Domestic Privacy Profile: Texas

Prepared in cooperation with
Shawn Tuma
Partner, Spencer Fane, LLP
Domestic Privacy Profile: TEXAS

Shawn Tuma of Spencer Fane, LLP, Plano, Tex., provided expert review of the Texas Profile and wrote the Risk Environment section. [Last updated August 2018. – Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS ............................................................................................................. 3
   A. Constitutional Provisions ................................................................................................................................. 3
   B. Personal Data Protection Provisions .................................................................................................................. 3
      1. Who is covered? ........................................................................................................................................... 3
      2. What is covered? ........................................................................................................................................... 3
      3. Who must comply? ....................................................................................................................................... 4
   C. Data Management Provisions ........................................................................................................................ 5
      1. Notice & Consent ......................................................................................................................................... 5
      2. Collection & Use ......................................................................................................................................... 5
      3. Disclosure to Third Parties .......................................................................................................................... 5
      4. Data Storage ............................................................................................................................................... 6
      5. Access & Correction ................................................................................................................................... 6
      6. Data Security ............................................................................................................................................... 6
      7. Data Disposal ............................................................................................................................................. 7
      8. Data Breach ............................................................................................................................................... 8
      9. Data Transfer & Cloud Computing ............................................................................................................ 9
     10. Other Provisions ...................................................................................................................................... 9
   D. Specific Types of Data ..................................................................................................................................... 10
      1. Biometric Data ........................................................................................................................................... 10
      2. Consumer Data .......................................................................................................................................... 10
      3. Credit Card Data ....................................................................................................................................... 11
      4. Credit Reports .......................................................................................................................................... 11
      5. Criminal Records ................................................................................................................................... 12
      6. Drivers’ Licenses/Motor Vehicle Records ................................................................................................. 12
      7. Electronic Communications/Social Media Accounts .................................................................................... 12
      8. Financial Information ................................................................................................................................. 13
      9. Health Data ............................................................................................................................................... 13
     10. Social Security Numbers .......................................................................................................................... 18
     11. Usernames & Passwords ........................................................................................................................... 29
E. Sector-Specific Provisions .................................................................................................................. 20
   1. Advertising & Marketing .................................................................................................................. 20
   2. Education ...................................................................................................................................... 21
   3. Electronic Commerce ..................................................................................................................... 21
   4. Financial Services .......................................................................................................................... 21
   5. Health Care ..................................................................................................................................... 21
   6. HR & Employment .......................................................................................................................... 22
   7. Insurance ........................................................................................................................................ 23
   8. Retail & Consumer Products ......................................................................................................... 27
   9. Social Media .................................................................................................................................. 27
  10. Tech & Telecom ............................................................................................................................... 27
  11. Other Sectors .................................................................................................................................. 28

F. Electronic Surveillance .......................................................................................................................... 28

G. Private Causes of Action ...................................................................................................................... 30
   1. Consumer Protection .................................................................................................................... 30
   2. Identity Theft ................................................................................................................................. 31
   3. Invasion of Privacy ........................................................................................................................ 31
   4. Computer Hacking ........................................................................................................................ 32
   5. Other Causes of Action .................................................................................................................. 32

H. Criminal Liability ................................................................................................................................ 33

II. REGULATORY AUTHORITIES AND ENFORCEMENT ......................................................................... 35
   A. Attorney General ............................................................................................................................. 35
   B. Other Regulators ............................................................................................................................. 35
   C. Sanctions & Fines ............................................................................................................................ 36
   D. Representative Enforcement Actions .............................................................................................. 38
   E. State Resources .................................................................................................................................. 39

III. RISK ENVIRONMENT ...................................................................................................................... 39

IV. EMERGING ISSUES AND OUTLOOK .............................................................................................. 39
   A. Recent Legislation ......................................................................................................................... 39
      1. Cybersecurity Act ........................................................................................................................... 39
      2. Direct Marketing to Students ....................................................................................................... 40
   B. Proposed Legislation (85(R) – 2017 Session) ............................................................................. 40
      1. Breach Liability and Notification ................................................................................................. 40
      2. Motor Vehicle Records ................................................................................................................ 41
   C. Other Issues .................................................................................................................................... 41
      1. Equifax Breach ............................................................................................................................... 41
      2. Child Online Privacy Protection .................................................................................................. 41
I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

There are no constitutional provisions in Texas conferring a general right of privacy on Texas residents. Under Tex. Const. art. 1 § 30, crime victims have the right to be treated with fairness and with respect for the victim's dignity and privacy throughout the criminal justice process.

B. PERSONAL DATA PROTECTION PROVISIONS

The primary laws governing privacy and data security in Texas are the Identity Theft Enforcement and Protection Act (hereinafter “ITEPA“) (Tex. Bus. & Com. Code § 521001 et seq.) and the Medical Records Privacy Act (hereinafter “MRPA“) (Tex. Health & Safety Code § 181001 et seq.), which are outlined below and are discussed in detail at Section I.C.6., Section I.C.7., and Section I.C.8. (ITEPA), as well as Section I.D.9. (MRPA). There are additional privacy laws, including laws governing the protection of driver's license and social security numbers (Tex. Bus. & Com. Code § 501001 et seq.; see Section I.D.6. and Section I.D.10.), the protection of biometric identifiers (Tex. Bus. & Com. Code § 503.001; see Section I.D.1), and the prohibition on the interception of wire, oral, or electronic communications (Texas Penal Code § 16.02; see Section I.F.). Finally, laws related to privacy and data security applicable to specific sectors, such as health care and insurance, are set forth in the portions of this profile dedicated to those sectors.

1. Who is covered?

ITEPA: With respect to its provisions preventing identity theft, the Identity Theft Enforcement and Protection Act (ITEPA) covers individuals whose personal identifying information has been obtained, possessed, transferred, or used by another without the person's consent (Tex. Bus. & Com. Code § 521051(a)). In relation to a business's duty to protect specified information, the ITEPA applies to persons whose sensitive personal information has been collected or maintained by a business (Tex. Bus. & Com. Code § 521052(a)). Finally, with respect to data breach notification requirements, the ITEPA covers any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person (Tex. Bus. & Com. Code § 521053(b)).

MRPA: The requirements of the Medical Records Privacy Act (MRPA) apply to any individual who is the subject of protected health information, as defined under the privacy regulations issued under the federal Health Insurance Affordability and Accountability Act (the HIPAA Privacy Rule) (Tex. Health & Safety Code § 181001(a); see 45 C.F.R. § 160.103).

2. What is covered?

ITEPA: The Identity Theft Enforcement and Protection Act (ITEPA) covers a number of specific items, including identity theft, the duty of businesses to protect and, when applicable, to destroy sensitive personal information, and data breach notification.

Identity theft: Under ITEPA, no person may obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with the intent to obtain anything of value in the person's name (Tex. Bus. & Com. Code § 521051(a)). For a comprehensive discussion of identity theft, including penalties and private causes of action for violations, see Section I.G.2.

Duty to protect: A business must implement and maintain reasonable procedures, including taking an appropriate corrective action, to protect any sensitive personal information collected by the
business during the regular course of business from unlawful use or disclosure (Tex. Bus. & Com. Code § 521052(a)). For more information on this duty to protect, see Section I.C.6.

Duty to destroy: Businesses must destroy or arrange for the destruction of customer records containing sensitive personal information in their custody that are not to be retained (Tex. Bus. & Com. Code § 521052(b)). For more information on this duty to destroy, see Section I.C.7.

Data breach notification: A person conducting business in Texas who owns or licenses computerized data including sensitive personal information must disclose any breach of system security after discovering or receiving notification of the breach, to any person whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person (Tex. Bus. & Com. Code § 521053). For details on data breach notification requirements, see Section I.C.8.

**MRPA:** The Medical Records Privacy Act (MRPA) covers a variety of issues related to the privacy and handling of protected health information, including training for employees with respect to federal and state privacy law and regulations regarding protected health information (Tex. Health & Safety Code § 181.101), access to electronic health records (Tex. Health & Safety Code § 181.102 et seq.), and restrictions on the sale or disclosure of such information (Tex. Health & Safety Code § 181.153 and Tex. Health & Safety Code § 181.154) and on its use for marketing purposes (Tex. Health & Safety Code § 181.152). For purposes of the MRPA, “protected health information” has the same meaning as under the HIPAA Privacy Rule (Tex. Health & Safety Code § 181.001(a); see 45 C.F.R. § 160.103). For a comprehensive overview of the MRPA, see Section I.D.9.

3. Who must comply?

**ITEPA:** The restrictions imposed by Identity Theft Enforcement and Protection Act (ITEPA) with respect to identity theft apply to any person obtaining, possessing, transferring, or using the personal identifying information of another person (Tex. Bus. & Com. Code § 521051(a)). The law’s provisions regarding a duty to protect and, when applicable, destroy sensitive personal information apply to all businesses, including nonprofit athletic or sports associations, but not financial institutions as defined by the federal Gramm-Leach-Bliley Act (Tex. Bus. & Com. Code § 521052(a) to Tex. Bus. & Com. Code § 521052(d)). The ITEPA’s data breach notification requirements apply to any person doing business in the state who owns or licenses computerized data that includes sensitive personal information, as well as to any person who maintains, but does not own, sensitive personal information, and who discovers any breach of system security where sensitive personal information was, or was reasonably expected to be, acquired by an unauthorized person (Tex. Bus. & Com. Code § 521053(b) to Tex. Bus. & Com. Code § 521053(c)).

**MRPA:** The requirements regarding the collection, use, and disclosure of protected health information under the Medical Records Privacy Act (MRPA) apply to covered entities. A “covered entity” is defined as any person who—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 and constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information, including 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 maintaining an Internet website (Tex. Health & Safety Code § 181001(b)(2)(A)). The term also includes any person who comes into possession of protected health information, obtains or stores protected information, or is an employee, agent, or contractor of any person described above (Tex. Health & Safety Code § 181001(b)(2)(B) to Tex. Health & Safety Code § 181001(b)(2)(D)).
C. Data Management Provisions

1. Notice & Consent

ITEPA: Under the Identity Theft Enforcement and Protection Act (ITEPA), no person may obtain, possess, transfer, or use personal identifying information of another person without the other person’s consent and with the intent to obtain anything of value in the person’s name (Tex. Bus. & Com. Code § 521.051(a)). For a comprehensive discussion of identity theft, including penalties and private causes of action for violations, see Section I.G.2.

MRPA: Under the Medical Records Privacy Act (MRPA), covered entities are restricted from disclosing protected health information about an individual without providing prior notice and authorization (Tex. Health & Safety Code § 181.154). For a comprehensive overview of the MRPA, see Section I.D.9.

Biometric identifier law: Under the law governing the collection or use of biometric identifiers, no person may capture such an identifier of an individual for a commercial purpose unless the person informs the individual before capturing the identifier and receives the individual’s consent (Tex. Bus. & Com. Code § 503.001(b)). For more information, see Section I.D.1

2. Collection & Use

ITEPA: Under the Identity Theft Enforcement and Protection Act (ITEPA), no person may obtain, possess, transfer, or use personal identifying information of another person without the other person’s consent and with the intent to obtain anything of value in the person’s name (Tex. Bus. & Com. Code § 521.051(a)). For a comprehensive discussion of identity theft, including penalties and private causes of action for violations, see Section I.G.2.

MRPA: Under the Medical Records Privacy Act (MRPA), covered entities generally are prohibited from selling the protected health information of an individual, unless a specific exception applies (Tex. Health & Safety Code § 181.153). For a comprehensive overview of the MRPA, see Section I.D.9.

Biometric identifier law: Under the law governing the collection or use of biometric identifiers, no person may capture such an identifier of an individual for a commercial purpose unless the person informs the individual before capturing the identifier and receives the individual’s consent (Tex. Bus. & Com. Code § 503.001(b)). For more information, see Section I.D.1

Other provisions: For information on the collection and use of social security numbers, see Section I.D.10. For information on the collection and use of driver’s license information, see Section I.D.6. For information on restrictions on the use of crime victim or motor vehicle accident information, see Section I.D.5.

3. Disclosure to Third Parties

ITEPA: Under the Identity Theft Enforcement and Protection Act (ITEPA), no person may transfer personal identifying information of another person without the other person’s consent and with the intent to obtain anything of value in the person’s name (Tex. Bus. & Com. Code § 521.051(a)). For a comprehensive discussion of identity theft, including penalties and private causes of action for violations, see Section I.G.2.

MRPA: Under the Medical Records Privacy Act (MRPA), covered entities are restricted from disclosing protected health information about an individual without providing prior notice and authorization (Tex. Health & Safety Code § 181.154). For a comprehensive overview of the MRPA, see Section I.D.9.
**Biometric identifier law:** The Texas law governing the collection or use of biometric identifiers contains provisions governing the disclosure of such data (see Section I.D.1).

**Social security numbers:** Persons generally are prohibited from disclosing or making available to the public an individual’s social security number. For more information, see Section I.D.10.

**Additional health data provisions:** Specific disclosure requirements apply to hospitals, physicians, mental health facilities and providers, chiropractors, podiatrists, and emergency medical services personnel (see Section I.D.9).

4. **Data Storage**

There are no general laws in Texas governing the storage of data containing personal information. The Texas law governing the collection or use of biometric identifiers contains provisions governing the storage of such data (see Section I.D.1).

5. **Access & Correction**

There are no general provisions regarding an individual’s right to access or correct personal information held by another person or business. Governmental bodies are required to permit access to information they maintain that relates to the person and is protected from public disclosure by laws intended to protect the person’s privacy interests (Tex. Govt Code § 552.023). In addition, governmental bodies must establish a reasonable procedure under which an individual may request a body to correct information possessed by the body that is incorrect (Tex. Govt Code § 559.004).

The Medical Records Privacy Act (MRPA) contains provisions regarding access to patient records (see Section I.D.9.). In addition, several specific provisions governing health care data practitioners and health data contain access requirements (see Section I.D.9.).

6. **Data Security**

**ITEPA:** Under the Identity Theft Enforcement and Protection Act (ITEPA), a business must implement and maintain reasonable procedures, including taking an appropriate corrective action, to protect any sensitive personal information collected by the business during the regular course of business from unlawful use or disclosure (Tex. Bus. & Com. Code § 521052(a)). “Sensitive personal information” includes:

- an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - social security number;
  - driver’s license number or government-issued ID number; or
  - account number or debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or
- information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual (Tex. Bus. & Com. Code § 521002(a)(2)).

Sensitive personal information does not include publicly available information lawfully made available to the public by federal, state, or local government (Tex. Bus. & Com. Code § 521002(b)).

The duty to protect the information described above does not apply to financial institutions as defined under the federal Gramm-Leach-Bliley Act (Tex. Bus. & Com. Code § 521052(c)).
Persons who violate the requirements outlined above are subject to civil penalties and injunctive action (see Section II.C.).

**Biometric identifier law:** The Texas law governing the collection or use of biometric identifiers contains provisions governing the security of such data (see Section I.D.1).

**Hospitals:** Hospitals must adopt and maintain reasonable safeguards for the security of all health care information they maintain (Tex. Health & Safety Code § 241.155).

### 7. Data Disposal

**ITEPA:** Under the Identity Theft Enforcement and Protection Act (ITEPA), businesses must destroy or arrange for the destruction of customer records containing sensitive personal information in their custody that are not to be retained by shredding, erasing, or otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means (Tex. Bus. & Com. Code § 521.052(b)). “Sensitive personal information” includes:

- an individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - social security number;
  - driver’s license number or government-issued ID number; or
  - account number or debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or
- information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual (Tex. Bus. & Com. Code § 521.002(a)(2)).

Sensitive personal information does not include publicly available information lawfully made available to the public by federal, state, or local government (Tex. Bus. & Com. Code § 521.002(b)).

The duty to destroy information described above does not apply to financial institutions as defined under the federal Gramm-Leach-Bliley Act (Tex. Bus. & Com. Code § 521.052(c)).

Persons who violate the requirements outlined above are subject to civil penalties and injunctive action (see Section II.C.).

**Disposal of business records:** Any business record required to be maintained by state law may be destroyed at any time after three years from the date the record was created, unless a separate law or rule specifies a different retention period (Tex. Bus. & Com. Code § 72.002). A business that disposes of a business record containing personal identifying information of a customer must modify—by shredding, erasing, or other means—the personal identifying information to make it unreadable or indecipherable (Tex. Bus. & Com. Code § 72.004(b)). A business will be in compliance with this provision if it contracts with a person engaged in records disposal who follows the requirements (Tex. Bus. & Com. Code § 72.004(c)). This provision does not apply to financial institutions as defined under the federal Gramm-Leach-Bliley Act or covered entities under the Texas Insurance Code (Tex. Bus. & Com. Code § 72.004(a)).

Businesses are not required to modify a business record if the business is required to retain the record under another law, or if the record is historically significant and (a) there is no potential for identity theft or fraud while the business retains custody of the record, and (b) the record is transferred to a professionally managed historical repository (Tex. Bus. & Com. Code § 72.004(f)).
Violators are subject to civil penalties (see Section II.C.).

Under specified circumstances, a business that accepts checks from customers in the ordinary course of business must delete any electronic record indicating that the customer has issued a dishonored check within 30 days of agreement between the parties that the information is incorrect or the customer presents information to the business regarding the fact that the dishonored check was unauthorized (Tex. Bus. & Com. Code § 72.051). Businesses failing to delete such information are subject to civil penalties (see Section II.C.).

**Biometric identifier law:** The Texas law governing the collection or use of biometric identifiers contains provisions governing the destruction of such data (see Section I.D.1).

**8. Data Breach**

Under the Identity Theft Enforcement and Protection Act (ITEPA), a person conducting business in Texas that owns or licenses computerized data including sensitive personal information must disclose any breach of system security after discovering or receiving notification of the breach, to any person whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notification described above must be made as quickly as possible, although delays are available under certain circumstances (see below) (Tex. Bus. & Com. Code § 521053(b)). If an individual whose sensitive personal information has been or is reasonably believed to have been acquired by an unauthorized individual is from another state that requires data breach notification, the person required to provide the notification may do so under Texas law or under the law of the state in which the person has residence (Tex. Bus. & Com. Code § 521053(b-1)). Any person who maintains, but does not own, sensitive personal information must notify the owner or licensee of the information of any breach of the system security immediately after discovering the breach if sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person (Tex. Bus. & Com. Code § 521053(c)).

**Primary definitions:** For purposes of the data breach notification law, a “breach of system security” is defined as unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person acquiring the data has the encryption key. Good faith acquisition of such data by an employee or agent of the person for the purposes of the person does not constitute a breach of system security unless the information is used in an unauthorized manner (Tex. Bus. & Com. Code § 521053(b)).

“Sensitive personal information” includes:

- an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
  - social security number;
  - driver's license number or government-issued ID number;
  - account number or debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account; or
- information that identifies an individual and relates to:
  - the physical or mental health or condition of the individual;
  - the provision of health care to the individual; or
  - payment for the provision of health care to the individual (Tex. Bus. & Com. Code § 521002(a)(2)).

Sensitive personal information does not include publicly available information lawfully made available to the public by federal, state, or local government (Tex. Bus. & Com. Code § 521002(b)).
Delays in providing notice: Notice may be delayed briefly as necessary to determine the scope of the breach and to restore the reasonable integrity of the data system (Tex. Bus. & Com. Code § 521.053(a)). In addition, such notice may be delayed at the request of a law enforcement agency that determines that notice will impede a criminal investigation. Notice must be provided as soon as the agency determines that the investigation is no longer impeded (Tex. Bus. & Com. Code § 521.053(d)).

Proper form of notice: A person required to provide breach notification may provide written notice at the last known address of the individual; electronic notice, provided that it meets federal electronic notice and signature requirements; or substitute notice (Tex. Bus. & Com. Code § 521.053(e)). Substitute notice is authorized if the person required to provide notice can show that the cost of providing notice would exceed $250,000, the number of affected persons exceeds 500,000, or the person does not have sufficient contact information. On such a showing, the person may give notice via e-mail, if the person has e-mail addresses for the affected individuals; conspicuous posting of the notice on the person’s website; or notice published in or broadcast on statewide media (Tex. Bus. & Com. Code § 521.053(f)). A person making notification in accordance with an information security policy that complies with the breach notification requirements described above is in compliance with these provisions if it provides notification in accordance with the policy (Tex. Bus. & Com. Code § 521.053(g)).

Consumer reporting agency notification: Any person required under the data breach notification law to notify at one time more than 10,000 persons of a breach must also, without unreasonable delay, notify each consumer reporting agency maintaining files on consumers on a nationwide basis of the timing, distribution, and content of the notices (Tex. Bus. & Com. Code § 521.053(h)).

Insurance providers: The Texas Department of Insurance (TDI) requires domestic or commercially-domiciled insurance companies and health maintenance organizations to contact their assigned financial analysts at TDI following the unauthorized acquisition, release, or use of personal information or sensitive company information (see Commissioner’s Bulletin # B-0022-16). TDI may then request information concerning the incident.

Civil penalties: Persons who violate the requirements outlined above are subject to civil penalties and injunctive action (see Section II.C.).

9. Data Transfer & Cloud Computing

While our research has revealed no laws of general application in Texas addressing data transfers or cloud computing, Tex. Gov’t Code § 2157.007 provides that state agencies may consider cloud computing service options when making purchases for a major information resources project. When doing so, the state agency “shall ensure that information resources projects that use cloud computing service options meet or exceed required state standards for cybersecurity.” Tex. Gov’t Code § 2157.007(c).

Moreover, Tex. Gov’t Code § 2054.068 requires the Department of Information Resources to collect from each state agency information on the status and condition of the agency’s information technology infrastructure, including information regarding “an inventory of the agency’s servers, mainframes, cloud services, and other information technology equipment.” Tex. Gov’t Code § 2054.068(b)(2).

10. Other Provisions

Regulations addressing the maintenance, release, transfer, and disposal of medical records are found in Tex. Admin. Code tit. 22 § 155.1 et seq.
D. SPECIFIC TYPES OF DATA

1. Biometric Data

Texas is one of a handful of states to have a law specifically addressing the collection, use, and disclosure of biometric identifier information (Tex. Bus. & Com. Code § 503.001). Under the law, a “biometric identifier” is defined as a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry (Tex. Bus. & Com. Code § 503.001(a)).

Restrictions on collection, use, sale, or disclosure: A person may not capture a biometric identifier of an individual for commercial purposes unless the person informs the individual before capturing the identifier and receives the individual’s consent (Tex. Bus. & Com. Code § 503.001(b)). In addition, a person possessing such an identifier may not sell, lease, or otherwise disclose it to another person unless:

- The individual consents to the disclosure for identification purposes in the event of the individual’s disappearance or death;
- The disclosure completes a financial transaction requested or authorized by the individual;
- The disclosure is required or permitted by federal or state law; or
- The disclosure is made by or to a law enforcement agency in response to a warrant (Tex. Bus. & Com. Code § 503.001(c)(1)).

Security requirements: A person possessing a biometric identifier for commercial purposes must store, transmit, and protect from disclosure the identifier using reasonable care and in a manner that is as or more protective than the manner in which the person handles any other confidential information in its possession (Tex. Bus. & Com. Code § 503.001(c)(2)).

Destruction requirements: A person possessing a biometric identifier for commercial purposes must destroy the biometric identifier within a reasonable time, but no more than one year from the date that the purpose for collecting the identifier expires (Tex. Bus. & Com. Code § 503.001(c)(3)). However, if such a biometric identifier has been captured for use in connection with an instrument or document that must be retained for a longer period by law than that described above, the person must destroy it within a reasonable time, but not later than one year after the date the instrument or document is no longer required to be maintained (Tex. Bus. & Com. Code § 503.001(c-1)). In addition, if a biometric identifier has been collected for security purposes by an employer, the purpose for collection is deemed to have expired on the date of the employee’s termination (Tex. Bus. & Com. Code § 503.001(c-2)).

Exemption: The prohibitions outlined above do not apply to voiceprint data retained by a financial institution or its affiliates as defined under the federal Gramm-Leach-Bliley Act (Tex. Bus. & Com. Code § 503.001(e)).

Penalties: Persons violating the provisions outlined above are subject to civil penalties (see Section II.C.).

2. Consumer Data

Many types of consumer data, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.). In addition, under the breach notification law, any person required to notify at one time more than 10,000 persons of a breach must also, without unreasonable delay, notify each consumer reporting agency maintaining files on consumers on a nationwide basis of the timing, distribution, and content of the notices (Tex. Bus. & Com. Code § 521053(h)).
3. Credit Card Data

Information relevant to credit card data, including names in combination with data elements such as social security numbers or account numbers, is “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Businesses accepting a credit or debit card for a transaction may not print more than the last four digits of a credit or debit card number or the month or year of expiration for a credit or debit card on a receipt or other document evidencing the transaction (Tex. Bus. & Com. Code § 502.002(a)). The prohibition does not apply to transactions where the sole means of recording the credit or debit card number on a receipt or other document is by handwriting or an imprint of the card (Tex. Bus. & Com. Code § 502.002(b)). A person providing, selling, or leasing a cash register to a business must provide notice of the prohibition to the business (Tex. Bus. & Com. Code § 502.002(c)). Civil penalties apply to a violation (see Section II.C.).

Businesses that accept credit cards from customers may require them to provide their zip codes to verify the customers’ identities with the credit card issuer (Tex. Bus. & Com. Code § 505.002)). However, the business may not retain the zip code information after completion of the purchase (Tex. Bus. & Com. Code § 505.003). In addition, effective Jan. 1, 2018, a merchant may require an individual using a credit or debit card to provide a photo identification to verify the individual’s identity, and may refuse to accept the card if the individual refuses (Tex. Bus. & Com. Code § 508.002).

4. Credit Reports

ITEPA: Information relevant to credit reports, including names in combination with data elements such as social security numbers or account numbers, is “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Credit reporting agency provisions: Under Texas law governing the regulation of consumer credit reporting agencies, such agencies are permitted to furnish consumer reports in a number of circumstances, including pursuant to a court order, or to persons intending to use the information for credit transactions, employment decisions, or insurance underwriting, among others (Tex. Bus. & Com. Code § 20.02). Some items may not be included, such as certain bankruptcy adjudications that are over 10 years old, or suits or judgments, tax liens, arrest or indictment records, or other items that are over seven years old (Tex. Bus. & Com. Code § 20.05(a)). However, such information may be included in a consumer report if it is provided in connection with a credit transaction with a principal amount over $150,000, the underwriting of life insurance with a face amount of over $150,000, or an employment application for an annual salary of $75,000 or more (Tex. Bus. & Com. Code § 20.05(b)). A consumer reporting agency may not provide any medical information about a consumer in a consumer report for employment purposes or in connection with a credit, insurance, or direct marketing transaction without the consent of the consumer (Tex. Bus. & Com. Code § 20.05(d)).

Consumer reporting agencies must provide consumers who provide consumer credit information to the agency with the opportunity to correct previously reported inaccurate information through reasonable procedures designed to ensure that the file is corrected in a prompt and timely fashion (Tex. Bus. & Com. Code § 20.07).

Texas law governing credit reporting agencies also contains provisions governing required disclosures to consumers (Tex. Bus. & Com. Code § 20.03), as well as the placement of security
alerts and security freezes on such reports at the request of the consumer (Tex. Bus. & Com. Code § 20.031et seq.). Consumers have a private right of action or a right to binding arbitration to enforce the obligations on consumer reporting agencies outlined above (see Section I.G.1), as well as civil penalties (see Section II.C.).

5. Criminal Records

Child care facilities, child placing agencies, and family homes: The director, owner, or operator of a child care facility, child placing agency, or family home must submit the names of the director, owner, or operator, all current and prospective employees, all current or prospective foster or adoptive parents, and other specified persons to the Department of Family and Protective Services for the conduct of a criminal history check. The names must be submitted at the time of application for operation or registration as a family home, and at least once during every 24 months after receiving a license or registration (Tex. Hum. Res. Code § 42.056(a)). Submission of fingerprint information sufficient to the Department of Public Safety and the FBI is also required under specified circumstances (Tex. Hum. Res. Code § 42.056(a-2) to Tex. Hum. Res. Code § 42.056(a-5)). The Department must conduct the criminal background check according to specific statutory requirements (Tex. Hum. Res. Code § 42.056(b) to Tex. Hum. Res. Code § 42.056(f). No person whose name is submitted may provide direct care or have direct access to a child before the background check is completed unless an exception applies (Tex. Hum. Res. Code § 42.056(g) to Tex. Hum. Res. Code § 42.056(h)). Violations of these provisions constitute a class B misdemeanor (see Section I.H.).

Expunction of arrest records: Upon an order of expunction of arrest records (sometimes referred to as expungement, see Tex. Code Crim. Proc. § 55.01et seq.), a person may deny the occurrence of an arrest and the existence of the expunction order (Tex. Code Crim. Proc. § 55.03).

In-home service companies and residential services companies: Certain in-home service companies and residential delivery companies are required to conduct a criminal background check on a prospective employee (see Section I.E.6.).

6. Drivers’ Licenses/Motor Vehicle Records

Prohibitions on agency disclosure: Under the Motor Vehicle Records Disclosure Act (Tex. Transp. Code § 730.001et seq.), no Texas state agency may disclose personal information about a person obtained by the agency in connection with a motor vehicle record, excepted for specified exceptions and permitted disclosures under the Act.

Driver’s license numbers used in merchandise returns: A merchant or third party under contract with the merchant who requires a consumer returning merchandise to provide his driver’s license number may use the number solely for identification purposes if the customer is seeking a refund or store credit and does not have a valid receipt. The merchant may not disclose the driver’s license number to any other party not involved in the initial transaction and may use the information only to monitor, investigate, or prosecute fraudulent returns. In addition, a merchant must destroy the information at the expiration of six months from the date of the transaction (Tex. Bus. & Com. Code § 501.101). Violations of these provisions are subject to civil penalties (see Section II.C.).

Prohibition on printing driver’s license number on receipt: A person may not print an individual’s driver’s license number on a receipt evidencing payment for goods or services (Tex. Bus. & Com. Code § 501.111). Violations are subject to civil penalties (see Section II.C.).

Security requirements for enhanced licenses: Enhanced driver’s licenses and personal identification certificates issued by the Texas Department of Transportation must include reasonable security measures to protect against unauthorized disclosure of information about the
holder. If the enhanced license or ID includes a radio frequency identification chip or other technology, it must be encrypted (Tex. Transp. Code § 521032(c)).

7. Electronic Communications/Social Media Accounts

**Warrants required for data held by e-mail service providers:** Under the Texas Code of Criminal Procedure, law enforcement agencies must obtain a warrant to obtain stored communications data, including wire communications and electronic communications, held by e-mail providers. The law outlines the requirements agencies must meet in obtaining a warrant (Tex. Code Crim. Proc. § 18.21(5A) and Tex. Code Crim. Proc. § 18.21(5B)).

**Online impersonation:** A person commits an offense if he uses the name or persona of another person to create a webpage or send messages through or on a commercial social networking site or other Internet website, or sends an e-mail designed to cause the recipient to believe that another person authorized or transmitted the e-mail (Tex. Penal Code § 33.07). For more information, see Section I.H.

**Anti-spam law:** For information on Texas provisions regarding the prohibition on certain commercial electronic communications, see Section I.E.1

**Illegal divulgence of public communications:** A person who provides an electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication, unless the communication was divulged (a) as authorized by federal or state law, (b) to a person at a facility used to forward the communication to the communication's destination, or (c) to a law enforcement agency (Tex. Penal Code § 16.05(b) to Tex. Penal Code § 16.05(c)). In general, a divulgement of a scrambled or encrypted radio communication is a state jail felony (Tex. Penal Code § 16.05(d)). However, if a divulgement is committed for a tortious or illegal purpose or to gain a benefit, an offense involving a radio communication that is not scrambled or encrypted is a class A misdemeanor if the communication is not a public land mobile radio service communication or a paging service communication, or a class C misdemeanor if the communication is a public land mobile radio service communication or a paging service communication (Tex. Penal Code § 1605(e)).

**Interception of electronic communications:** For information on legal limitations on the interception of electronic communications under the Texas Penal Code, see Section I.F.

8. Financial Information

There are no Texas laws dealing generally with the collection, use, or disclosure of financial information. However, regulations issued by the Texas Department of Insurance governing the disclosure of nonpublic personal financial information of consumers and customers of insurers licensed under Texas Insurance law essentially implement the requirements applicable to the insurance industry under the federal Gramm-Leach-Bliley Act (Tex. Admin. Code tit. 28 § 22.1 et seq.). For more information, see Section I.E.7.

Under the Finance Code, with respect to requests for financial records in the course of litigation, an affected customer who is not a party to the proceeding must give written permission to the financial institution before the institution may release the information pursuant to subpoena (Tex. Fin. Code § 59.006(c) to Tex. Fin. Code § 59.006(d)).

9. Health Data

**MRPA:** The Medical Records Privacy Act (MRPA) (Tex. Health & Safety Code § 181001 et seq.) governs the collection, use, and disclosure of protected health information (PHI). The law generally
follows the provisions of the HIPAA Privacy Rule (45 C.F.R. § 160.101 et seq., and 45 C.F.R. Subpart A and Subpart E), but the Texas provisions impose additional restrictions, as outlined below.

Primary definitions: For purposes of the MRPA, “protected health information” has the same meaning as under the HIPAA Privacy Rule (Tex. Health & Safety Code § 181.001(a); see 45 C.F.R. § 160.103).

A “covered entity” is defined as any person who—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 and constructive knowledge, in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information, including 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 maintaining an Internet website (Tex. Health & Safety Code § 181.001(b)(2)(A)). The term also includes any person who comes into possession of protected health information, obtains or stores protected information, or is an employee, agent, or contractor of any person described above (Tex. Health & Safety Code § 181.001(b)(2)(B) to Tex. Health & Safety Code § 181.001(b)(2)(D)).

Notice and authorization requirements: A covered entity must provide notice to an individual for whom the entity creates or receives PHI if it is subject to electronic disclosure. The notice may be given by posting written notice in the entity’s place of business, posting the notice on the entity’s website, or posting the notice in another place where affected individuals are likely to see it (Tex. Health & Safety Code § 181.154(a)). A covered entity may not electronically disclose an individual’s PHI without a separate authorization from the individual or the individual’s representative for each disclosure. The authorization may be made in written or electronic form, or oral form if the covered entity documents the oral authorization (Tex. Health & Safety Code § 181.154(b)).

Authorization is not required if the disclosure is to another covered entity or to an entity covered under the Insurance Code for the purposes of treatment, payment, health care operations, or performing an insurance or health maintenance organization function, or for any purpose otherwise authorized by state or federal law (Tex. Health & Safety Code § 181.154(c)).

Access to PHI: Any health care provider using an electronic health records system capable of fulfilling a request must provide the electronic health record of a person to that person within 15 business days of receiving a request for the record. The record must be provided electronically unless the person agrees to receive it in another form (Tex. Health & Safety Code § 181.102(a)). Health care providers are not required to provide access if such access is excepted under the HIPAA Privacy Rule (Tex. Health & Safety Code § 181.102(b); see 45 C.F.R. § 164.524).

Certain insurers and employers exempted: Entities covered under the Texas Insurance Code and employers are exempt from the MRPA except for the provisions related to notice and authorization requirements (see above) and prohibited acts (see below) (Tex. Health & Safety Code § 181.051).

Exemptions: The following entities are exempt from the MRPA with respect to activities specified in the law:

- a covered entity engaged in the activities of a financial institution for purposes of the processing of a payment transaction (Tex. Health & Safety Code § 181.052);
- nonprofit agencies paying for health care services or prescription drugs for an indigent person (Tex. Health & Safety Code § 181.053);
- workers’ compensation insurance or any entities in connection with the administration of self-insured worker’s compensation insurance (Tex. Health & Safety Code § 181.054);
- employee benefit plans or covered entities or other persons acting in connection with such a plan (Tex. Health & Safety Code § 181.055);
- the American Red Cross (Tex. Health & Safety Code § 181.056);
• agencies disclosing information relating to patients in custody with mental impairments (Tex. Health & Safety Code § 181.057);
• certain educational records (Tex. Health & Safety Code § 181.058); and

Prohibited acts: A person may not reidentify or attempt to reidentify an individual who is the subject of any PHI without first obtaining the individual’s consent or authorization (Tex. Health & Safety Code § 181.151).

Covered entities must obtain clear and unambiguous permission in written or electronic form to use or disclose PHI for any marketing communication, unless the communication is a face-to-face communication between the covered entity and the individual, is a promotional gift of nominal value provided by the covered entity, is necessary for the administration of a patient assistance program or other prescription savings or discount program, or is made at the oral request of the individual (Tex. Health & Safety Code § 181.152(a)). Additional restrictions apply to permitted uses or disclosures of PHI in marketing material (Tex. Health & Safety Code § 181.152(b) to Tex. Health & Safety Code § 181.152(d)).

Covered entities may not disclose an individual’s PHI for direct or indirect remuneration unless disclosure is to another covered entity or to an entity covered under the Insurance Code for the purposes of treatment, payment, health care operations, or performing an insurance or health maintenance organization function, or for any purpose otherwise authorized by state or federal law (Tex. Health & Safety Code § 181.153(a)). Any remuneration received for a disclosure for performing an insurance or health maintenance organization function may not exceed the covered entity’s reasonable costs of preparing and transmitting the PHI (Tex. Health & Safety Code § 181.153(b)).

Training required: Each covered entity must provide training to its employees regarding the state and federal law requirements governing PHI as necessary and appropriate to carry out their duties. The training must be completed within 90 days from the date of the hire of the employee. Additional training with respect to material changes in the law must be provided within a reasonable period not to exceed one year from the date of the material change. Employees must sign a statement verifying completion of all training, and the covered entity must retain the statement for six years (Tex. Health & Safety Code § 181.101).

Civil penalties: Covered entities violating the requirements of the MRPA are subject to civil penalties and injunctive action (see Section II.C.).

Insurance regulations on privacy of consumer health information: Regulations issued by the Texas Department of Insurance govern the disclosure of nonpublic personal health information of consumers and customers of insurers licensed under Texas Insurance law (Tex. Admin. Code tit. 28 § 22.51 et seq.). For more information, see Section I.E.7.

Requirements specific to hospitals: Hospitals or agents or employees of hospitals may not disclose health care information to any person other than the patient or the patient’s representative without written authorization (Tex. Health & Safety Code § 241.152(a)). The authorization must be dated and signed and identify the information to be disclosed and the person to whom it is to be disclosed. It cannot be contained in the same document containing the patient’s consent to medical treatment (Tex. Health & Safety Code § 241.152(b)). An authorization is valid for 180 days after the date it is signed (Tex. Health & Safety Code § 241.152(c)). In general, the authorization may be revoked at any time, but an exception exists for disclosure required for payment purposes (Tex. Health & Safety Code § 241.152(d) to Tex. Health & Safety Code § 241.152(e)). Patients may not maintain an action against a hospital for a disclosure made by the hospital in good faith that relies
on an authorization for which the hospital did not have notice of revocation (Tex. Health & Safety Code § 241.152(f)).

Specified disclosures without written authorization are permitted, including to other health care providers rendering health care to the patient, transporting emergency medical service providers, or specified state and local government agencies, among others (Tex. Health & Safety Code § 241.153).

Hospitals must provide access to and copies of patient records upon request. Within 15 days of receipt of a request, the hospital must make the information available for inspection during regular business hours and provide a copy of the records if requested, or must notify the requestor if the information does not exist or cannot be found (Tex. Health & Safety Code § 241.154(a)). The hospital may charge a reasonable fee for access and copies, although certain exceptions apply (Tex. Health & Safety Code § 241.154(b) to Tex. Health & Safety Code § 241.154(e)).

Hospitals must adopt and maintain reasonable safeguards for the security of all health care information they maintain (Tex. Health & Safety Code § 241.155). Patients are entitled to bring an action for violations of these provisions (see Section I.G.4.).

**Physicians:** Communications between physicians and patients, as well as records created by the physician, are confidential, and any person receiving information with respect to such communications or records may not disclose the information except as consistent with the authorized purposes for which the information was obtained. The prohibitions on disclosure apply regardless of when the patient received services from the physician, except for medical records at least 75 years old requested for historical research purposes (Tex. Occ. Code § 159.002(a) to Tex. Occ. Code § 159.002(d)).

An exception to the nondisclosure requirement is provided for certain disclosures related to judicial proceedings (Tex. Occ. Code § 159.002(f)). Additional exceptions apply for administrative purposes (Tex. Occ. Code § 159.003) and for other reasons, such as to government, law enforcement, or medical personnel under specified circumstances (Tex. Occ. Code § 159.004).

Physicians must have written consent for any release of confidential information. The consent must be signed by the patient, parent, legal guardian, attorney, or personal representative and must specify the records or other information covered, the reasons or purposes for release, and the persons to whom the release is to be made (Tex. Occ. Code § 159.005(a) to Tex. Occ. Code § 159.005(b)). In general, the authorization may be revoked at any time (Tex. Occ. Code § 159.005(c)). Patients may not maintain an action against a hospital for a disclosure made by the physician in good faith that relies on an authorization for which the physician did not have notice of revocation (Tex. Occ. Code § 159.005(d)). Any person receiving such information may disclose the information to another only for the specified purposes of the original disclosure (Tex. Occ. Code § 159.005(e)).

A physician receiving a written request for information as outlined above must furnish copies of records or a summary or narrative of the records. In providing such records, the physician may delete confidential information about another patient or family member of the patient who has not consented to the release. Similarly, a physician must furnish copies of records to subsequent or consulting physicians on receiving a written consent (Tex. Occ. Code § 159.006(a) to Tex. Occ. Code § 159.006(c)). The physician must provide the information within 15 days of receiving the request (Tex. Occ. Code § 159.006(d)). If the physician denies the request, he must furnish the patient with a signed and dated written statement providing the reasons for the denial and must place a copy of that statement in the patient's records (Tex. Occ. Code § 159.006(e)). The information may be provided in any medium agreed upon by the parties (Tex. Occ. Code § 159.007), and the physician may charge a reasonable fee (Tex. Occ. Code § 159.008).
Patients are entitled to bring an action for violations of these provisions (see Section I.G.4.).

**Mental health facilities and professionals:** Records maintained by a mental health facility are confidential and may not be disclosed unless permitted by other state law (Tex. Health & Safety Code § 576.005).

Communications between a professional and a patient regarding the diagnosis or treatment of any mental condition or disorder, including alcoholism and drug addiction, are confidential and generally may not be disclosed (Tex. Health & Safety Code § 611.002). However, disclosures may be made under specified circumstances, such as to government, medical, or law enforcement personnel, or to persons with the patient’s written consent, among others (Tex. Health & Safety Code § 611.004 and Tex. Health & Safety Code § 611.006).

In addition, patients are entitled to access their records, unless the professional determines that release would be harmful to the patient’s health. The statute outlines the obligations of professionals who deny access (Tex. Health & Safety Code § 611.0045(a) to Tex. Health & Safety Code § 611.0045(e)). Records must be made available to the patient or specified persons acting on their behalf, and information concerning another person that has not consented to the release must be deleted. If the patient or representative requests a summary or narrative of the record, the professional must prepare it (Tex. Health & Safety Code § 611.0045(f) to Tex. Health & Safety Code § 611.0045(h)). Access must be granted within a reasonable time and for a reasonable fee (Tex. Health & Safety Code § 611.008), and the law further provides that access and copies must be provided within 15 days of receipt of a written request (Tex. Health & Safety Code § 611.007).

Consent for the disclosure of confidential information as outlined above may be revoked at any time by the patient or representative, but authorization for payment purposes may not be revoked (Tex. Health & Safety Code § 611.007).

A person aggrieved by the improper disclosure of or the improper failure to disclose information as described above may petition a court for injunctive relief and damages (see Section I.G.4.).

**Chiropractors and podiatrists:** Communications between chiropractors and patients are confidential, and any person receiving information with respect to such communications may not disclose the information except as consistent with the authorized purposes for which the information was obtained (Tex. Occ. Code § 201.402). Exceptions to the disclosure requirement are provided for administrative purposes (Tex. Occ. Code § 201.403) and for other reasons, such as to government, law enforcement, or medical personnel under specified circumstances (Tex. Occ. Code § 201.404).

Chiropractors must furnish a copy of records requested or a summary of such records on the “written consent” of the patient within a reasonable time and may charge a reasonable fee for doing so (Tex. Occ. Code § 201.405(f)). The written consent must be signed by the patient or his representative and must include the information to be released, the reasons for the disclosure, and the persons to whom the information is to be disclosed (Tex. Occ. Code § 201.405(c)). Consent may be withdrawn at any time (Tex. Occ. Code § 201.405(d)). Any person receiving information pursuant to valid consent may disclose the information to another only for the specified purposes of the original disclosure (Tex. Occ. Code § 201.405(e)). Finally, chiropractors may refuse to release requested information if they determine that access would be harmful to the patient (Tex. Occ. Code § 201.405(g)).


**Emergency medical services providers:** Communications between emergency medical services (EMS) providers and patients, as well as records created by EMS personnel, are confidential, and
any person receiving information with respect to such communications may not disclose the information except as consistent with the authorized purposes for which the information was obtained (Tex. Health & Safety Code § 773.091). Exceptions to confidentiality are provided for certain court or administrative proceedings and other specific circumstances (Tex. Health & Safety Code § 773.092).

Consent for release of confidential information must be in writing; must be signed by the patient, parent, legal guardian, attorney, or personal representative; and must specify the records or other information covered, the reasons or purposes for release, and the persons to whom the release is to be made (Tex. Health & Safety Code § 773.093(a)). In general, the authorization may be revoked at any time (Tex. Health & Safety Code § 773.093(a)). Any person receiving such information may disclose the information to another only for the specified purposes of the original disclosure (Tex. Health & Safety Code § 773.093(c)).

Patients are entitled to bring an action for violations of these provisions (see Section I.G.4.).

**HMOs:** Health maintenance organizations (HMOs) are specifically restricted from disclosing health information under the Texas Insurance Code. In general, any health information of an enrollee or applicant obtained by an HMO is confidential and may not be disclosed to any person except for specified purposes, including with the consent of the enrollee or applicant, to carry out certain statutory purposes, in compliance with a law or court order, or in the event of litigation. The HMO may claim any privilege that a physician or provider would be entitled by law to claim (Tex. Ins. Code § 843.007). Civil remedies and criminal penalties for violations of these provisions are provided (see Section II.C. and Section I.H.).

**Birth defect and cancer registries and communicable disease reporting:** Under the Health and Safety Code, specific restrictions apply to the release of any information by a state agency collected in connection with the state’s birth defect registry (Tex. Health & Safety Code § 87.002) and cancer registry (Tex. Health & Safety Code § 82.009). Similar provisions restrict the release of any information regarding communicable diseases such as HIV/AIDS that is required to be reported to local health authorities (Tex. Health & Safety Code § 81046).

**HIV/AIDS:** HIV/AIDS tests are confidential, and any person who possesses or has knowledge of a test result may not release or disclose it except under specified circumstances (Tex. Health & Safety Code § 81103). A violation of this nondisclosure requirement is a class A misdemeanor (Tex. Health & Safety Code § 81103(j)). In addition, a civil cause of action is available (see Section I.G.4.).

**Mental retardation programs:** Records of the identity, diagnosis, evaluation, or treatment of a person in connection with an intellectual disability are confidential and may only be disclosed under specified circumstances (Tex. Health & Safety Code § 595.001). A record may be disclosed with the consent of the person about whom the record is maintained or a parent, guardian, or executor (Tex. Health & Safety Code § 595.003). Such records may be made available without consent under specified circumstances (Tex. Health & Safety Code § 595.005). The person about whom a record is made must be made available upon the person’s request unless the qualified professional responsible for supervising the person states in writing that access is not in the person’s best interest. Parents or guardians of a minor are entitled to access (Tex. Health & Safety Code § 595.004)

**Texas Medical Board:** Regulations addressing the maintenance, release, transfer, and disposal of medical records are found in Tex. Admin. Code tit. 22 § 165.1 et seq.

10. Social Security Numbers

Provisions of the Business and Commerce Code impose a confidentiality obligation on social security numbers (SSNs), as outlined below.
**Privacy policy required:** No person may require an individual to disclose an SSN to obtain goods or services or enter into a transaction unless the person adopts a privacy policy, makes the policy available, and maintains the confidentiality and security of the SSN disclosed (Tex. Bus. & Com. Code § 501.052(a)). The privacy policy must include information on how personal information is collected, how and when it will be used, how it is protected, the persons who have access to the information, and the method of disposal (Tex. Bus. & Com. Code § 501.052(b)). Civil penalties apply to a violation (see Section II.C.).

**Communication of SSNs:** A person other than a government or governmental subdivision may not intentionally communicate or make public an individual’s SSN, display an SSN on a card or other device required to access a product, require a person to transmit an SSN over the Internet unless the connection is secure and the number is encrypted, require an SSN for access to a website unless a password or unique personal ID is also required, or print an SSN on material sent by mail unless an exception applies (Tex. Bus. & Com. Code § 501.001(a)). A person using an SSN in contravention of the requirements above before Jan. 1, 2005, may continue to do so if the person provides an annual disclosure to the individual that he can opt out of the use, and no person may deny services to an individual because of an opt-out (Tex. Bus. & Com. Code § 501.001(b) to Tex. Bus. & Com. Code § 501.001(c)). A person must comply with an opt-out request no later than 30 days after receiving the request (Tex. Bus. & Com. Code § 501.001(d)). Certain exceptions apply (Tex. Bus. & Com. Code § 501.001(e) to Tex. Bus. & Com. Code § 501.001(f)).

**Other uses of SSNs:** No person may print an SSN on a card or other device required to access a product or service unless the individual consents in writing, and the person may not require such printing as a condition of receipt of or access to a product or service (Tex. Bus. & Com. Code § 501.002(a)). Certain exceptions apply, as do civil penalties for violation (Tex. Bus. & Com. Code § 501.002(b) to Tex. Bus. & Com. Code § 501.002(d); see Section II.C.).

**Use in merchandise returns:** A merchant or third party under contract with the merchant who requires a consumer returning merchandise to provide his social security number may use the number solely for identification purposes if the customer is seeking a refund or store credit and does not have a valid receipt. The merchant may not disclose the social security number to any other party not involved in the initial transaction and may use the information only to monitor, investigate, or prosecute fraudulent returns. Finally, a merchant must destroy the information at the expiration of six months from the date of the transaction (Tex. Bus. & Com. Code § 501.101).

**11. Usernames & Passwords**

There are no specific provisions of Texas law governing the privacy of usernames or passwords. Such information, when combined with a name, may be considered “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

**12. Information about Minors**

Under certain circumstances, a child may consent to medical, dental, psychological, or surgical treatment without the consent of a parent or guardian (Tex. Fam. Code § 32.003). However, a physician, dentist, or psychologist may, with or without the consent of a child who is a patient, advise the parent or guardian of the treatment given to or needed by the child (Tex. Fam. Code § 32.003(d)).

Parents generally must be given 48 hours’ notice before a physician may perform an abortion on an unemancipated minor. Exceptions exist for procedures conducted pursuant to a court order authorizing the minor to consent or in emergency situations (Tex. Fam. Code § 33.002).
A report of alleged or suspected child abuse or neglect, and the identity of the person making it, and files, records, and communications used in a child abuse investigation are confidential and may not be disclosed by any person except under specified circumstances. Adoptive parents of a child who was the subject of an investigation, and any adult who was the subject of an investigation as a child, are entitled to examine and make copies of the records associated with the investigation (Tex. Fam. Code § 261.201).

13. Location Data

Manufacturers of new motor vehicles sold or leased in Texas that are equipped with a recording device must disclose the existence of the device in the vehicle’s owner’s manual (Tex. Transp. Code § 547.615(b)). A “recording device” is defined as any feature installed in a vehicle that performs a specified recording function, including the recording of vehicle location data (Tex. Transp. Code § 547.615(a)(2)). No person other than the owner may retrieve information recorded or transmitted by a recording device except on court order; with the consent of the owner; for the purpose of improving motor vehicle safety, including medical research, provided the owner’s identity is not disclosed; or for the purpose of determining whether emergency medical response is necessary after an accident (Tex. Transp. Code § 547.615(c)).

The Texas Penal Code prohibits a person from knowingly installing an electronic or mechanical tracking device on a motor vehicle owned or leased by another person (see Section I.F.).

14. Other Personal Data

There are no other Texas provisions regarding data beyond those specified above.

E. Sector-Specific Provisions

1. Advertising & Marketing

Anti-spam law: A person may not intentionally transmit a commercial e-mail message that (a) is an unsolicited message and falsifies the e-mail transmission or routing information, (b) contains false, deceptive, or misleading information in the subject line, or (c) uses another person’s Internet domain name without the other person’s consent (Tex. Bus. & Com. Code § 321.051). In addition, a person may not intentionally take an action to transmit an unsolicited commercial e-mail message unless the term “ADV:” appears first in the subject line, or the term “ADV: ADULT ADVERTISEMENT” appears in the subject line in the case of a message containing obscene material or depicting sexual conduct, and the sender provides a functioning return e-mail address to which the recipient may reply requesting removal from the sender’s e-mail list. Senders receiving such a request must remove the recipient’s address within three business days of receipt (Tex. Bus. & Com. Code § 321.052). Finally, a sender may not sell or otherwise provide to another the e-mail address of any person who has requested removal from the sender’s e-mail list, unless otherwise required by law (Tex. Bus. & Com. Code § 321.053).

There are a variety of civil and criminal enforcement provisions related to the anti-spam law (see Section I.G.1., Section I.H., and Section II.C.).

ITEPA: Many types of data collected by businesses in the advertising and marketing sector, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).
MRPA: Under the Medical Records Privacy Act (MRPA), covered entities are restricted from using protected health information for any marketing purposes unless they have written permission or are subject to an exception (Tex. Health & Safety Code § 181.152). For a comprehensive overview of the MRPA, see Section I.D.9.

Do-not-call: Texas law provides for a state no-call list that is updated quarterly (Tex. Bus. & Com. Code § 304.051). Telemarketers are prohibited from making a call to a phone number on the Texas no-call list more than 60 days after the date the number appears on the current list (Tex. Bus. & Com. Code § 304.052).

2. Education

Parents are entitled to access all written records of a school district concerning their child, including attendance records, test scores, grades, disciplinary records, counseling records, and psychological records, among others (Tex. Educ. Code § 26.004). In addition, parents are entitled to full information regarding the school activities of their child (Tex. Educ. Code § 26.008).

3. Electronic Commerce

ITEPA: Many types of data collected by businesses engaged in electronic commerce, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

4. Financial Services

ITEPA: Many types of data collected by businesses in the financial services sector, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Insurance regulations: For information on regulations issued pursuant to the insurance code governing the collection, use, and disclosure of nonpublic personal financial information, see Section I.E.7.

5. Health Care

MRPA: The Medical Records Privacy Act (MRPA) (Tex. Health & Safety Code § 181.001 et seq.) governs the collection, use, and disclosure of protected health information (PHI) and is applicable to health care practitioners in Texas, as well as to other entities collecting or possessing PHI. For a comprehensive overview of MRPA, see Section I.D.9.

In addition, specific collection, access, and disclosure requirements apply under Texas laws specific to hospitals, physicians, and other health care facilities and practitioners. For information on these requirements, see Section I.D.9.

Texas Medical Board: Regulations addressing the maintenance, release, transfer, and disposal of medical records are found in Tex. Admin. Code tit. 22 § 165.1 et seq.

Child care facilities, child placing agencies, and family homes: The director, owner, or operator of a child care facility, child placing agency, or family home must conduct criminal background checks on current and potential employees and other individuals (see Section I.D.5.).
6. HR & Employment

**ITEPA:** Many types of data collected by employers, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

**In-home service companies and residential delivery companies:** Companies that employ persons to enter another person’s residence for specified repair services or to deliver an item to another person’s residence and enter the residence to place, assemble, or install the item must obtain a criminal history record from the Department of Public Safety or a private vendor prior to associating with or hiring an officer, employee, or prospective employee whose duties will include entering into another person’s residence, or must ascertain that such a person holds a valid occupational license from a licensing authority who performed a criminal history background check in connection with the license (Tex. Civ. Prac. & Rem. Code § 145.002). A business that has followed these provisions will not be considered to have acted negligently for the purpose of any suit arising out of the subsequent criminal activity of an officer or employee, provided that the history includes 20 years of felony history and 10 years of misdemeanor history for convictions or deferred adjudications showing that the officer or employee had not been convicted for an offense against family or property or an offense of public indecency (Tex. Civ. Prac. & Rem. Code § 145.003). The presumption generally extends to persons contracting with an in-home service company or residential services company who has complied with the background check requirements (Tex. Civ. Prac. & Rem. Code § 145.004).

**Limits on liability for hiring employees convicted of crime:** No action may be brought against an employer or contractor for negligently hiring an employee based on evidence that the employee has been convicted of a crime. The prohibition does not apply, however, if the employer knew or should have known of the conviction, and the offense was committed while performing duties substantially similar to those for which the employee was hired, or was an offense listed under provisions of the criminal code not eligible for judge-ordered community supervision (see Tex. Code Crim. Proc. § 42A.054) or a sexually violent offense (Tex. Civ. Prac. & Rem. Code § 142.002(a) to Tex. Civ. Prac. & Rem. Code § 142.002(b)). The prohibition also does not apply to a suit concerning a misuse of funds or property if the employee, on the date of hire, had been convicted of a crime including fraud or misuse of property as an element of the offense and it was foreseeable that the position for which the employee was hired would involve a fiduciary responsibility (Tex. Civ. Prac. & Rem. Code § 142.002(c)).

**Expunction of arrest records:** Upon an order of expunction of arrest records (sometimes referred to as expungement, see Tex. Code Crim. Proc. § 55.01 et seq.), a person may deny the occurrence of an arrest and the existence of the expunction order (Tex. Code Crim. Proc. § 55.03).

**Consumer credit reporting agency requirements:** Under Texas law governing the regulation of consumer credit reporting agencies, such agencies may generally provide information to employers for the purpose of making employment decisions (Tex. Bus. & Com. Code § 20.02(a)(3)(B)). Some items may not be furnished, including certain bankruptcy adjudications that are over 10 years old, or suits or judgments, tax liens, arrest or indictment records, or other items that are over seven years old (Tex. Bus. & Com. Code § 20.05(a)). However, such information may be included in a consumer report if it is provided in connection with an employment application for an annual salary of $75,000 or more (Tex. Bus. & Com. Code § 20.05(b)). A consumer reporting agency may not provide any medical information about a consumer in a consumer report for employment purposes without the consent of the consumer (Tex. Bus. & Com. Code § 20.05(d)).
Social security numbers: In general, employers may not intentionally communicate or make public an individual’s social security number (SSN), display an SSN on a card or other device required to access a product, require a person to transmit an SSN over the Internet unless the connection is secure and the number is encrypted, require an SSN for access to a website unless a password or unique personal ID is also required, or print an SSN on material sent by mail unless an exception applies (Tex. Bus. & Com. Code § 501.001(a)). For more information on Texas law governing the privacy and security of SSNs, see Section I.D.10.

Genetic information: Under the Texas Labor Code, genetic information is confidential, and no employer may disclose or be compelled to disclose such information unless specifically authorized by the individual to whom the information relates (Tex. Lab. Code § 21403). The authorization may be made by the individual or his representative. It must be in writing and must include a description of the information to be disclosed, the name of the person to whom the disclosure is made, and the purpose of the disclosure (Tex. Lab. Code § 214032).

Genetic information may be disclosed without authorization under specified circumstances, including where authorized under certain criminal laws, when required by court order, for the purpose of establishing paternity as authorized by law, for medical diagnostic purposes, or to identify a decedent (Tex. Lab. Code § 214031(a)). Additional exceptions apply for disclosures pursuant to a research study that meet specified federal standards, provided that the information does not identify a specific individual (Tex. Lab. Code § 214031(b)). An individual who submits to a genetic test has a right to know the results, and upon written request from an individual, the person performing the test must disclose the results to the individual or the individual’s physician (Tex. Lab. Code § 21404). In general, genetic samples must be destroyed promptly after the purpose for which they were collected is accomplished, unless the sample is retained by court order, the individual authorizes the retention for medical treatment or scientific purposes, the sample was obtained for research cleared by an institutional review board for which retention is a requirement imposed by the board and authorized by the research participant, or the sample was obtained by the Texas Department of Health pursuant to certain newborn screening tests required by law (Tex. Lab. Code § 21405).

References: An employer may disclose information about a current or former employee’s job performance to a prospective employer on the request of the prospective employer or the employee. Certain exceptions apply to licensed nurses engaged in protected conduct (Tex. Lab. Code § 103.003). However, nothing in the law requires an employer to provide an employment reference to or about a current or former employee (Tex. Lab. Code § 103.005).

An employer disclosing information as outlined above is immune from civil liability in connection with the disclosure unless it is proven by clear and convincing evidence that the information disclosed was known by the employer to be false or that the disclosure was made with malice or with reckless disregard for the truth or falsity of the information. This provision applies to managerial employees or other representatives to the same extent that it does to employers (Tex. Lab. Code § 103.004).

7. Insurance

Financial information: Entities covered under the Texas Insurance Code generally are required to comply with federal law provisions on the disclosure of nonpublic personal financial information under the Gramm-Leach-Bliley Act (Tex. Ins. Code § 601002). However, the requirement does not apply to a covered entity acting as an insurance agent, employee, or other authorized representative of another covered entity (Tex. Ins. Code § 601003). Under authority granted to it by law (Tex. Ins. Code § 601051), the Texas Department of Insurance has issued regulations to ensure compliance with the federal Gramm-Leach-Bliley Act standards (Tex. Admin. Code tit. 28 § 22.1through Tex. Admin. Code tit. 28 § 22.27). These regulatory provisions are outlined below.
Primary definitions: “Covered entities” include all individuals or entities receiving authorization from the Texas Department of Insurance, including all types of insurers listed under Tex. Ins. Code § 82.002 (Tex. Admin. Code tit. 28 § 22.2(11)). “Consumers” are generally defined to include individuals seeking to obtain an insurance product or service from a covered entity (Tex. Admin. Code tit. 28 § 22.2(8)), while “customers” are consumers who have a continuing relationship with the covered entity (Tex. Admin. Code tit. 28 § 22.2(12)). The regulations provide information regarding the determination of consumer status (Tex. Admin. Code tit. 28 § 22.4), as well as examples of a continuing relationship with a customer (Tex. Admin. Code tit. 28 § 22.5).

“Nonpublic personal financial information” means personally identifiable information and any list, description, or other grouping of consumers derived using any personally identifiable financial information that is not publicly available, but does not include health information (Tex. Admin. Code tit. 28 § 22.2(21)). The regulations provide guidance on what constitutes a reasonable basis for determining that information is publicly available (Tex. Admin. Code tit. 28 § 22.7). “Personally identifiable financial information” is any information provided by a consumer to a covered entity, any information about a customer from any transaction with the covered entity, or information otherwise obtained by the covered entity, among other specified items (Tex. Admin. Code tit. 28 § 22.2(23)).

Privacy and opt-out notices: Covered entities must provide an initial notice to a customer no later than when a customer relationship is established, or to a consumer before the covered entity discloses nonpublic personal financial information to any nonaffiliated third party (Tex. Admin. Code tit. 28 § 22.8(a)). Initial notice to a consumer is not required if the covered entity does not disclose any information about the consumer to a nonaffiliated third party except as allowed by the regulations or if a notice has been provided by an affiliate entity that meets regulatory requirements (Tex. Admin. Code tit. 28 § 22.8(b)). With respect to existing customers buying new products, a covered entity satisfies the notice requirement if it provides a revised policy notice or if the initial notice previously given was accurate with respect to the new product (Tex. Admin. Code tit. 28 § 22.8(d)). Certain exceptions apply when establishing the customer relationship is not at the customer’s election or when notice would substantially delay the transaction (Tex. Admin. Code tit. 28 § 22.8(e)).

With respect to opt-out notices, covered entities must provide clear and conspicuous notice to consumers that explain the right to opt out. The notice must state that the covered entity discloses or reserves the right to disclose nonpublic financial information about a consumer and that the consumer has the right to opt out of the disclosure, together with a reasonable means by which the consumer may opt out. The regulation provides examples of adequate opt-out notices, and reasonable and unreasonable opt-out means (Tex. Admin. Code tit. 28 § 22.11). The opt-out notice may be provided on the same form as the initial notice form, but if it is provided subsequent to the initial notice, a copy of the initial notice must accompany the opt-out notice (Tex. Admin. Code tit. 28 § 22.11(f) to Tex. Admin. Code tit. 28 § 22.11(g)). Covered entities must comply with a consumer opt-out as soon as practicable after receiving it, and the consumer may exercise the right at any time (Tex. Admin. Code tit. 28 § 22.11(j) to Tex. Admin. Code tit. 28 § 22.11(k)). The opt-out is effective until the consumer revokes it. When a customer relationship terminates, the covered entity must continue to comply with any opt-out direction in effect at the time of termination, but if a customer relationship is reestablished, the prior opt-out notice does not apply to the new relationship (Tex. Admin. Code tit. 28 § 22.11(l) to Tex. Admin. Code tit. 28 § 22.11(m)).

In general, covered entities must provide an annual privacy notice to customers, although they are not required to provide annual notice to former customers (Tex. Admin. Code tit. 28 § 22.9). The regulations specify the contents of privacy notices (Tex. Admin. Code tit. 28 § 22.10), as well as requirements for revising privacy notices (Tex. Admin. Code tit. 28 § 22.12) and delivery of privacy notices (Tex. Admin. Code tit. 28 § 22.13).
Limitations on disclosure: A covered entity may not disclose nonpublic personal financial information about a consumer unless the covered entity has provided an initial notice to the consumer and an opt-out notice as provided above, the covered entity gives the consumer a reasonable opportunity to opt out prior to disclosing the information, and the consumer does not opt out. The regulation provides examples of actions constituting a reasonable opportunity to opt out (Tex. Admin. Code tit. 28 § 22.14(a) to Tex. Admin. Code tit. 28 § 22.14(b)). Covered entities must comply with these requirements with respect to all consumers regardless of whether a consumer has established a customer relationship, and consumers may select the portions of their nonpublic personal financial information for which they choose to exercise the opt-out (Tex. Admin. Code tit. 28 § 22.14(c) to Tex. Admin. Code tit. 28 § 22.14(d)).

Covered entities that receive nonpublic personal financial information under a regulatory exception (see below) may only disclose the information to the affiliates of the financial institution from which it received the information, to its affiliates, or in the ordinary course of business to carry out the activity giving rise to the exception. Similar requirements apply to information received outside an exception and to disclosures to nonaffiliated third parties (Tex. Admin. Code tit. 28 § 22.15). Covered entities also are prohibited from disclosing policy numbers or similar access numbers or codes to any nonaffiliated third party for marketing purposes, unless a statutory exception applies (Tex. Admin. Code tit. 28 § 22.16).

Exceptions to notice or opt-out requirements: The opt-out requirements described above do not apply when a covered entity discloses nonpublic personal financial information to a nonaffiliated third party performing a service for the covered entity if the covered entity provides the initial notice described above and enters into a contractual agreement with the third party prohibiting it from disclosing or using the information other than to carry out the purposes for which the covered entity disclosed the information (Tex. Admin. Code tit. 28 § 22.17(a)). If a covered entity discloses nonpublic personal financial information to a financial institution with which it performs joint marketing, its contractual agreement with the financial institution must prohibit the institution from using or disclosing the information except as necessary to carry out the joint marketing activity or under other regulatory exceptions (Tex. Admin. Code tit. 28 § 22.17(b)). The services a nonaffiliated third party may perform under this exception include joint marketing activities with the covered entity (Tex. Admin. Code tit. 28 § 22.17(c)).

Initial notice and opt-out requirements, including those related to joint marketing activities, do not apply if the covered entity discloses nonpublic personal financial information that is required to effect, administer, or enforce a transaction requested by the consumer in connection with specified purposes (Tex. Admin. Code tit. 28 § 22.18). Other exceptions apply to covered entity disclosures where the consumer has consented to the disclosure, to protect the confidentiality or security of a covered entity’s records or protect against actual or potential fraud, to provide information to insurance rate advisory organizations or other regulators, or specified disclosures authorized under federal law (Tex. Admin. Code tit. 28 § 22.19).

Violations: Violations of the regulations governing the use and disclosure of nonpublic personal financial information by insurers subject the insurer to general disciplinary and enforcement sanctions and penalties under Tex. Ins. Code Chapter 82, Tex. Ins. Code Chapter 83, and Tex. Ins. Code Chapter 84, as well as to specific provisions related to privacy of nonpublic personal financial information at Tex. Ins. Code § 601.102 (Tex. Admin. Code tit. 28 § 22.22; see Section II.C.).

Breach notification: The Texas Department of Insurance (TDI) requires domestic or commercially-domestic insurance companies and health maintenance organizations to contact their assigned financial analysts at TDI following the unauthorized acquisition, release, or use of personal information or sensitive company information (see Commissioner’s Bulletin #B-0022-16). TDI may then request information concerning the incident.
Domestic Privacy Profile: TEXAS

Health information: The Texas Insurance Code sets forth requirements for covered entities with respect to the privacy of individually identifiable health information (Tex. Ins. Code § 602.001 et seq.). However, these provisions do not apply to a covered entity that is required to comply with the standards governing the privacy of such information under the federal Health Insurance Portability and Accountability Act (HIPAA) (Tex. Ins. Code § 602.002; Tex. Admin. Code tit. 28 § 22.61). In addition to the provisions of the Insurance Code, under authority granted to it by law (Tex. Ins. Code § 602.004), the Texas Department of Insurance has issued regulations to ensure compliance with the federal Gramm-Leach-Bliley Act standards (Tex. Admin. Code tit. 28 § 22.51 through Tex. Admin. Code tit. 28 § 22.67). The code and regulatory provisions are outlined below.

Primary definitions: “Covered entities” include all persons holding or required to hold a license, registration, certificate of authority, or other authorization under the Insurance Code, including specified insurance companies, health maintenance organizations, and insurance agents (Tex. Ins. Code § 602.001(1); Tex. Admin. Code tit. 28 § 22.52(4)). “Health information” means any oral or recorded information created by or derived from a health care provider or consumer, other than the individual’s age or gender, relating to the individual’s past or future physical, mental, or behavioral health or condition, or the provision of or payment for health care to the individual (Tex. Ins. Code § 602.001(2)). The regulations reference health information with a similar definition of “protected health information” (Tex. Admin. Code tit. 28 § 22.52(11)). “Nonpublic personal health information” is health information that identifies the subject or for which there is a reasonable basis to believe that the information could be used to identify the subject (Tex. Ins. Code § 602.001(13)). The regulations define “nonpublic personal health information” to have the same meaning as “protected health information” (Tex. Admin. Code tit. 28 § 22.52(8)).

Disclosure authorization requirements: A covered entity must obtain authorization to disclose nonpublic personal health information before making such a disclosure (Tex. Ins. Code § 602.051(a); Tex. Admin. Code tit. 28 § 22.53). The authorization may be in written or electronic form and must

- state the identity of the consumer or customer who is the subject of the information;
- describe the type of information, the parties to whom it will be disclosed, the purpose of the disclosure, how the information will be used, and the procedure for revoking an authorization;
- include the signature of the consumer or customer or a legally authorized representative;
- state the date the authorization is signed; and
- provide notice of the period for which the authorization is valid and the customer’s or consumer’s right to revoke the authorization (Tex. Ins. Code § 602.051(b); Tex. Admin. Code tit. 28 § 22.54).

Authorizations may not be valid for longer than 24 months. The right of revocation is subject to the rights of an individual who acted in reliance on an authorization prior to receiving notice of revocation. A covered entity must maintain the original or a copy of the authorization in the records of the individual (Tex. Ins. Code § 602.051(c) to Tex. Ins. Code § 602.051(e); Tex. Admin. Code tit. 28 § 22.56).

A covered entity may deliver a request for authorization and an authorization form only if the request and form are clear and conspicuous. The authorization form is required to be included in a notice to a consumer or customer only if the covered entity intends to disclose nonpublic personal health information (Tex. Ins. Code § 602.052; Tex. Admin. Code tit. 28 § 22.55).

Exceptions to disclosure requirements: Covered entities may disclose nonpublic personal health information to the extent necessary to perform a variety of insurance or health maintenance organization functions, including fraud investigation, underwriting, risk and case management, or
utilization and peer review activities, among many others (Tex. Ins. Code § 602.052(1) to Tex. Ins. Code § 602.052(3); Tex. Admin. Code tit. 28 § 22.57(1) to Tex. Admin. Code tit. 28 § 22.57(3)).

Third parties: A covered entity that discloses protected health information to a third party to perform any function on its behalf may not make such a disclosure unless the third party agrees not to disclose or use the protected information other than to carry out the purposes for which it is disclosed or in a manner consist with the regulations (Tex. Admin. Code tit. 28 § 22.60).

Penalties: Covered entities who violate the provisions outlined above are subject to penalties, injunction, and other disciplinary action (see Section II.C.).

ITEPA: Many types of data collected by businesses in the insurance sector, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Credit reporting information: Under Texas law governing the regulation of consumer credit reporting agencies, such agencies may generally provide information to employers for the purpose of making insurance underwriting decisions (Tex. Bus. & Com. Code § 20.02(a)(3)(C)). Some items may not be furnished, including certain bankruptcy adjudications that are over 10 years old, or suits or judgments, tax liens, arrest or indictment records, or other items that are over seven years old (Tex. Bus. & Com. Code § 20.05(a)). However, such information may be included in a consumer report if it is provided in connection with the underwriting of life insurance with a face amount of over $150,000 (Tex. Bus. & Com. Code § 20.05(b)). A consumer reporting agency may not provide any medical information about a consumer in a consumer report in connection with an insurance transaction without the consent of the consumer (Tex. Bus. & Com. Code § 20.05(d)).

HMO nondisclosure requirements: Health maintenance organizations are specifically restricted in the disclosure of health information under the Texas Insurance Code (see Section I.D.9.).

8. Retail & Consumer Products

ITEPA: Many types of data collected by businesses in the retail and consumer products sector, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

9. Social Media

ITEPA: Many types of data collected by businesses in the social media sector, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Online impersonation: Persons commit a crime under the Texas Penal Code if they engage in online impersonation. For more information, see Section I.H.

10. Tech & Telecom

ITEPA: Many types of data collected by businesses in the tech and telecommunications sectors, including names in combination with data elements such as social security numbers or account numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).
numbers, are “personal identifying information” or “sensitive personal information” for purposes of the provisions of the Identity Theft Enforcement and Protection Act (ITEPA) regarding identity theft (see Section I.G.2.), data security and disposal (see Section I.C.6. and Section I.C.7.), and data breach notifications (see Section I.C.8.).

Do-not-call list: For information on Texas Code provisions establishing a do-not-call list, see Section I.E.1

11. Other Sectors

There are no Texas provisions regarding privacy and data security related to other business sectors.

F. ELECTRONIC SURVEILLANCE

Eavesdropping law: Under the Texas Penal Code, a person commits an offense when he intentionally intercepts, endeavors to intercept, or procures another person to intercept or endeavor to intercept a wire, oral, or electronic communication. It is also an offense to intentionally disclose or endeavor to disclose a communication intercepted in violation of the law, to use the contents of such an interception, to effect a covert entry for the purposes of such an interception, or to use an electronic or mechanical device to intercept a communication (Tex. Penal Code § 16.02(b)).

Defenses: There are a number of defenses to a prosecution under this law, most importantly in cases where a person intercepts a communication if the person is a party to the conversation or one of the parties to the communication has given prior consent to the interception, unless the communication is intercepted for purposes of committing an unlawful act (making Texas a so-called “one-party consent state”) (Tex. Penal Code § 16.02(c)(4)(a)). Other defenses are available for switchboard operators and employees of telecommunications common carriers under specified circumstances, as well as for persons acting under color of law (Tex. Penal Code § 16.02(c)(1) to Tex. Penal Code § 16.02(c)(3)). A person is acting under color of law if the person has oral or written permission of a magistrate, an immediate, life-threatening situation exists, the person is a member of a law enforcement unit trained to intervene in such situations, and the intercepting ceases immediately on termination of the life-threatening situation (Tex. Penal Code § 16.02(c)(5)). Additional defenses are specified by law (Tex. Penal Code § 16.02(c)(6) to Tex. Penal Code § 16.02(c)(11)).

Manufacturing or selling eavesdropping devices: It is also an offense to intentionally manufacture, assemble, possess, or sell an electronic, mechanical, or other device knowing or having reason to know that the device is designed primarily for nonconsensual interception of wire, electronic, or oral communications and that the device has been or will be used for an unlawful purpose, or to place an advertisement in a newspaper or other publication concerning such a device (Tex. Penal Code § 16.02(d)). However, this prohibition does not apply to certain common carriers or providers acting in the normal course of business; officers, agents, or persons doing business with the United States or Texas; members of the Department of Public Safety specifically trained to install such equipment; and local law enforcement agencies responding to life-threatening situations (Tex. Penal Code § 16.02(e) to Tex. Penal Code § 16.02(e-1)). Finally, it is an offense to obstruct or impede a government attorney or law enforcement officer that the person knows to have authorization to intercept wire, electronic, or oral communications, or to give, or attempt to give, notice of the interception to another (Tex. Penal Code § 16.02(g)).

Criminal code application: The Texas Code of Criminal Procedure also prohibits the use of any communication intercepted in violation of the provisions described above or the disclosure of the
contents of such a communication as evidence in a criminal proceeding (Tex. Code Crim. Proc. § 18.20(2)(a)).

Criminal penalties and remedies: Offenses generally are considered second-degree felonies, but an offense for unlawfully manufacturing an electronic, mechanical, or other device knowing it was designed for nonconsensual interception, as well as an offense for obstruction, is a state jail felony (Tex. Penal Code § 16.02(f)).

 Parties to a communication may sue a person who impermissibly intercepts or attempts to intercept a communication (see Section I.G.4.).

**Tracking devices:** A person commits an offense when the person knowingly installs an electronic or mechanical tracking device on a motor vehicle owned or leased by another person (Tex. Penal Code § 16.06(b)). It is a defense to prosecution if the person obtained the effective consent of the owner or lessee prior to installing the device, assisted someone the person reasonably believed to be a law enforcement officer to install a device as part of a criminal investigation, or was a licensed private investigator who installed the device with written consent from the owner or lessee to install the device and to enter onto private property if such entry was necessary to install the device (Tex. Penal Code § 16.06(d)). In addition, the prohibition does not apply to a peace officer installing a device in the course of a criminal investigation or pursuant to court order (Tex. Penal Code § 16.06(e)).

A violation of the prohibition outlined above is a class A misdemeanor (Tex. Penal Code § 16.06(c)).

**Drone law:** Under the Texas Government Code, it is an offense for a person to use an unmanned aircraft (commonly referred to as a drone) to capture an image of an individual or privately owned real property in Texas with the intent to conduct surveillance on the individual or property captured in the image (Tex. Gov't Code § 423.003(a)). A person may avoid prosecution for this provision, however, if he destroys the image as soon as he has knowledge that it was captured in violation, without disclosing, displaying, or distributing the image to a third party (Tex. Gov't Code § 423.003(a)).

The use of a drone to capture an image is permitted under a variety of circumstances, including for professional or scholarly research, as part of a military operation, for mapping purposes, pursuant to specified law enforcement purposes, or with the consent of the individual or property owner, among others (Tex. Gov't Code § 432.002). Images illegally or incidentally captured in violation of the law may not be used as evidence in criminal or juvenile proceedings and are not subject to disclosure or discovery (Tex. Gov't Code § 423.005).

The unlawful capture of an image by drone, as well as the possession of such an image, is a class C misdemeanor (Tex. Gov't Code § 423.003(b) and Tex. Gov't Code § 423.004(b)). The disclosure, display, distribution, or other use of the image is a class B misdemeanor (Tex. Gov't Code § 423.004(b)). In both cases, each image captured, possessed, displayed, or used constitutes a separate offense (Tex. Gov't Code § 423.004(c)). Defenses are available if the person destroys the image as soon as he has knowledge of the impermissible capture or if the person stops displaying, distributing, or using the image on gaining such knowledge (Tex. Gov't Code § 423.004(d) to Tex. Gov't Code § 423.004(e)).

Separate prohibitions apply to the use of a drone over correctional facilities, critical infrastructure facilities, and detention centers (Tex. Gov't Code § 423.0045), as well as sports venues (Tex. Gov't Code § 423.0046).

An owner or tenant of private property may bring an action against a person who captured an image of the property of the owner or tenant (see Section I.G.4.).
G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Consumer reporting agency requirements: Consumers aggrieved by a violation of the obligations imposed on consumer reporting agencies under Texas law (see Section I.D.4.) have a private right of action or a right to binding arbitration to enforce these provisions (Tex. Bus. & Com. Code § 20.08(a)). The prevailing party in any such proceeding is entitled to attorney fees and costs (Tex. Bus. & Com. Code § 20.08(c)). Consumers may not submit more than one action against a particular agency to arbitration during any 120-day period (Tex. Bus. & Com. Code § 20.08(d)), but if, after a consumer prevails in arbitration, the agency does not remove or strike adverse information in a timely manner, a consumer may bring an action within the 120-day period (Tex. Bus. & Com. Code § 20.08(f)).

A consumer reporting agency in willful violation is liable to the consumer for the greater of three times actual damages or $1,000, reasonable attorney fees, and costs (Tex. Bus. & Com. Code § 20.09(a)). A negligent violation subjects the agency to liability of the amount of actual damages or $500, whichever is higher, but an agency will not be considered to have been negligent if it completes, and sends notification of the results of, a reinvestigation within 30 days after receiving notice of the dispute (Tex. Bus. & Com. Code § 20.09(b)). Finally, an agency that does not correct a report before the 10th day after the date on which judgment is entered against it is liable for $1,000 per day until the report is corrected (Tex. Bus. & Com. Code § 20.09(c)).

Anti-spam law: A person injured by a violation of the Texas anti-spam law (see Section I.E.1.) may bring an action to recover actual damages or the amount prescribed by law (see below) (Tex. Bus. & Com. Code § 321.104(a)). A prevailing party in such an action is entitled to recover reasonable attorney fees and costs (Tex. Bus. & Com. Code § 321.104(b)). No action brought under this law may be certified as a class action (Tex. Bus. & Com. Code § 321.109).

In lieu of the actual damages outlined above, a person injured by the transmission of an unsolicited or commercial e-mail may recover an amount equal to the lesser of $10 per message or $25,000 for each day the unlawful message is received. However, these damages are not available against e-mail service providers (Tex. Bus. & Com. Code § 321.105). An e-mail service provider injured as described above may recover the same amounts in lieu of actual damages (Tex. Bus. & Com. Code § 321.106).

Any person bringing an action for violation of the anti-spam law must notify the Attorney General by mailing a copy of the petition by registered mail no later than 30 days after the date it was filed and at least 10 days prior to the date of the hearing. Persons failing to provide this notice are subject to a fine of $200 for each violation (Tex. Bus. & Com. Code § 321.107). The Attorney General is entitled to intervene in a civil action (Tex. Bus. & Com. Code § 321.108).

At the request of any party, the court may conduct the proceedings in a manner that protects the secrecy and security of the computer, computer network, data, programs, and software to prevent a possible recurrence of the act by another person, as well as the trade secrets of any party (Tex. Bus. & Com. Code § 321.110). Certain persons are immune from liability as described above, including persons transmitting a commercial e-mail message as a result of error or accident (Tex. Bus. & Com. Code § 321.111), telecommunications providers and e-mail service providers under specified circumstances (Tex. Bus. & Com. Code § 321.112), and senders who contract with an e-mail service provider and have no reason to believe that the e-mail service provider will transmit messages in violation of the anti-spam law (Tex. Bus. & Com. Code § 321.113).
2. Identity Theft

**ITEPA:** Under the Identity Theft Enforcement and Protection Act (ITEPA), no person may obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with the intent to obtain anything of value in the person's name (Tex. Bus. & Com. Code § 521051(a)). “Personal identifying information” is defined as information that alone, or in conjunction with other information, identifies an individual, including:

- a name, social security number, date of birth, or government-issued ID number;
- the individual's mother's maiden name;
- unique biometric data, including fingerprints, voice prints, and retina or iris images;
- a unique electronic ID number, address, or routing code; or
- a telecommunication access device (Tex. Bus. & Com. Code § 521002(a)(3)).

A defense to any action brought pursuant to this prohibition is available to a person whose act is covered by the federal Fair Credit Reporting Act and is in compliance with that Act and its regulations (Tex. Bus. & Com. Code § 521051(b)). In addition, the prohibitions do not apply to financial institutions as defined under the federal Gramm-Leach-Bliley Act, or to covered entities under the Texas Insurance Code (Tex. Bus. & Com. Code § 521051(b)).

Persons who violate the requirements outlined above are subject to civil penalties and injunctive action (see Section II.C.).

**Identity theft by electronic device:** In addition to the provisions outlined above, a person who uses a scanning device or re-encoder to access, read, scan, store, or transfer information encoded in the magnetic strip of a payment card without the consent of the authorized user and with intent to harm or defraud is guilty of a class B misdemeanor. Such a person is guilty of a state felony if the information at issue was protected health information as defined under the HIPAA Privacy Rule (Tex. Bus. & Com. Code § 522.002).

**Victim’s rights:** No person who has been notified by an individual that the individual has been the victim of identity theft may deny or restrict credit to the individual solely because the individual was a victim. Persons licensed under the Texas Finance Code who violate this prohibition are subject to revocation or suspension of their license (Tex. Bus. & Com. Code § 523.001). In addition, financial institutions must submit specified information to an electronic notification system if they receive a completed request from an identity theft victim (Tex. Bus. & Com. Code § 523.052).

**Warning signs in bars and restaurants:** Restaurants or bars that accept credit or debit cards in the ordinary course of business must post a conspicuous sign that warns customers about the penalties for identity theft. Failure to do so may result in a $25 fine (Tex. Bus. & Com. Code § 502.001).

**Penal Code provisions:** A separate provision of the Texas Penal Code makes it a felony to obtain, possess, transfer, or use identifying information of another person without their consent. Similar provisions apply to information concerning a deceased natural person that is used or obtained without legal consent, as well as to information of a child under age 18 (Tex. Penal Code § 32.51(b)). For more information, see Section I.H.

3. Invasion of Privacy

In general, invasion of privacy actions are governed under common law in Texas. However, a number of law provisions involve prohibited activities that would commonly be understood to involve an invasion of privacy. A discussion of most of these provisions, including eavesdropping laws and prohibitions on the installation of tracking devices, is set forth at Section I.F. For information on online impersonation, see Section I.H.
4. Computer Hacking

Texas permits a private cause of action for anyone who was injured or whose property was injured by a violation of the state’s criminal computer hacking provisions (Tex. Penal Code § 33.02), provided the violation was committed knowingly or intentionally (Tex. Civ. Prac. & Rem. Code § 143.001). A person must file the civil action “before the earlier of the fifth anniversary of the date of the last act in the course of the conduct constituting a violation [of the criminal statute], or the second anniversary of the date the claimant first discovered or had reasonable opportunity to discover the violation.” Tex. Civ. Prac. & Rem. Code § 143.001(b).

5. Other Causes of Action

Disclosure of HIV/AIDS information: A person may bring an action to restrain a violation of provisions prohibiting the disclosure of information regarding an HIV/AIDS test (see Section I.D.9.). A person negligently violating these requirements is liable for actual damages, a civil penalty of not more than $5,000, and court costs and reasonable attorney fees. A person willfully violating these requirements is liable for actual damages, a civil penalty of not less than $5,000 nor more than $10,000, and court costs and reasonable attorney fees. Each release or disclosure constitutes a separate offense (Tex. Health & Safety Code § 81.104).

Mental health professional disclosure requirements: A person aggrieved by the improper disclosure or the improper failure to disclose confidential mental health information (see Section I.D.9.) may petition the court for appropriate relief, including an injunction. The aggrieved person also has a civil cause of action for damages, although the amount of damages is not specified (Tex. Health & Safety Code § 611.005).

Hospital disclosure requirements: Under provisions of the Health and Safety Code governing hospitals’ responsibilities with respect to the unauthorized disclosure of confidential patient information (see Section I.D.9.), patients aggrieved by a violation of these requirements may bring an action for injunctive relief and damages resulting from the release. The law does not specify any limits on damages that may be sought (Tex. Health & Safety Code § 241.156).

Physician disclosure requirements: Under provisions of the Occupations Code governing physicians’ responsibilities with respect to the unauthorized disclosure of confidential patient information (see Section I.D.9.), patients aggrieved by a violation of these requirements may bring an action for injunctive relief and also may prove a cause of action for civil damages (Tex. Occ. Code § 159.009).

Emergency medical services providers disclosure requirements: Under provisions of the Occupations Code governing responsibilities of emergency medical services providers with respect to the unauthorized disclosure of confidential patient information (see Section I.D.9.), patients aggrieved by a violation of these requirements may bring an action for injunctive relief and also may bring an action for damages (Tex. Health & Safety Code § 773.094).

Impermissible interception of communications: A party to a communication may sue a person who intercepts, attempts to intercept, or employs another person to intercept or attempt to intercept a communication; uses or divulges information that the person knew or reasonably should have known was obtained by interception; or, as a landlord, building operator, or communication common carrier, aids or knowingly permits interception or attempted interception of a communication. No cause of action may be brought, however, with respect to an interception of a communication authorized under federal law (Tex. Civ. Prac. & Rem. Code § 123.002). For purposes of this cause of action, a “communication” is speech uttered by a person or information including speech that is transmitted in whole or in part with the aid of a wire or cable (Tex. Civ. Prac. & Rem. Code § 123.001(1)), while an “interception” is generally defined as the aural acquisition of the contents of a communication through an electronic, mechanical, or other device without the
consent of a party to the communication, with exceptions provided for the ordinary use of telephone or telegraph instruments; hearing aids; radio, television, or other wireless receivers; or cable systems relaying public wireless broadcasts (Tex. Civ. Prac. & Rem. Code § 123.001(2)).

[Note: The Civil Practice and Remedies Code does not specifically mention provisions of the Penal Code and the Criminal Procedure Code prohibiting the interception of wire, electronic, or oral communications under specified circumstances, but presumably, to the extent that a violation of those provisions constitutes an interception of a “communication” as defined above, a cause of action for such a violation would be available. For information on the eavesdropping provisions, see Section I.F.]

An exception is provided for switchboard operators or employees of a communication common carrier whose facilities are used in the transmission of wire communication in the normal course of employment if engaged in an activity that is necessary to service or for the protection of the carrier’s rights or property. A carrier may not use service observation or random monitoring except for mechanical or service quality control checks (Tex. Civ. Prac. & Rem. Code § 123.003).

Persons establishing a cause of action as described above are entitled to injunctive relief, statutory damages of $10,000 for each occurrence, all actual damages in excess of $10,000, punitive damages as determined by the court, and reasonable attorney fees and costs (Tex. Civ. Prac. & Rem. Code § 123.004).

**Drone law:** An owner or tenant of private property located in Texas may bring an action against a person who captures an image of the property in violation of the state’s drone law (see Section I.F.). The action may seek injunctive relief; a civil penalty of (a) $5,000 for all images captured in a single episode, or (b) $10,000 for the disclosure, display, distribution, or other use of images captured in a single episode; or actual damages if the person who captured the image discloses, displays, or distributes the image with malice (Tex. Gov’t Code § 423.006(a)). For purposes of these penalties, all owners of a parcel of real property are considered a single owner, and all tenants of a parcel of real property are considered to be a single tenant (Tex. Gov’t Code § 423.006(b)).

In addition to penalties, a court must award court costs and reasonable attorney fees to the prevailing parties (Tex. Gov’t Code § 423.006(d)). An action must be brought within two years of the date the image was captured or initially disclosed, displayed, distributed, or otherwise used (Tex. Gov’t Code § 423.006(f)).

**Zombies and botnets:** Texas authorizes a private cause of action for Internet service providers and others who have “incurred a loss or disruption” to their business against those who “knowingly cause or offer to cause a computer to become a zombie or part of a botnet.” Tex. Bus. & Com. Code § 324.055. A person bringing the action may obtain both injunctive relief and damages.

### H. CRIMINAL LIABILITY

**Identity theft by electronic device:** A person who uses a scanning device or re-encoder to access, read, scan, store, or transfer information encoded in the magnetic strip of a payment card without the consent of the authorized user and with intent to harm or defraud is guilty of a class B misdemeanor. Such a person is guilty of a state felony if the information at issue was protected health information as defined under the HIPAA Privacy Rule (Tex. Bus. & Com. Code § 522.002).

**Background checks for child care service employees:** With respect to requirements that specified child care facilities, child placing agencies, or family homes submit the names of current and prospective employees for criminal background and history checks (see Section I.D.5.), a director, owner, or operator of such a facility commits a class B misdemeanor when he fails to submit the required information about a person and allows the person to work at the facility, or when, after
receiving notice that the background check precludes the person’s employment, knowingly employs the person (Tex. Hum. Res. Code § 42.056(i) to Tex. Hum. Res. Code § 42.056(k)).

**Penal Code provision on use of identifying information:** The Texas Penal Code makes it a felony to obtain, possess, transfer, or use identifying information of another person without his consent. Similar provisions apply to information concerning a deceased natural person that is used or obtained without legal consent, as well as to information of a child under age 18 (Tex. Penal Code § 32.51(b)). The law defines “identifying information” to include items such as date of birth, biometric data, unique electronic identification or financial account numbers, and social security numbers, among others (Tex. Penal Code § 32.51(a)). Offenses range from a state felony to a first-degree felony depending on the number of items obtained, possessed, transferred, or used (Tex. Penal Code § 32.51(c)). The category is enhanced one level for offenses against elderly individuals or offenses involving the use of such information in connection with a violation of requirement regarding the sex offender registration program (Tex. Penal Code § 32.51(c-1)). Defendants may be subject to restitution requirements, including lost income and other expenses, other than attorney fees, if the court so decides (Tex. Penal Code § 32.51(d)).

**Online impersonation:** A person commits an offense if—without consent and with the intent to harm, defraud, threaten, or intimidate—he uses the name or persona of another person to create a webpage on a commercial social networking site or other Internet website, or to post or send messages on or through a commercial social networking site or other Internet website other than on or through an electronic mail program or message board program (Tex. Penal Code § 33.07(a)). In addition, an offense is committed if a person sends an e-mail, instant message, text message, or similar communication referencing a name, domain address, phone number, or other item of identifying information belonging to another person without his consent, with the intent to cause the recipient to believe that the other person authorized or transmitted the communication and with intent to harm or defraud (Tex. Penal Code § 33.07(b)). The former offense is a third-degree felony, and the latter offense is a Class A misdemeanor, or a third-degree felony if the communication is sent to solicit a response by emergency personnel (Tex. Penal Code § 33.07(c)).

**Anti-spam law:** A person who intentionally takes an action to transmit an e-mail message that contains obscene material or depicts sexual conduct without providing the appropriate subject line banners required under the state’s anti-spam law (see Section I.E.1) is guilty of a class B misdemeanor (Tex. Bus. & Com. Code § 321001).

**HMO disclosure requirements:** Any person, including an agent or officer of a health maintenance organization (HMO), who violates the restrictions on disclosing health information by HMO personnel (see Section I.D.9.) is guilty of a class B misdemeanor (Tex. Ins. Code § 843.464).

**HIV/AIDS:** A violation of the nondisclosure requirement with respect to information regarding HIV/AIDS tests (see Section I.D.9.) is a class A misdemeanor (Tex. Health & Safety Code § 81.103(j)).

**Divulgement of electronic communications:** A person who provides an electronic communications service to the public commits an offense if the person knowingly divulges the contents of a communication to another who is not the intended recipient of the communication. For more information, see Section I.D.7.

**Eavesdropping law:** Offenses in violation of the Texas eavesdropping law (see Section I.F.) generally are considered second-degree felonies, but an offense for unlawfully manufacturing an electronic, mechanical, or other device knowing it was designed for nonconsensual interception, as well as an offense for obstruction, is a state jail felony (Tex. Penal Code § 16.02(f)). A violation of the prohibition against installing a tracking device in a motor vehicle without consent (see Section I.F.) is a class A misdemeanor (Tex. Penal Code § 16.06(c)).
Drone law: Violations of the state’s law prohibiting the capture of images by a drone except under specified circumstances (see Section I.F.) constitute a class B or class C misdemeanor, depending on the circumstances of the violation (see Section I.F.).

Computer hacking: A person who “knowingly accesses a computer, computer network, or computer system without the effective consent of the owner” violates the state’s Breach of Computer Security Act (Tex. Penal Code § 33.02). The offense can be a misdemeanor or a felony, depending on the circumstances. The statute specifies two defenses:

- when the person acted with the intent to facilitate a lawful search or seizure for a legitimate law enforcement purpose (Tex. Penal Code § 33.02(e)); or
- when the person’s conduct was taken pursuant to a contract with the owner of the computer (Tex. Penal Code § 33.02(e)).

Revenge porn: Tex. Penal Code § 21.15 prohibits a person from photographing, videotaping, broadcasting, or transmitting “a visual image of an intimate area of another person” without that person’s consent and with the intent to invade the privacy of that person. An offense constitutes a state jail felony. The presence of a sign indicating that the person is being photographed or that a visual image of the person is being recorded, broadcast, or transmitted is not sufficient to establish consent.

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. ATTORNEY GENERAL

The Attorney General is responsible for the enforcement of a variety of Texas privacy law provisions, including the Identity Theft Enforcement and Protection Act (ITEPA) and the Medical Records Privacy Act (MRPA) (see Section I.C.6., Section I.C.7., Section I.C.8., and Section I.D.9.). Other laws enforced by the Attorney General include laws governing the protection of driver’s license and social security numbers (see Section I.D.6. and Section I.D.10.) and the protection of biometric identifiers (see Section I.D.1), among others. For specific information on the enforcement powers of the Attorney General, see Section II.C.

B. OTHER REGULATORS

The Texas Department of Insurance is responsible for enforcing provisions related to the privacy and security of personal information, including certain financial and health information (see Section I.E.7.).

Under the Medical Records Privacy Act (MRPA; see Section I.D.9.), the Texas Commission of Health and Human Services is charged with coordinating with the Attorney General, the Texas Department of Insurance, and the Texas Health Service Authority to request the U.S. Department of Health and Human Services to conduct an audit of covered entities to determine their compliance with HIPAA privacy requirements and to monitor and review the results. If the Commission has evidence that a covered entity committed violations of Texas law that are egregious and constitute a pattern or practice, it may require the covered entity to submit a risk analysis or request a licensing agent to conduct an audit of the covered entity (Tex. Health & Safety Code § 181.206).

The Public Utility Commission of Texas is responsible for the maintenance and enforcement of the state’s do-not-call provisions (see Section I.E.1).
C. Sanctions & Fines

ITEPA: The Attorney General is authorized under the Identity Theft Enforcement and Protection Act (ITEPA) to bring an action to enforce a civil penalty for any violation of the ITEPA, including identity theft (see Section I.G.2.), a failure of a business's duty to protect or, where applicable, destroy sensitive personal information (see Section I.C.6. and Section I.C.7.), and a failure by a person conducting business in Texas to properly notify affected persons in the event of a data breach (see Section I.C.8.). In each instance, the person in violation is liable to the state for a civil penalty of at least $2,000 but not more than $50,000 for each violation (Tex. Bus. & Com. Code § 521.151(a)). In addition, with respect to a failure to comply with data breach notification requirements, a person is liable for a civil penalty of not more than $100 for each individual to whom notification is due for each day that the person fails to take reasonable action to comply, up to a maximum of $250,000 for a single breach (Tex. Bus. & Com. Code § 521.151(a-1)). The Attorney General may bring an action for a temporary restraining order or a temporary or permanent injunction (Tex. Bus. & Com. Code § 521.151(c)). The court may grant other equitable relief as appropriate, and the Attorney General is entitled to recover reasonable expenses, including attorney fees and costs (Tex. Bus. & Com. Code § 521.151(e) to Tex. Bus. & Com. Code § 521.151(g)).

MRPA: The Attorney General may institute an action for injunctive relief to restrain a violation of the Medical Records Privacy Act (MRPA; see Section I.D.9.) (Tex. Health & Safety Code § 181.201(a)). In addition, the Attorney General may institute an action for civil penalties. The penalty may not exceed $5,000 for each negligent violation that occurs in one year, regardless of how long the violation continues; $25,000 for each knowing or intentional violation that occurs in one year, regardless of how long the violation continues; and $250,000 for any knowing or intentional use of protected health information (PHI) for financial gain (Tex. Health & Safety Code § 181.201(b)).

With respect to violations of MRPA’s prohibition on the use or disclosure of PHI without prior notice and authorization, the total amount of penalty assessed against a covered entity may not exceed $250,000 annually if the court finds that the disclosure was made only to another covered entity in accordance with an exception for disclosures for treatment or payment purposes and that:

- the PHI was encrypted or transmitted using encryption technology designed to protect against disclosure;
- the recipient did not use or release the PHI; or
- at the time of the disclosure, the covered entity had developed, implemented, and maintained security policies (Tex. Health & Safety Code § 181.201(b-1)).

The court may assess a penalty not to exceed $1.5 million if it finds that violations have occurred as a pattern or practice (Tex. Health & Safety Code § 181.201(c)). The law describes the factors a court must take into account in determining the penalty, including the seriousness of the violation, the entity’s compliance history, the amount necessary to deter future violations, and the entity’s remedial efforts, among others (Tex. Health & Safety Code § 181.201(d)).

Covered entities in violation of MRPA are subject to additional disciplinary action (Tex. Health & Safety Code § 181.202) and exclusion from state programs (Tex. Health & Safety Code § 181.203).

Biometric identifier law: Persons violating the restrictions on collection, use, and disclosure of biometric identifier information (see Section I.D.1.) are subject to a civil penalty of no more than $25,000 per violation. The Attorney General may bring an action to recover the penalty (Tex. Bus. & Com. Code § 503.001(d)).

Business records destruction requirements: A business that fails to meet requirements regarding the proper destruction of business records (see Section I.C.7.) is liable for a civil penalty not to exceed $500 for each business record. The Attorney General may bring an action to collect the penalty and to seek injunctive relief, other remedies, and costs and attorney fees (Tex. Bus. & Com. Code § 503.001(d)).
Credit or debit card information on receipts: Any business that violates provisions prohibiting the display of credit or debit card number or expiration information on a receipt (see Section I.D.3.) is subject to a civil penalty of not more than $500 for each month in which a violation occurs. The Attorney General may bring the action to recover the penalty and for a restraining order or injunction. However, no class action may be certified with respect to a violation (Tex. Bus. & Com. Code § 502.002(d) to Tex. Bus. & Com. Code § 502.002(f)).

Consumer reporting agency requirements: With respect to violations of the obligations imposed on consumer reporting agencies under Texas law (see Section I.D.4.), the Attorney General may file suit for injunctive relief or a civil penalty not exceeding $2,000 for each violation. Upon prevailing in such an action, the Attorney General may also recover reasonable expenses, costs, and attorney fees. For purposes of these penalties, each day of violation constitutes a separate violation (Tex. Bus. & Com. Code § 20.11). In addition, a violation by a consumer reporting agency is considered a false, misleading, or deceptive practice under the Deceptive Trade Practices-Consumer Protection Act (Tex. Bus. & Com. Code § 20.12).

Provisions protecting driver's license and social security numbers: A merchant violating provisions regarding the use of a driver's license number or social security number pursuant to returns of merchandise (see Section I.D.6. and Section I.D.10.) is subject to a civil penalty of $500 for each violation. The Attorney General may bring an action to recover the penalty or to restrain or enjoin violations (Tex. Bus. & Com. Code § 501.102(a) and (b)).

A person violating provisions prohibiting printing a driver's license number on a receipt (see Section I.D.6.) is subject to a civil penalty of $500 for each calendar month in which a violation occurs, but the penalty may not be imposed for more than one violation occurring in a month. The Attorney General may bring an action to recover the penalty or to restrain or enjoin violations (Tex. Bus. & Com. Code § 501.102(a-1) and Tex. Bus. & Com. Code § 501.102(b)).

HMO disclosure requirements: Health maintenance organizations (HMOs) that violate the restrictions on disclosing health information (see Section I.D.9.) are subject to disciplinary action by the Insurance Commission, including cease-and-desist orders, suspension or revocation of authority, administrative penalties, and sanctions. (Tex. Ins. Code § 843.461). The Commissioner may also bring an action for injunctive relief (Tex. Ins. Code § 843.463).

Social security numbers: Provisions of the Business and Commerce Code prohibiting the printing of a social security number (SSN) on documents required to access a product or service (see Section I.D.10.) provide that a violator is liable to the state for a civil penalty of not more than $500 for each violation. The Attorney General may bring an action to enforce the penalty or to enjoin or restrain violations (Tex. Bus. & Com. Code § 501.002(b) to Tex. Bus. & Com. Code § 501.002(c)).

In addition, a person who fails to adopt a privacy policy with respect to a requirement regarding the disclosure of an SSN (see Section I.D.10.) is liable for a civil penalty of not more than $500 for each month of violation. The Attorney General may bring an action to recover the penalty or to enjoin or restrain the violation (Tex. Bus. & Com. Code § 501053).
**Anti-spam law:** Persons in violation of the Texas anti-spam law (see Section I.E.1) are liable for civil penalties in an amount not to exceed the lesser of $10 for each unlawful message or unlawful action, or $25,000 for each day an unlawful message is received or each day an unlawful action is taken. The Attorney General may bring an action to recover the penalty and for injunctive relief. The Attorney General is entitled to recover reasonable expenses, including court costs and attorney fees (Tex. Bus. & Com. Code § 321.02). In addition, a violation of the anti-spam law is a false, misleading, or deceptive act under the Deceptive Trade Practices-Consumer Protection Act (Tex. Bus. & Com. Code § 321.03).

**Insurance Code and regulation provisions on disclosure of nonpublic personal financial information:** The Department of Insurance is responsible for enforcing the provisions of the federal Gramm-Leach-Bliley Act concerning the disclosure of nonpublic personal financial information, as implemented through its regulations (Tex. Ins. Code § 601.101; see Section I.E.7.) A covered entity who violates these provisions is subject to an action for injunctive relief brought by the Attorney General (Tex. Ins. Code § 601.102(a)). In addition, the Attorney General may bring a civil action to recover penalties, which may not be less than $3,000 per violation. If the court finds that violations have occurred as a pattern or practice, it may assess a civil penalty of not more than $250,000 (Tex. Ins. Code § 601.102(b) to Tex. Ins. Code § 601.102(c)). If the Attorney General substantially prevails in an action for injunctive relief or civil penalties, it may recover reasonable costs and attorney fees (Tex. Ins. Code § 601.102(d)).

**Insurance Code and regulation provisions on disclosure of nonpublic personal health information:** A covered entity who violates provisions of the Insurance Code regarding the disclosure of nonpublic personal health information (see Section I.E.7.) is subject to an action for injunctive relief brought by the Attorney General (Tex. Ins. Code § 602.102). In addition, the Attorney General may bring a civil action to recover penalties, which may not be less than $3,000 per violation. If the court finds that violations have occurred as a pattern or practice, it may assess a civil penalty of not more than $250,000 (Tex. Ins. Code § 602.103). Covered entities also are subject to investigation, disciplinary proceedings, and probation or suspension of the entity’s license, as well as a revocation of a license if the investigation reveals a pattern or practice of violations (Tex. Ins. Code § 602.104). Covered entities found to have engaged in a pattern or practice of violations also will be excluded from participating in a state-funding health care program (Tex. Ins. Code § 602.105). Regulations issued by the Department of Insurance reiterate these penalty provisions (Tex. Admin. Code tit. 28 § 22.64).

**D. REPRESENTATIVE ENFORCEMENT ACTIONS**

In May 2016, Texas Attorney General Ken Paxton announced a $175,000 settlement with PayPal Inc. for alleged violations of the Texas Deceptive Trade Practices-Consumer Protection Act, Tex. Bus. & Com. Code § 17.41 et seq. According to the statement, Venmo, a digital Internet wallet application owned by PayPal, “used consumers' phone contacts without clearly disclosing how the contact would be used, did not clearly disclose how consumers’ transactions and interactions with other users would be shared, and misrepresented that communications from Venmo were actually from particular Venmo users.”

Under the terms of the assurance of voluntary compliance, PayPal agreed to pay $175,000, promised to increase the amount of disclosures with Venmo app consumers regarding privacy and security, and vowed to use better safeguards “to ensure consumers understand who will be able to view their transaction information.”
E. State Resources

The Attorney General provides general information to businesses and consumers on protecting consumer personal data, state and federal health privacy laws, telemarketing and junk mail, and strategies to avoid spam or unsolicited e-mails. The latest annual report as required under the Medical Records Privacy Act (MRPA; see Section I.D.9.) was issued in December 2013.

The Texas Department of Insurance provides a resource page dedicated to explaining the implementation of privacy provisions relating to the disclosure of nonpublic personal financial information under the federal Gramm-Leach-Bliley Act and state law (see Section I.E.7.).

The Texas Public Utilities Commission maintains a website outlining the procedures for and providing access to the state’s do-not-call lists.

III. Risk Environment

While the Attorney General is primarily responsible for enforcing most of Texas’ privacy laws, there are few publicly available records showing how often the Attorney General has brought enforcement actions against companies that have had data breaches. Because of this, many view the Attorney General as being not particularly aggressive in enforcing these laws. However, it should be noted that the Identity Theft Enforcement and Protection Act (ITEPA) (Tex. Bus. & Com. Code § 521001et seq.) does not require businesses to provide notice to the Attorney General in the wake of a breach. Consequently, the Texas Attorney General does not see the same volume of reported data breaches as do attorneys general in states that require such notification.

When privacy incidents involve protected health information (PHI), the likelihood of enforcement increases. Not only does the Texas Attorney General have the authority to enforce the provisions of the Medical Records Privacy Act (Tex. Health & Safety Code § 181.001et seq.), but the Texas Medical Board may conduct investigations and open administrative proceedings against medical professionals who have had incidents involving PHI when such cases are reported to the Board. See generally, Tex. Admin. Code tit. 22 § 165.1et seq.

Moreover, the vast majority of the investigations and enforcement actions involving PHI in Texas are brought by the United States’ Department of Health and Human Services, Office of Civil Rights (OCR) pursuant to the Health Insurance Portability and Accountability Act (HIPAA). The OCR’s level of enforcement of these laws in Texas is comparable to its enforcement in other jurisdictions.

Texas has a reputation as a business-friendly environment with a pro-business legislature and supreme court. Generally speaking, Texas is not known as a hotbed for privacy-related class actions, and there are no notable watershed privacy cases that have come out of the Texas courts.

IV. Emerging Issues and Outlook

A. Recent Legislation

1. Cybersecurity Act

On June 12, 2017, Governor Abbot signed into law H.B. 8, known as the Texas Cybersecurity Act, which sets forth cybersecurity requirements for state agencies to follow. In particular, the law:

- requires an assessment of an agency’s cybersecurity practices when determining whether to sunset an agency, its advisory committees, or any of its functions (Tex. Gov’t Code § 325.011(14));
• permits an exception to the open meeting requirement when governmental bodies deliberate security assessments or deployments (Tex. Gov’t Code § 551.089);
• requires state agencies to redact certain confidential information from contracts posted online (Tex. Gov’t Code § 552.139(d));
• establishes an “information sharing and analysis center” to provide a forum for state agencies to share information regarding cybersecurity threats, best practices, and remediation strategies (Tex. Gov’t Code § 2054.0594);
• requires the establishment of mandatory guidelines regarding continuing education requirements for cybersecurity training to be completed by all information resources employees (Tex. Gov’t Code § 2054.076);
• requires the preparation of a vulnerability report (Tex. Gov’t Code § 2054.077);
• amends the security breach notification provisions to require notice to certain officials within 48 hours of a breach (Tex. Gov’t Code § 2054.1125(b));
• mandates the establishment of a cybersecurity council, drawing from both the public and private sectors, to collaborate on “matters of cybersecurity concerning this state” (Tex. Gov’t Code § 2054.512);
• requires the inclusion of an acknowledgment of risks in the agency’s information security plan (Tex. Gov’t Code § 2054.133);
• requires the preparation of an information security assessment and report (Tex. Gov’t Code § 2054.515), as well as a data security plan for online and mobile applications (Tex. Gov’t Code § 2054.516);
• requires the development of a plan to remediate and mitigate any information security issues (Tex. Gov’t Code § 2054.575);
• expands the scope of the provisions related to confidential network security information to include any governmental entity (Tex. Gov’t Code § 2059.055(b));
• directs the secretary of state to conduct a study and prepare a report on cyber-attacks on the election infrastructure (Tex. Elec. Code § 276.011);
• mandates the establishment of Select Committees on Cybersecurity for both the House and Senate; and
• directs the Department of Information Resources, in consultation with the Texas State Library and Archives Commission, to conduct a study and prepare a report on state agency digital data storage and records management practices.


2. Direct Marketing to Students

H.B. 2087 amended the Education Code to prohibit the operator of a website used, designed, and marketed for a school purpose from engaging in targeted advertising if the target of such advertising is based on any information that the operator has acquired through use of the operator’s website, or from creating a profile about a student for non-school purposes, with stated exceptions. The Act also requires operators to implement reasonable security practices and delete personal information belonging to students within 60 days of a request or as specified in a contract or in terms of service. The Act took effect on Sept. 1, 2017.

B. PROPOSED LEGISLATION (85(R) - 2017 SESSION)

1. Breach Liability and Notification

HB 2333 (SB 1409), introduced Feb. 23, 2017, would amend the Business and Commerce Code to impose breach notification requirements upon businesses that accept and retain credit and debit card information for purchases. Businesses would be required to provide notice of a breach of such
information to the attorney general within 24 hours of learning of the breach and to financial institutions issuing affected cards as soon as practicable. The bill would also subject a business that fails to secure its computer system leading to a breach to a civil penalty of $50 per affected card.

Along similar lines, HB 2001, introduced Feb. 16, 2017, would amend the Business and Commerce Code to prohibit consumer reporting agencies from charging a fee in exchange for the placement or removal or a security freeze following a breach of a consumer’s personal information.

2. Motor Vehicle Records

SB 1013, introduced Feb. 22, 2017, would amend the Transportation Code to impose further restrictions on individuals or entities who request personal information from an agency in connection with motor vehicles. The bill would require any requestor to maintain records specifying the use of the personal information and, if the requestor rediscloses the information, the identity of any person or entity receiving the information and the permitted use for which it was obtained. The requestor would also be required to provide copies of those records to the agency that provided the information upon request from the agency. Furthermore, the requestor would be required to take measures to minimize access to data following a breach and to notify the agency that originally provided the information of any resale or redisclosure of the information within 30 days of the sale or disclosure.

C. Other Issues

1. Equifax Breach

Following the Equifax security breach, Texas Attorney General Ken Paxton released two consumer alerts with recommendations for Texas residents who may have been affected. The Attorney General’s office also maintains an informational page on fighting identity theft and a resource for filing complaints online.

2. Child Online Privacy Protection

In October 2016, Texas Attorney General Ken Paxton reached a settlement with the application developer Juxta Labs, Inc. over the company’s information collection practices. According to the Attorney General, Juxta Labs misled consumers in relation to its development and operation of a messaging application that collected personal information from children, in violation of the Texas Deceptive Trade Practices-Consumer Protection Act. Among the provisions in the settlement is an assurance that Juxta Labs will not collect personal information from children without satisfying the requirements of the Children’s Online Privacy Protection Act, 15 U.S.C. § 6501 et seq.
Minimize the risks.

Global news and timely insight on emerging issues.

Access a single-source solution that harnesses the expertise of our editorial team and dozens of national and global experts to deliver actionable intelligence that equips privacy professionals with confidence to advise clients and respond quickly to complex issues.

Request a complimentary trial at bna.com/privacy-data-security

Bloomberg Law®