DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Utah – Protection of Personal Information Act
PAGE: 1 of 5	**REPLACES POLICY DATED:**
EFFECTIVE DATE: August 1, 2021	**REFERENCE NUMBER:** IP.DP.UT.015
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility for identifying and responding to a security breach, in compliance with Utah Code §§ 13-44-101 *et seq*., Protection of Personal Information Act.

POLICY: Any person who conducts business in the state of Utah and maintains personal information shall implement and maintain reasonable procedures to prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business and destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. The destruction of records shall be by: (a) shredding; (b) erasing; or (c) otherwise modifying the personal information to make the information indecipherable.

A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. If an investigation reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident.

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

PROCEDURE:

A. Notification

1. If an investigation reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification, in the most expedient time possible without unreasonable delay, to each affected Utah resident.
   a. Considering legitimate investigative needs of law enforcement after determining the scope of the breach of system security; and
   b. After restoring the reasonable integrity of the system.

2. A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if

misuse of the personal information occurs or is reasonably likely to occur. This includes sharing information relevant to the breach with the owner or licensee of the information.

3. A person may delay providing notification at the request of a law enforcement agency that determines that notification may impede a criminal investigation. A person who delays providing notification shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation.

   A notification may be provided:
   a. In writing by first-class mail to the most recent address the person has for the resident;
   b. electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001;
   c. by telephone, including through the use of automatic dialing technology not prohibited by other law; or
   d. For residents of the state for whom notification is not feasible, by publishing notice of the breach of system security in a newspaper of general circulation.

4. If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information, the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach.

5. A person who is regulated by state or federal law, and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator, is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach.

B. Enforcement, Confidentiality Agreements and Penalties
   1. The attorney general may enforce this chapter's provisions. Nothing in this chapter creates a private right of action. Nothing in this chapter affects any private right of action existing under other law, including contract or tort.

   2. A person who violates this chapter's provisions is subject to a civil penalty of no greater than two thousand five hundred dollars ($2,500) for a violation or series of violations concerning a specific consumer and no greater than one hundred thousand dollars ($100,000) in the

aggregate for related violations concerning more than one consumer, unless the violations concern:
   a. Ten thousand (10,000) or more consumers who are residents of the state;
   b. Ten thousand (10,000) or more consumers who are residents of other states; or
   c. The person agrees to settle for a greater amount.

3. In addition to these penalties, the attorney general may seek injunctive relief to prevent future violations of this chapter and attorney fees and costs. The attorney general shall bring an action under this chapter in the district court located in Salt Lake City or the district court for the district in which resides a consumer who is affected by the violation. The attorney general shall deposit any amount received into the Attorney General Litigation Fund.
   In enforcing this chapter, the attorney general may:
   a. investigate the actions of any person alleged to violate Section 13-44-201 or 13-44-202;
   b. subpoena a witness;
   c. subpoena a document or other evidence;
   d. require the production of books, papers, contracts, records, or other information relevant to an investigation;
   e. conduct an adjudication in accordance with Title 63G, Chapter 4, Administrative Procedures Act, to enforce a civil provision under this chapter; and
   f. Enter into a confidentiality agreement.

4. The attorney general has reasonable cause to believe that an individual is in possession, custody, or control of information that is relevant to enforcing this chapter, the attorney general may enter into a confidentiality agreement with the individual. In a civil action brought under this chapter, a court may issue a confidentiality order that incorporates the confidentiality agreement. A confidentiality agreement or a confidentiality order may:
   a. address a procedure;
   b. address testimony taken, a document produced, or material produced under this section;
   c. provide whom may access testimony taken, a document produced, or material produced under this section;
   d. provide for safeguarding testimony taken, a document produced, or material produced under this section; or
   e. Require that the attorney general:
      i. return a document or material to an individual; or
      ii. Notwithstanding Section 63A-12-105 or a retention schedule created in accordance with Section 63G-2-604, destroy the document or material at a designated time.

5. A subpoena issued may be served by certified mail. A person's failure to respond to a request or subpoena from the attorney general is a violation of this chapter. The attorney general may inspect and copy all records related to the business conducted by the person alleged to have violated this chapter, including records located outside the state. For records located outside of the state, the person who is found to have violated this chapter shall pay the attorney

general's expenses to inspect the records, including travel costs. Upon notification from the attorney general of the attorney general's intent to inspect records located outside of the state, the person who is found to have violated this chapter shall pay the attorney general five hundred dollars ($500), or a higher amount if five hundred dollars ($500) is estimated to be insufficient to cover the attorney general's expenses to inspect the records. To the extent an amount paid to the attorney general by a person who is found to have violated this chapter is not expended by the attorney general, the amount shall be refunded to the person who is found to have violated this chapter. The Division of Corporations and Commercial Code or any other relevant entity shall revoke any authorization to do business in this state of a person who fails to pay any amount that is required.

6. The attorney general shall keep confidential a procedure agreed to, testimony taken, a document produced, or material produced under this section pursuant to a subpoena, confidentiality agreement, or confidentiality order, unless the individual who agreed to the procedure, provided testimony, produced the document, or produced material waives confidentiality in writing.

7. The attorney general may use, in an enforcement action taken under this section, testimony taken, a document produced, or material produced under this section to the extent the use is not restricted or prohibited by a confidentiality agreement or a confidentiality order.

8. The attorney general may use, in an enforcement action taken under this section, testimony taken, a document produced, or material produced under this section that is restricted or prohibited from use by a confidentiality agreement or a confidentiality order if the individual who provided testimony or produced the document or material waives the restriction or prohibition in writing.

9. The attorney general may disclose testimony taken, a document produced, or material produced under this section, without consent of the individual who provided the testimony or produced the document or material, or the consent of an individual being investigated, to:
   a. a grand jury; or
   b. a federal or state law enforcement officer, if the person from whom the information was obtained is notified 20 days or greater before the day on which the information is disclosed, and the federal or state law enforcement officer certifies that the federal or state law enforcement officer will maintain the confidentiality of the testimony, document, or material and use the testimony, document, or material solely for an official law enforcement purpose.

10. An administrative action filed under this chapter shall be commenced no later than 10 years after the day on which the alleged breach of system security last occurred. A civil action under this chapter shall be commenced no later than five years after the day on which the alleged breach of system security last occurred.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Utah – Protection of Personal Information Act
PAGE: 5 of 5	**REPLACES POLICY DATED:**
EFFECTIVE DATE: August 1, 2021	**REFERENCE NUMBER:** IP.DP.UT.015
APPROVED BY: Ethics and Compliance Policy Committee	

DEFINITIONS

"Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner.

"Consumer" means a natural person.

"Financial institution" means the same as that term is defined in 15 U.S.C. Sec. 6809.

"Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable:

a. social security number;
b. financial account number, or credit or debit card number; and
c. any required security code, access code, or password that would permit access to the person's account; or
d. Driver's license number or state identification card number.

Personal information does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.

"Record" includes materials maintained in any form, including paper and electronic.

REFERENCES:

1. Protection of Personal Information Act:
   a. Utah Code 13-44-101
   b. Utah Code 13-44-102
   c. Utah Code 13-44-103
   d. Utah Code 13-44-201
   e. Utah Code 13-44-202
   f. Utah Code 13-44-301
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