DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Tennessee – Breach of Personal Information under the Identity Theft Deterrence Law
PAGE: 1 of 3	**REPLACES POLICY DATED:**
EFFECTIVE DATE: May 1, 2021	**REFERENCE NUMBER:** IP.DP.TN.008
APPROVED BY: Ethics and Compliance Policy Committee	

SCOPE: All Company-affiliated facilities in the state of Tennessee, 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 Tennessee Affiliates).

PURPOSE: To provide guidance regarding workforce members' responsibility for identifying and responding to an incident involving the unauthorized disclosure of unencrypted personal information, in compliance with the Release of Personal Consumer Information section under Tennessee Code Annotated § 47-18-2107.

POLICY: All Tennessee Affiliates shall implement and maintain reasonable security measures to protect and secure data containing personal information when a breach of system security (as defined below) has occurred. Notifications must be sent to the affected resident of this state no later than 45 days after the discovery of the breach of system security.

The analysis of a potential breach and whether notifications must be provided should be done in coordination with other breach notification laws, including the Health Information Portability and Accountability Act (HIPAA) breach notification requirements addressed at the Protected Health Information Breach Risk Assessment and Notification policy, IP.PRI.011, and other Federal laws, regulations and interpretive guidelines, and Facility policies promulgated thereunder. The statute discussed in this policy do not apply to Tennessee Affiliates that are information holders (as defined below and that are subject to (i) HIPAA or (ii) the Gramm-Leach-Bliley Act of 1999 (Pub. L. No. 106-102). Further, (1) if an information holder maintains its own notification procedures as part of its information security policy for the treatment of personal information (as defined below) and (2) if the information holder's policy is consistent with the timing requirements of this policy, the information holder is deemed to comply with the notification requirements of this Tennessee statute, as long as the information holder notifies subject persons in accordance with its policies in the event of a breach of system security.

DEFINITIONS

"Breach of system security":

1. Means the acquisition of unencrypted computerized data or encrypted computerized data and the encryption key by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder; and
2. Does not include the good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder if the personal information is not used or subject to further unauthorized disclosure.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Tennessee – Breach of Personal Information under the Identity Theft Deterrence Law
PAGE: 2 of 3	**REPLACES POLICY DATED:**
EFFECTIVE DATE: May 1, 2021	**REFERENCE NUMBER:** IP.DP.TN.008
APPROVED BY: Ethics and Compliance Policy Committee	

"Encrypted" means computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2.

"Information holder" means any person or business that conducts business in the state of Tennessee, or any Tennessee agency or any of its political subdivisions, that owns or licenses computerized personal information of Tennessee residents.

"Personal information":

1. Means an individual's first name or first initial and last name, in combination with any one or more of the following data elements:
   a. Social security number;
   b. Driver license number; or
   c. Account, credit card, 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; and
2. Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable.

"Unauthorized person" includes an employee of the information holder who is discovered by the information holder to have obtained personal information with the intent to use it for an unlawful purpose.

PROCEDURE:

Notifications

A. Following discovery or notification of a breach of system security by an information holder, the information holder shall disclose the breach of system security to any Tennessee resident whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in section (3).

B. Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of system security if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure must be made no later than forty-five (45) days from the discovery or notification of the breach of system security, unless a longer period of time is required due to the legitimate needs of law enforcement, as provided in section (3).

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Tennessee – Breach of Personal Information under the Identity Theft Deterrence Law
PAGE: 3 of 3	**REPLACES POLICY DATED:**
EFFECTIVE DATE: May 1, 2021	**REFERENCE NUMBER:** IP.DP.TN.008
APPROVED BY: Ethics and Compliance Policy Committee	

C. The notification required by Sections 2 and 3 above may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. If the notification is delayed, it must be made no later than forty-five (45) days after the law enforcement agency determines that notification will not compromise the investigation.

D. For purposes of this section, notice may be provided by one (1) of the following methods:
   1. Written notice;
   2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001 or if the information holder's primary method of communication with the Tennessee resident has been by electronic means; or
   3. Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), that the affected class of subject persons to be notified exceeds five hundred thousand (500,000) persons, or the information holder does not have sufficient contact information and the notice consists of all of the following:
      a. Email notice, when the information holder has an email address for the subject persons;
      b. Conspicuous posting of the notice on the information holder's website, if the information holder maintains a website page; and
      c. Notification to major statewide media.

E. If an information holder discovers circumstances requiring notification pursuant to this policy of more than one thousand (1,000) persons at one (1) time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies, as defined by 15 U.S.C. § 1681a, and credit bureaus that compile and maintain files on consumers on a nationwide basis, of the timing, distribution, and content of the notices.

F. Any customer of an information holder who is a person or business entity, but who is not an agency of Tennessee or any political subdivision of Tennessee, and who is injured by a violation of this policy, may institute a civil action to recover damages and to enjoin the information holder from further action in violation of this policy and Tennessee Code Annotated § 47-18-2107. The rights and remedies available under Tennessee Code Annotated § 47-18-2107 are cumulative to each other and to any other rights and remedies available under Tennessee or Federal law.

REFERENCES:

1. Tennessee Code Annotated § 47-18-2107
2. 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
3. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011