DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Florida - Breach of Confidential Information under the Florida Information Protection Act of 2014
PAGE: 1 of 5	**REPLACES POLICY DATED:** 7/1/14 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.FL.005
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to data breaches and establish the requirements for each Company-affiliated facility in Florida to protect confidential personal information as required by The Florida Information Protection Act of 2014, effective July 1, 2014.

POLICY: Covered entities shall take reasonable measures to protect and secure data in electronic form containing personal information. Covered entities must notify each individual in Florida whose personal information was, or was reasonably believed to have been, accessed as a result of a breach. Breaches involving more than 500 individuals must be reported to the Florida Department of Legal Affairs. If a breach involves more than 1,000 individuals at a single time, the covered entity must notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis.

A covered entity that does not provide breach notification to the individual or to the Department of Legal Affairs as required will be liable for a civil penalty. The civil penalty will be $1,000 for each day the breach goes undisclosed for the first 30 days, and $50,000 for each 30-day period, or portion of a 30-day period, for up to 180 days. If the required notification is not made within 180 days, the maximum civil penalty is $500,000. The civil penalties are applied per breach and not per individual affected by the breach. This does not establish a private cause of action.

DEFINITIONS

"Breach of security" or "breach" means unauthorized access of data in electronic form containing personal information. Good faith access of personal information by an employee or agent of the covered entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

"Covered entity" means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information. For purposes of the notice requirements of subsections (3) - (6) of the Florida Information Protection Act of 2014, the term includes a governmental entity.

"Customer records" means any material, regardless of the physical form, on which personal information is recorded or preserved by any means, including, but not limited to, written or spoken words, graphically depicted, printed, or electromagnetically transmitted that are provided by an individual in this state to a covered entity for the purpose of purchasing or leasing a product or obtaining a service.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Florida - Breach of Confidential Information under the Florida Information Protection Act of 2014
PAGE: 2 of 5	**REPLACES POLICY DATED:** 7/1/14 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.FL.005
APPROVED BY: Ethics and Compliance Policy Committee	

"Data in electronic form" means any data stored electronically or digitally on any computer system or other database and includes recordable tapes and other mass storage devices.

"Department" means the Department of Legal Affairs.

"Governmental entity" means any department, division, bureau, commission, regional planning agency, board, district, authority, agency, or other instrumentality of this state that acquires, maintains, stores, or uses data in electronic form containing personal information.

"Personal information" means either of the following:

1. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:
   a. A social security number;
   b. A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
   c. A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;
   d. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or
   e. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.
2. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

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

PROCEDURE:

1. Notice to the Department of Legal Affairs

   a. Covered entities must provide notice to the Department of Legal Affairs of any breach of security affecting 500 or more individuals in the state of Florida. Such notice must be provided to the department as expeditiously as practicable, but no later than 30 days after the determination of the breach or reason to believe a breach occurred. A covered entity may receive 15 additional days to provide notice if good cause for delay is

provided in writing to the department within 30 days after determination of the breach or reason to believe a breach occurred.

b. The written notice to the department must include:
   i. A synopsis of the events surrounding the breach at the time notice is provided.
   ii. The number of individuals in this state who were or potentially have been affected by the breach.
   iii. Any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions as to how to use such services.
   iv. A copy of the notice to the patient or an explanation of the other actions taken.
   v. The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about the breach.

c. Covered entities must provide the following information to the department upon its request:
   i. A police report, incident report, or computer forensics report.
   ii. A copy of the policies in place regarding breaches.
   iii. Steps that have been taken to rectify the breach.

d. Covered entities may provide the department with supplemental information regarding a breach at any time.

2. Notice to the Individual
   a. Covered entities must notify each individual in Florida whose personal information was, or the covered entity reasonably believes to have been, accessed as a result of 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 data system that was breached, but no later than 30 days after the determination of a breach or reason to believe a breach occurred unless subject to an authorized delay or waiver as outlined below.

   b. If a federal, state, or local law enforcement agency determines that notice to individuals required under this subsection would interfere with a criminal investigation, the notice shall be delayed upon the written request of the law enforcement agency for a specified period that the law enforcement agency determines is reasonably necessary. A law enforcement agency may, by a subsequent written request, revoke such delay as of a specified date or extend the period set forth in the original request made under this paragraph to a specified date if further delay is necessary.

c. Notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed. Such a determination must be documented in writing and maintained for at least five (5) years. The covered entity shall provide the written determination to the department within 30 days after the determination.

d. 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. E-mail notice sent to the e-mail address of the individual in the records of the covered entity.

e. 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 accessed or reasonably believed to have been accessed 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 and the personal information that the covered entity maintained about the individual.

f. 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, because the affected individuals exceed 500,000 persons, or because the covered entity does not have an e-mail address or mailing address for the affected individuals. Such substitute notice shall include the following:
   i. A conspicuous notice on the website of the covered entity if the covered entity maintains a website; and
   ii. Notice in print and to broadcast media, including major media in urban and rural areas where the affected individuals reside.

g. Notice provided pursuant to rules, regulations, procedures, or guidelines established by the covered entity's primary or functional federal regulator is deemed to be in compliance with the notice requirement in this subsection if the covered entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security. Under this paragraph, a covered entity that timely provides a copy of such notice to the department is deemed to be in compliance with the notice requirement.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Florida - Breach of Confidential Information under the Florida Information Protection Act of 2014
PAGE: 5 of 5	**REPLACES POLICY DATED:** 7/1/14 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.FL.005
APPROVED BY: Ethics and Compliance Policy Committee	

3. Notice to Credit Reporting Agencies
   If a covered entity discovers circumstances requiring notice pursuant to this section of more than 1,000 individuals at a single time, the covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, 15 U.S.C. s. 1681a(p), of the timing, distribution, and content of the notices.

4. Notice By Third-Party Agents; Duties of Third-Party Agents; Notice by Agents
   a. In the event of a breach of security of a system maintained by a third-party agent, such third-party agent shall notify the covered entity of the breach of security as expeditiously as practicable, but no later than 10 days following the determination of the breach of security or reason to believe the breach occurred. Upon receiving notice from a third-party agent, a covered entity shall provide the required notices. A third-party agent shall provide the covered entity with all information that the covered entity needs to comply with its notice requirements.
   b. An agent may provide notice as required on behalf of the covered entity; however, an agent's failure to provide proper notice shall be deemed a violation of this section against the covered entity.

5. Requirements for Disposal of Customer Records
   Each covered entity or third-party agent shall take all reasonable measures to dispose, or arrange for the disposal, of customer records containing personal information within its custody or control when the records are no longer to be retained. Such disposal shall involve shredding, erasing, or otherwise modifying the personal information in the records to make it unreadable or undecipherable through any means.

REFERENCES:

1. Florida State Bill 1524, The Florida Information Protection Act of 2014
2. Section 501.171, Florida Statues
3. Section 282.0041, Florida Statues
4. Section 282.318, Florida Statues