| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Colorado - Breach of Personal Information under Colorado's Consumer Data Privacy Law |
| **PAGE:** 1 of 4 | **REPLACES POLICY DATED:** 8/18 (Model Policy) |
| **EFFECTIVE DATE:** February 1, 2020 | **REFERENCE NUMBER:** IP.DP.CO.004 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

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

**PURPOSE:** To provide guidance regarding workforce members' responsibility related to data breaches and establish the requirements for each Company-affiliated facility in Colorado to protect personal information as required by Colorado House Bill 18-1128, effective September 1, 2018.

**POLICY:** Covered entities shall implement and maintain reasonable security measures to protect and secure personal information. If a breach of security may have occurred, a covered entity must promptly conduct a good faith investigation to determine the likelihood that personal information has been or will be misused. Unless the investigation determines that misuse of the personal information has not occurred and is not reasonably likely to occur, the covered entity must give notice to certain individuals, agencies and other entities.

Covered entities must notify each individual in Colorado whose personal information was, or was reasonably believed to have been, accessed as a result of a breach. Breaches involving 500 or more individuals must be reported to the Department of Legal Affairs and the Colorado Attorney General. If a single breach involves more than 1,000 individuals, the covered entity must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

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

**DEFINITIONS**

**"Breach of security" or "breach"** means unauthorized acquisition or use of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the covered entity.

**"Covered entity"** means a person that maintains, owns, or licenses personal information in the course of the person's business, vocation, or occupation. "Covered entity" does not include a person acting as a third-party service provider.

**"Personal information" or "PI"** means a Colorado resident's first name or first initial and last name plus at least one of the following: social security number, document (student ID, military ID, passport, driver's license) number, medical information, health insurance identification number, or biometric data. "Personal information" also includes a Colorado resident's username, email address,

account number, credit or debit card number, plus any access codes, security questions and answers, or passwords that would permit access to an account.

**"Third-party service provider"** means an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity.

**PROCEDURE:**

1. Notice to the Individual
   a. Unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, covered entities must notify each individual in Colorado affected by the breach. Notice to individuals shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of the breach of security, to identify individuals affected by the breach, and to restore the reasonable integrity of the computerized data system that was breached, but no later than 30 days after the determination that a breach of security occurred.
   b. Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's state or federal regulator is in compliance with the notice requirement in this subsection. As such, to the extent the covered entity must otherwise notify individuals under federal law (*e.g.*, HIPAA), such notice will suffice, if provided no later than 30 days after the determination that a breach of security occurred.
   c. If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would impede a criminal investigation and the law enforcement agency notifies the covered entity not to send notice as required by this policy, the notice may be delayed for a specified period that the law enforcement agency determines is reasonably necessary.
   d. Notice to the affected individuals is not required if, after a good faith investigation, the covered entity reasonably determines that misuse of the personal information has not occurred and is not reasonably likely to occur.
   e. In the case of a breach of encrypted or otherwise secured personal information, notice to the affected individuals is not required if the encryption key, the confidential process, or other means to decipher the secured information was not acquired or reasonably believed to have been acquired.
   f. The notice to an affected individual shall be by one of the following methods:
      i. Written notice sent to the mailing address of the individual in the records of the covered entity; or
      ii. Electronic notice, if a primary means of communication by the covered entity is by electronic means; or
      iii. Telephonic notice.

| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Colorado - Breach of Personal Information under Colorado's Consumer Data Privacy Law |
| **PAGE:** 3 of 4 | **REPLACES POLICY DATED:** 8/18 (Model Policy) |
| **EFFECTIVE DATE:** February 1, 2020 | **REFERENCE NUMBER:** IP.DP.CO.004 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

g. The notice to an individual with respect to a breach of security shall include, at a minimum:
   i. The date, estimated date, or estimated date range of the breach of security.
   ii. A description of the personal information that was acquired or reasonably believed to have been acquired as a part of the breach of security.
   iii. Information that the individual can use to contact the covered entity to inquire about the breach of security.
   iv. The toll-free numbers, addresses, and websites for consumer reporting agencies.
   v. The toll-free number, address, and website for the Federal Trade Commission.
   vi. A statement that the individual can obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.
   vii. A statement directing the individual to promptly change his or her password and security question, or to take other steps appropriate to protect the individual's online account with the covered entity and all other online accounts for which the individual uses the same username, email address and password, or security question or answer.

h. Covered entities that are required to provide notice to an individual may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, or because the covered entity does not have sufficient contact information to provide notice. Such substitute notice shall include the following:
   i. Email notice if the covered entity has email addresses for the individuals;
   ii. A conspicuous notice on the website of the covered entity if the covered entity maintains a website; and
   iii. Notification to a major statewide media.

2. <u>Notice to Credit Reporting Agencies</u>
   a. In the case where a single breach event affects more than 1,000 Colorado residents and unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, the covered entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by the federal Fair Credit Reporting Act, specifically Equifax, Transunion, and Experian.
   b. Notification shall include the anticipated date of the covered entity's separate notification to Colorado residents, as well as the approximate number of Colorado residents to be notified.
   c. Notification shall be provided in the most expedient time possible and without unreasonable delay.

3. <u>Notice to the Colorado Attorney General</u>
   a. In the case where a single breach is reasonably believed to have affected 500 residents of Colorado or more and unless a prompt investigation determines that misuse of personal information has not occurred and is not reasonably likely to occur, the covered entity shall also notify the Colorado Attorney General.

| | |
|---|---|
| **DEPARTMENT:** Information Protection and Security | **POLICY DESCRIPTION:** Colorado - Breach of Personal Information under Colorado's Consumer Data Privacy Law |
| **PAGE:** 4 of 4 | **REPLACES POLICY DATED:** 8/18 (Model Policy) |
| **EFFECTIVE DATE:** February 1, 2020 | **REFERENCE NUMBER:** IP.DP.CO.004 |
| **APPROVED BY:** Ethics and Compliance Policy Committee | |

b. Notification shall be provided in the most expedient time possible and without unreasonable delay but in no event later than 30 days from the date of the determination that a breach occurred.

4. Notice By Third-Party Agents; Duties of Third-Party Agents; Notice by Agents (including Business Associates under HIPAA)
   a. In the event of a breach of security of a system maintained by a third-party agent that contains personal information, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable and without unreasonable delay, if misuse of personal information is likely to occur. Upon receiving notice from a third-party agent, a covered entity shall provide the required notices to individuals, consumer reporting agencies, the Colorado Attorney General, and to any other party required by law. A third-party agent shall provide the covered entity with all information that the covered entity needs to comply with its notice requirements.

5. Requirements for Destruction of Records with Personal Information
   a. Each covered entity or third-party agent shall take all reasonable measures to destroy, or arrange for the destruction of, any paper or electronic documents containing personal information and within its custody or control when such documents are no longer needed, unless otherwise required by state or federal law or regulation. Such destruction shall involve shredding, erasing, or otherwise modifying the personal information in the documents to make it unreadable or indecipherable through any means.

**REFERENCES:**


1. Colorado House Bill 18-1128
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