DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** North Carolina Identity Theft Act: Breach of Personal and Identifying Information
PAGE: 1 of 4	**REPLACES POLICY DATED:** 6/3/19 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.NC.007
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to an incident involving the unauthorized disclosure of unencrypted personal information, in compliance with the Identity Theft Protection Act of 2005, North Carolina General Statutes § 7560 et seq. and § 132-1.10 of the Public Records Act (together, the "Act").

POLICY: This policy is applicable to all Company-affiliated facilities in the state of North Carolina, 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 North Carolina Affiliates) shall take measures to protect and secure data containing personal information.

As required by law, all Company-affiliated facilities safeguard certain information of patients, employees, vendors, and other individuals who provide information covered by the Act.

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

A. **Security Breach**:
   1. An incident of unauthorized access to and acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to an individual.
   2. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key also shall constitute a security breach.
   3. Good faith acquisition of personal information by an employee or agent of the facility for a legitimate purpose is not a security breach, provided that the personal information is not used

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** North Carolina Identity Theft Act: Breach of Personal and Identifying Information
PAGE: 2 of 4	**REPLACES POLICY DATED:** 6/3/19 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.NC.007
APPROVED BY: Ethics and Compliance Policy Committee	

for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure.

B. **Identifying Information:** Under the Act and N.C.G.S. § 14-113.20, the following is considered identifying information for purposes of the Act:
   1. Social security or employer taxpayer identification numbers.
   2. Driver's license, State identification card, or passport numbers.
   3. Checking account numbers.
   4. Savings account numbers.
   5. Credit card numbers.
   6. Debit card numbers.
   7. Personal Identification (PIN) Code as defined in G.S. 14-113.8(6).
   8. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
   9. Digital signatures.
   10. Any other numbers or information that can be used to access a person's financial resources
   11. Biometric data.
   12. Fingerprints.
   13. Passwords.
   14. Parent's legal surname prior to marriage.

C. **Personal Information:** A person's first name or first initial and last name in combination with identifying information.

D. **Business:** A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency.

PROCEDURE:

1. Security Incidents
   The facility will take all reasonable steps to prevent security breaches of personal information and identifying information, as defined in Sections B and C above. If a security breach is

suspected or discovered, the facility will investigate the incident and, where necessary, provide notifications in accordance with the Act and as outlined in this policy.

2. Notification to Affected Individuals
   Notify affected individuals without unreasonable delay, with the following information:
   a. The incident in general terms;
   b. The type of identifying information that was subject to the unauthorized access and acquisition;
   c. The general acts of the facility to protect the personal information from further unauthorized access;
   d. A telephone number that the person may call for further information and assistance;
   e. Advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports;
   f. Provide the affected individuals with contact information including toll-free numbers and addresses for the three (3) major consumer reporting agencies, the Federal Trade Commission, and the North Carolina Attorney General's Office, along with a statement that the individual can obtain information from the FTC and the AG's Office about preventing identity theft;
   g. Notice to affected persons may be provided by one or more of the following methods:
      i. Written notice;
      ii. Electronic notice for those persons for whom the facility has a valid email address and who have agreed to receive communications electronically, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing set forth in 15 U.S.C. § 7001; or
      iii. Telephonic notice, provided that contact is made directly with the affected persons and appropriately documented by the facility.

3. Optional Notification to Affected Individuals
   a. If appropriate, the facility may offer affected individuals the option to enroll in a credit monitoring service for a defined period of time at the facility's expense.
   b. Whether this option is provided will depend on the circumstances surrounding the incident.

4. Delayed Notice
   a. Notice shall be delayed if law enforcement informs the facility that disclosure of the breach would impede a criminal investigation or jeopardize national security.
   b. A request for delayed notification must be made in writing or documented contemporaneously by the facility in writing, including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** North Carolina Identity Theft Act: Breach of Personal and Identifying Information
PAGE: 4 of 4	**REPLACES POLICY DATED:** 6/3/19 (Model Policy)
EFFECTIVE DATE: February 1, 2020	**REFERENCE NUMBER:** IP.DP.NC.007
APPROVED BY: Ethics and Compliance Policy Committee	

c. The required notice shall be provided without unreasonable delay after the law enforcement agency communicates to the facility, its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

5. Substitute Notice

Substitute notice may be given if:

a. The cost of providing the notice exceeds $250,000;
b. The number of affected persons is greater than 500,000; or
c. The facility does not have the necessary contact information to notify the individual in any of the aforementioned manners.
d. Substitute notice will include posting a notice on the facility's website, emailing the affected persons if they have provided their email addresses, and notifying major statewide media.

6. NC Attorney General Notification

a. If the facility provides notice to an affected individual, it also will notify without unreasonable delay the Consumer Protection Division of the Attorney General's Office as to the nature of the breach, the number of consumers affected by the breach, steps taken to investigate the breach, steps taken to prevent a similar breach in the future, and information about the timing, distribution, and content of the notice.
b. If a security breach, as defined in this policy, involves the personal information of more than 1,000 persons, the facility will provide written notice of the timing, distribution, and content of the notice to the Consumer Protection Division of the North Carolina Attorney General's Office, as well as to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p). In addition, the facility will submit to the Consumer Protection Division a completed "North Carolina Security Breach Reporting Form" which includes the number of North Carolina residents affected and the total number of persons affected by the security breach.

REFERENCES:

1. Identity Theft Protection Act of 2005, North Carolina General Statutes (N.C.G.S.) § 75-60 et seq. and § 132-1.10 of the Public Records Act (together, the "Act").
2. N.C.G.S. § 14-113.20
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