DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Georgia – Breach of Personal Information under Georgia's Personal Identity Protection Act
PAGE: 1 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2021	**REFERENCE NUMBER:** IP.DP.GA.009
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to an incident involving a breach of security of the system involving the unauthorized acquisition and use of an individual's personal information. To establish the requirements for each Company-affiliated facility in Georgia to protect personal information as required by Georgia Code Annotated § 10-1-910 *et seq.*, effective May 24, 2007.

POLICY: Covered entities shall implement and maintain reasonable security measures to protect and secure personal information (PI). 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.

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 the security of the system" means unauthorized acquisition of an individual's electronic data that compromises the security, confidentiality, or integrity of personal information of such individual maintained by an information broker or data collector. Good faith acquisition or use of personal information by an employee or agent of an information broker or data collector for the purposes of such information broker or data collector is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

"Data collector" means any state or local agency or subdivision thereof including any department, bureau, authority, public university or college, academy, commission, or other government entity; provided, however, that the term "data collector" shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information.

"Information broker" means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental

agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.

"Notice" means the following:

A. Written notice;
B. Telephone notice;
C. Electronic notice, if the notice provided is consistent with the provisions regarding
   1. electronic records and signatures set forth in Section 7001 of Title 15 of the United
   2. States Code; or
D. Substitute notice, if the information broker or data collector demonstrates the cost of providing notice would exceed $50,000.00, the affected class of individuals to be notified exceeds 100,000, or the information broker or data collector does not have sufficient contact information to provide written or electronic notice to such individuals.

   Substitute notice shall consist of all of the following:
   1. E-mail notice, if the information broker or data collector has an e-mail address for the individuals to be notified;
   2. Conspicuous posting of the notice on the information broker's or data collector's website page, if the information broker or data collector maintains one; and
   3. Notification to major statewide media.

   Notwithstanding any provision of this paragraph to the contrary, an information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this policy shall be deemed to be in compliance with the notification requirements of this policy if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

"Person" means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. The term "person" as used in this policy shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

A. Social security number;
B. Driver's license number or state identification card number;
C. Account number, credit card number, or debit card number, if circumstances exist; and
D. Wherein such a number could be used without additional identifying information, access codes, or passwords;

E. Account passwords or personal identification numbers or other access codes; or
Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform Identity theft against the person whose information was compromised.

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.

PROCEDURE:

Notification:

Notice to the individual who is a resident of Georgia is required following a breach of security of the system.

A. Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C) of this section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

B. Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

C. The notification may be delayed if a law enforcement agency determines that the notification will compromise a criminal investigation. The notification shall be made after the law enforcement agency determines that it will not compromise the investigation.

In the event that an information broker or data collector discovers circumstances requiring notification pursuant to O.C.G.A. § 10-1-912 of more than 10,000 residents of this state at one time, the information broker or data collector shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Georgia – Breach of Personal Information under Georgia's Personal Identity Protection Act
PAGE: 4 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2021	**REFERENCE NUMBER:** IP.DP.GA.009
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. O.C.G.A § 10-1-910 - 912
2. 15 U.S.C. Section 1681a
3. 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
4. Protected Health Information Breach Risk Assessment and Notification, IP.PRI.011