individuals of a breach of their PHI, limits the Act's effectiveness to protect PHI and increases the risk of unauthorized use or disclosure of PHI, again, which often results in harm to the individual, such as harm due to financial or medical identity theft.

Recommendation

HHSC recommends the Legislature consider adding a provision to the Act requiring adequate investigation, mitigation, and corrective action following a breach of PHI and a duty to promptly notify individuals of a breach of PHI in any form, electronic, oral, or paper, that risks individual

¹⁰ See, HHSC 2012 "Unsustainable Covered Entities Report," <http://www.hhsc.state.tx.us/reports/2012/Unsustainable-Covered.pdf>.

harm, applicable to HIPAA covered entities and entities that are subject to the Act, but who are not subject to HIPAA.

Terminology and Definitions

Issue

The Act's terminology and definitions vary from and could be aligned with other similar state and federal laws about health information. For example:

- "HIPAA" is defined in the Act to be limited to the *privacy* regulations as of September 1, 2011. In January, 2013, HIPAA Omnibus regulations were issued that made significant changes to HIPAA. HHSC recommends consideration of revision to the Act's Section 181.001, Definition (3), in order to (a) capture recent HIPAA updates and (b) capture security and breach notice regulations, as follows:
 - " 'Health Insurance Portability and Accountability Act Standards' means the administrative, privacy, security and breach notice regulations of the Health Insurance Portability and Accountability Act of 1996 (Pub. L. No. 104-191) and regulations adopted thereunder in 45 CFR Parts 160 and 164, *Subparts A, C, D and E.*" (Emphasis supplied).
- The Act and a number of state laws about health information employ the terms "use," "disclosure," and "access to" and sometimes do so inconsistently. The Act defines "disclosure" but not "use." HIPAA now uses the phrase "create, receive, maintain, have access to, or transmit" when regulating PHI, with accompanying definitions. Where appropriate, HHSC recommends consideration of adopting the HIPAA phrase and definitions, so as to not unintentionally limit applicability of the Act, for example only to "disclosures" but not "uses."
- HIPAA defers to state law to determine an individual's personal representative, with the right to act on behalf of, and receive or access PHI, on an individual's behalf. Texas law has not concisely determined who legally authorized representatives are in Texas. Texas law currently contains a variety of terminology and standards for persons with authority over individuals or their health information.¹¹ It would be helpful for HHSC business and other

¹¹ For example, the Family Code, Occupations Code, Health and Safety Code, Probate Code and Estates Code, and other federal law like Medicaid, provide for numerous possible representatives, for various purposes, such as:

- Parents or legal guardians of minors;
- Legal guardians for individuals adjudicated incompetent to manage personal affairs
- Agents designated to act for an individual under durable and medical powers of attorney
- Attorneys and Guardians ad litem appointed for an individual
- The deceased' statutory or personal representatives, e.g. executors, independent executors, administrators, independent administrators or temporary administrators of an estate
- The state- designated Protection and Advocacy System representatives

entities subject to the Act for Texas law to concisely provide who may act as a legally authorized representative to use, disclosure, receive, or access an individual's PHI.

- The Act frequently refers to people whose PHI is at issue as "patients." However, the Act and HIPAA are apparently designed to apply to all types of PHI settings, including those where the individuals are not considered "patients," but might be known or regulated as "individuals" or "clients," such as HHSC's "clients." HIPAA refers to the person whose PHI is at issue as an "individual." It would be helpful if the Act consistently used the term "individual" to refer to the person whose PHI is at issue, which would align the Act with HIPAA and other healthcare related laws.

These changes to the Act's terminology or definitions would clarify and guide HHSC and other entities subject to the Act on the Legislature's intended scope of the Act.

Recommendation

HHSC recommends the Legislature consider adding provisions to the Act that:

- Consistently employ defined terms: "use" or "disclosure."
- Add a definition for an individual's "Legally Authorized Representative" for HIPAA and Act purposes.
- Replace the term "Patient" with the term "Individual."

Appendix A

Covered entities, such as HHSC, must comply with a number of state or federal laws or regulations that require confidential information to be safeguarded and used or disclosed only for authorized persons and purposes, as applicable.

HHSC promulgated a rule in 1 Texas Administrative Code, Chapter 390, Information Practices, applicable to "covered entities," as defined by the Texas Medical Records Privacy Act, Health and Safety Code, Section 181.001(b)(2). The rule requires covered entities that electronically exchange, use or disclose PHI to comply with the minimum standards for confidential information in any form, and for specific types of information, individuals or facility types.

Specific Types of Confidential Information, such as:

- Cancer
- HIV/AIDS
- Genetic
- Sexual assault
- Communicable diseases
- Mental health
- Substance abuse or substance use disorder
- Immunizations
- Bureau of Vital Statistics
- Reports of abuse or neglect
- Federal tax information
- Social Security Administration data
- Occupational diseases
- Family planning
- Recipients of government benefits
- Individuals receiving intellectual and disability services

Specific Types of Providers, Facilities, or Services, such as:

- Hospitals
- Nursing facilities
- Intermediate care facilities for persons with an intellectual disability or related conditions
- Freestanding emergency medical care facilities
- Ambulatory surgical centers
- Emergency medical services
- Physicians
- Chiropractors
- Dentists
- Labs
- Pharmacists
- Podiatrists
- Personal health record vendors
- End stage renal disease facilities
- Special care facilities for AIDS
- Private psychiatric hospitals and crisis stabilization units
- Birthing centers
- Dyslexia therapists and dyslexia practitioners
- "Promotores" or community health workers
- Medical radiologic technologists
- Licensed chemical dependency counselors and treatment facilities

Specific Types of Individuals, such as:

- Minors and Children with Special Health Care Needs Services Program
- Early and Periodic Screening, Diagnosis, and Treatment