DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Alaska - Breach of Security Involving Personal Information
PAGE: 1 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.AK.019
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to a breach of the security of data that includes personal information. To establish the requirements for each Company-affiliated facility in Alaska to protect computerized personal information as required by the Alaska Personal Information Protection Act, Alaska Statute (AS) 45.48.010 to 45.48.090.

POLICY:

If a covered person owns or licenses personal information in any form that includes personal information on a state resident, and a breach of the security of the information system that contains personal information occurs, the covered person shall, after discovering or being notified of the breach, disclose the breach to each Alaska resident whose personal information was subject to the breach.

An information collector (collector) shall make the disclosure required above in the most expeditious time possible and without unreasonable delay, except as provided in AS 45.48.020 and as necessary to determine the scope of the breach and restore the reasonable integrity of the information system.

Notwithstanding the first paragraph of this section, disclosure is not required if, after an appropriate investigation and after written notification to the attorney general of this state, the covered person determines that there is not a reasonable likelihood that harm to the consumers whose personal information has been acquired has resulted or will result from the breach. The determination shall be documented in writing, and the documentation shall be maintained for five years. The notification required by this subsection may not be considered a public record open to inspection by the public.

A collector may delay disclosing the breach under AS 45.48.010 if an appropriate law enforcement agency determines that disclosing the breach will interfere with a criminal investigation. However, the collector shall disclose the breach to the state resident in the most expeditious time possible and without unreasonable delay after the law enforcement agency informs the collector in writing that disclosure of the breach will no longer interfere with the investigation.

The good faith acquisition of personal information by an employee or agent of a collector for a legitimate purpose of the collector is not a breach of the security of the information system if the employee or agent does not use the personal information for a purpose unrelated to a legitimate

purpose of the collector and does not make further unauthorized disclosure of the personal information.

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 all other Federal laws, regulations and interpretive guidelines, as well as Facility policies promulgated thereunder.

PROCEDURE:

A. Notification

A collector shall make the disclosure required by

1. a written document sent to the most recent address the collector has for the Alaska resident;
2. electronic means if the collector's primary method of communication with the state resident is by electronic means or if making the disclosure by the electronic means is consistent with the provisions regarding electronic records and signatures required for notices legally required to be in writing under 15 U.S.C. 7001 et seq. (Electronic Signatures in Global and National Commerce Act); or
3. if the collector demonstrates that the cost of providing notice would exceed $150,000, that the affected class of state residents to be notified exceeds 300,000, or that the collector does not have sufficient contact information to provide notice, by
   a. electronic email if the collector has an electronic mail address for the Alaska resident;
   b. conspicuously posting the disclosure on the Internet website of the information collector if the collector maintains an Internet website; and
   c. providing a notice to major statewide media.

B. Notification to other Agencies

1. If a collector is required to notify more than 1,000 state residents of a breach, the collector shall also notify without unreasonable delay all consumer credit reporting agencies that compile and maintain files on consumers on a nationwide basis and provide the agencies with the timing, distribution, and content of the notices to state residents.
   - "Consumer credit reporting agency that complies and maintains files on consumers on a nationwide basis" has the same meaning as in 15 U.S.C. 1681a(p).
2. This section may not be construed to require the collector to provide the consumer reporting agencies identified under (1) of this section with the names or other personal information of the state residents whose personal information was subject to the breach.
3. This section does not apply to a collector who is subject to the Gramm-Leach-Bliley Financial Modernization Act.

C. Treatment of Certain Breaches – Information Recipient

1. If a breach of the security of the information system containing personal information on a state resident that is maintained by an information recipient (recipient) occurs, the recipient is not required to comply with AS 45.48.010 to AS 45.48.030. However,

immediately after the recipient discovers the breach, the recipient shall notify the information distributor who owns the personal information or who licensed the use of the personal information to the recipient about the breach and cooperate with the distributor as necessary to allow the distributor to comply with (2) of this section. In this subsection, "cooperate" means sharing with the distributor information relevant to the breach, except for confidential business information or trade secrets.

2. If a recipient notifies an distributor of a breach under (1) of this section, the information distributor shall comply with AS 45.48.010 to AS 45.48.030 as if the breach occurred to the information system maintained by the distributor.

D. Violations

If a collector who is not a governmental agency violates AS 45.48.010 to AS 45.48.090 with regard to the personal information of a state resident, the violation is an unfair or deceptive act or practice under AS 45.50.471 to AS 45.50.561. However, the information collector is not subject to the civil penalties imposed under AS 45.50.551, but is liable to the state for a civil penalty of up to $500 for each state resident who was not notified under AS 45.48.010 to AS 45.48.090, except that the total civil penalty may not exceed $50,000, and damages that may be awarded against the collector under AS 45.50.531 are limited to actual economic damages that do not exceed $500 and AS 45.50.537 are limited to actual economic damages.

DEFINITIONS:

"Breach of the security" means unauthorized acquisition, or reasonable belief of unauthorized acquisition, of personal information that compromises the security, confidentiality, or integrity of the personal information maintained by the information collector; in this paragraph, "acquisition" includes acquisition by:

a. Photocopying, facsimile, or other paper-based method;
b. A device, including a computer, that can read, write, or store information that is represented in numerical form; or
c. A method not identified by a. or b.

“Covered person” means a:

a. Person doing business;
b. Governmental agency; or
c. Person with more than 10 employees;

“Governmental agency” means a state or local governmental agency, except for an agency of the judicial branch.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Alaska - Breach of Security Involving Personal Information
PAGE: 4 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.AK.019
APPROVED BY: Ethics and Compliance Policy Committee	

"Information collector (collector)" means a covered person who owns or licenses personal information in any form if the personal information includes personal information on an Alaska resident.

"Information distributor (distributor)" means a person who is an information collector and who owns or licenses personal information to an information recipient.

"Information recipient (recipient)" means a person who is an information collector but who does not own or have the right to license to another information collector the personal information received by the person from an information distributor.

"Personal information" means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of the following:

a. an individual's name that is a combination of an individual's first name or first initial; and last name; and
b. one or more of the following information elements:
    i. the individual's social security number;
    ii. the individual's driver's license number or state identification card number;
    iii. except as provided in (iv), the individual's account number, credit card number, or debit card number;
    iv. if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in this sub-subparagraph, "personal code" means a security code, an access code, a personal identification number, or a password;
    v. passwords, personal identification numbers, or other access codes for financial accounts.

REFERENCES:

1. Alaska Statute 45.48.010 to 45.48.090
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