| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Texas – Breach of Personal Identifying Information under the Texas Identity Theft Enforcement and Protection Act |
| **PAGE:** 1 of 5 | **REPLACES POLICY DATED:** 1/1/20 |
| **EFFECTIVE DATE:** September 1, 2021 | **REFERENCE NUMBER:** IP.DP.TX.002 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

**SCOPE:** All Company-affiliated facilities in the state of Texas, including, but not limited to, hospitals, ambulatory surgery centers, imaging and oncology centers, physician practices, shared services centers and corporate departments, Groups, Divisions and Markets (collectively Texas Affiliates).

**PURPOSE:** To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to an incident involving the unauthorized use or possession of personal identifying information, in compliance with the Texas Identity Theft Enforcement and Protection Act (the Act).

**POLICY:**

Texas Affiliates shall take measures to protect and secure data containing personal identifying information.

As required by law, all Texas Affiliates safeguard certain information of patients, employees, vendors, and other individuals who provide information covered by the Act.

The requirements in this policy are in addition to, and not in the place of, any requirements under the Health Information Portability and Accountability Act (HIPAA) and any and all other Federal laws, regulations and interpretive guidelines, and Facility policies promulgated thereunder.

**PROCEDURE:**

For all situations involving the inappropriate or unauthorized access, use, and/or disclosure of Personal Identifying Information/Personal Information, immediately notify an individual such as your Division and/or Facility Ethics and Compliance Officer (DECO and/or ECO), Facility Privacy Official (FPO), Facility Information Security Official (FISO)/Zone FISO or Director of Information Security (DISA), and contact the Information Protection and Security mailbox.

The facility will implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the facility in the regular course of business. A facility will destroy or arrange for the destruction of records containing sensitive personal information within the facility's custody or control that are not to be retained by the facility by:

a. Shredding;
b. Erasing; or
c. Otherwise modifying the sensitive personal information in the records to make the information unreadable or indecipherable through any means.

| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Texas – Breach of Personal Identifying Information under the Texas Identity Theft Enforcement and Protection Act |
| **PAGE:** 2 of 5 | **REPLACES POLICY DATED:** 1/1/20 |
| **EFFECTIVE DATE:** September 1, 2021 | **REFERENCE NUMBER:** IP.DP.TX.002 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

1. **Notice:**
   Notification required following a breach of security of computerized data:
   a. A person who conducts business in this state and owns or licenses computerized data that includes sensitive personal information shall disclose any breach of system security after discovering or receiving notification of the breach to any individual whose sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made without unreasonable delay, and in each case, not later than the 60th day after the date on which the person determines the breach occurred or as necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

   b. A person who is required to disclose or provide notification of a breach of system security shall notify the attorney general of that breach not later than the 60th day after the date on which the person determines that the breach occurred if the breach involves at least 250 residents of this state. The notification must include:
      i. a detailed description of the nature and circumstances of the breach or the use of sensitive personal information acquired as a result of the breach;
      ii. the number of residents of this state affected by the breach at the time of notification;
      iii. the number of affected residents that have been sent a disclosure of the breach by mail or other direct method of communication at the time of notification;
      iv. the measures taken by the person regarding the breach;
      v. any measures the person intends to take regarding the breach after the notification; and
      vi. information regarding whether law enforcement is engaged in investigating the breach.

   c. If the individual whose sensitive personal information was or is reasonably believed to have been acquired by an unauthorized person is a resident of a state that requires a person to provide notice of a breach of system security, the notice of the breach of system security may be provided under that state's law or under 1b.

   d. Any person who maintains computerized data that includes sensitive personal information not owned by the person shall notify the owner or license holder of the information of any breach of system security immediately after discovering the breach, if the sensitive personal information was, or is reasonably believed to have been, acquired by an unauthorized person.
      i. A person may give notice as required by 1b. or 1c. by providing written notice at the last known address of the individual;
      ii. electronic notice; or
      iii. notice as provided by 1e.

   e. If the person required to give notice demonstrates 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, the notice may be given by:

i. electronic mail, if the person has electronic mail addresses for the affected persons;
ii. conspicuous posting of the notice on the person's website; or
iii. notice published in or broadcast on major statewide media.

f. If a person is required to notify at one time more than 10,000 persons of a breach of system security, the person shall also notify each consumer reporting agency that maintains files on consumers on a nationwide basis, of the timing, distribution, and content of the notices. The person shall provide the notice required without unreasonable delay.

**2. Timely Review of Attorney General's Website**:

a. On the attorney general's public website a list of the notifications submitted are posted, excluding any sensitive personal information that may have been reported or that may compromise a data system's security. The attorney general:
   i. Updates the list not later than the 30th day after the date notification of a new breach of system security is received;
   ii. Removes a notification from the list not later than the first anniversary of the date it was added, if the person who submitted the notification has not informed the attorney general of any additional breaches during the period; and
   iii. Maintains only the most recently updated list on their public website.

b. If a facility submitted a breach of system security, after it was posted for one year and assuming no additional breaches have been submitted during the posting period, the FPO must review the attorney general's website to make sure it the reported breach was removed.

**3. Delayed Notice:**

A person may delay providing notice as required at the request of a law enforcement agency that determines that the notification will impede a criminal investigation. The notification shall be made as soon as the law enforcement agency determines that the notification will not compromise the investigation.

**4. Civil Penalty:**

a. A person who violates this chapter of the Act is liable to this state for a civil penalty of at least $2,000 but not more than $50,000 for each violation. The attorney general may bring an action to recover the civil penalty imposed.

b. In addition to penalties assessed under 3a, a person who fails to take reasonable action to comply is liable to this state for a civil penalty of not more than $100 for each individual to whom notification is due for each consecutive day that the person fails to take reasonable action to comply.

c. Civil penalties may not exceed $250,000 for all individuals to whom notification is due after a single breach. The attorney general may bring an action to recover the civil penalties imposed.

**DEFINITIONS:**

A. **Personal identifying information**: means information that alone or in conjunction with other information identifies an individual, including an individual's:
   1. Name;
   2. Social Security Number;
   3. Date of Birth;
   4. Government-issued identification number;
   5. Mother's maiden name;
   6. Unique biometric data, including the individual's fingerprint, voice print, and retina or iris image;
   7. Unique electronic identification number, address, or routing code; and
   8. Telecommunication access device.

B. **Sensitive personal information**: means 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:
   1. Social security number;
   2. Driver's license number or government-issued identification number; or
   3. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or
   4. Information that identifies an individual and relates to:
      i. The physical or mental health or condition of the individual;
      ii. The provision of health care to the individual; or
      iii. Payment for the provision of health care to the individual.

   The term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.

C. **Breach of system security:** means 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 accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system

security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

D. **Identity Theft:** means to obtain, possess, transfer, or use personal identifying information of another person without the other person's consent and with intent to obtain a good, a service, insurance, an extension of credit, or any other thing of value in the other person's name.

E. **Victim:** means a person whose identifying information is used by an unauthorized person.

**REFERENCES:**

1. Texas Identity Theft Enforcement and Protection Act
2. Business and Commerce Code, Title II, Subtitle B, Chapter 521, Sections 521.001, 521.002, 521.051, and 521.053
3. Penal Code, Title VII, Subtitled D, Chapter 32, Section 32.51
4. 15 U.S.C. Section 7001
5. 15 U.S.C. Section 1681a
6. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Standards for Notification in the Case of Breach of Unsecured Protected Health Information, 45 CFR Parts 160 and 164
7. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011
8. Records Management Policy, EC.014