DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Kansas – Consumer Information and Security Breach Requirements
PAGE: 1 of 3	**REPLACES POLICY DATED:**
EFFECTIVE DATE: August 1, 2021	**REFERENCE NUMBER:** IP.DP.KS.013
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility for identifying and responding to a security breach, in compliance with Kansas Statutes Annotated (K.S.A.) § 50-7a01, K.S.A. § 50-7a02, and K.S.A. §50-7a03.

POLICY: A person, according to the definition, that conducts business in Kansas, or a government, governmental subdivision or agency who owns or licenses computerized data that includes personal information shall, when it becomes aware of any breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused. If the investigation determines misuse of information has occurred or is reasonably likely to occur, the person or government, governmental subdivision or agency shall give notice as soon as possible to the affected Kansas resident.

PROCEDURE:

Notice must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

a) An individual or a commercial entity that maintains computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to the owner or licensee of the information of any breach of the security of the data following discovery of a breach, if the personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person.
b) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation. Notice required by this section shall be made in good faith, without unreasonable delay and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation.
c) Notwithstanding any other provision in this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information, and whose procedures are otherwise consistent with the timing requirements of this section, is deemed to be in compliance with the notice requirements of this section if the individual or the commercial entity notifies affected consumers in accordance with its policies in the event of a breach of security of the system.
d) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance or guidelines established by its primary or functional state or federal regulator is deemed to be in compliance with this section. This section does not relieve an individual or a

commercial entity from a duty to comply with other requirements of state and federal law regarding the protection and privacy of personal information.

e) In the event that a person discovers circumstances requiring notification pursuant to this section of more than one thousand (1,000) consumers at one time, the person shall also notify, without unreasonable delay, all nationwide consumer reporting agencies that compile and maintain files, as defined by 15 U.S.C. § 1681a(p), of the timing, distribution and content of the notices.

f) For violations of this section, except as to insurance companies licensed to do business in this state, the attorney general is empowered to bring an action in law or equity to address violations of this section and for other relief that may be appropriate. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

g) For violations of this section by an insurance company licensed to do business in this state, the insurance commissioner shall have the sole authority to enforce the provisions of this section.

Destruction of consumer information; exception

Unless otherwise required by federal law or regulation, a person or business shall take reasonable steps to destroy or arrange for the destruction of a customer's records containing personal information within its custody or control, which is no longer to be retained by the person or business by shredding, erasing or otherwise modifying personal information in the records to make it unreadable or undecipherable through any means.

DEFINITIONS

"Consumer" means an individual who is a resident of Kansas.

"Encrypted" means transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable.

"Notice" means:

a) written notice;

b) 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

c) substitute notice, if the individual or the commercial entity required to provide notice demonstrates that the cost of providing notice will exceed one hundred thousand dollars ($100,000), or that the affected class of consumers to be notified exceeds five thousand (5,000), or that the individual or the commercial entity does not have sufficient contact information to provide notice.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Kansas – Consumer Information and Security Breach Requirements
PAGE: 3 of 3	**REPLACES POLICY DATED:**
EFFECTIVE DATE: August 1, 2021	**REFERENCE NUMBER:** IP.DP.KS.013
APPROVED BY: Ethics and Compliance Policy Committee	

"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the personal information:

a) five digits of a social security number; or
b) the last four digits of a driver's license number, state identification card number or account number.

"Substitute notice" means:

a) e-mail notice if the individual or the commercial entity has e-mail addresses for the affected class of consumers;
b) conspicuous posting of the notice on the web site page of the individual or the commercial entity if the individual or the commercial entity maintains a web site; and
c) notification to major statewide media.

"Person" means any individual, partnership, corporation, trust, estate, cooperative, association, government, or governmental subdivision or agency or other entity.

"Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted:

a) social security number;
b) driver's license number or state identification card number; or
c) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.

"Security breach" means the unauthorized access and acquisition of unencrypted or unredacted computerized data that compromises the security, confidentiality or integrity of personal information maintained by an individual or a commercial entity and that causes, or such individual or entity reasonably believes has caused or will cause, identity theft to any consumer. Good faith acquisition of personal information by an employee or agent of an individual or a commercial entity for the purposes of the individual or the commercial entity is not a breach of the security of the system, provided that the personal information is not used for or is not subject to further unauthorized disclosure.

REFERENCES:

1. Kansas Statutes Annotated (K.S.A) § 50-7a01, § 50-7a02, and § 50-7a03
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