DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** New Hampshire – Notice of Security Breach
PAGE: 1 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.NH.018
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to a breach of security of computerized data that includes personal information. To establish the requirements for each Company-affiliated facility in New Hampshire to protect computerized personal information as required by New Hampshire Chapter 359-C, Section 359-C-19 and New Hampshire Chapter 332-I, and 332-I:5.

POLICY:

Security Breach of Computerized Personal Information

Any New Hampshire Affiliate that owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the New Hampshire Affiliate shall notify the affected individuals as soon as possible.

In addition, the New Hampshire Affiliate shall notify the New Hampshire attorney general's office. Notwithstanding the foregoing, to the extent that a New Hampshire Affiliate performs services that are subject to the jurisdiction of the New Hampshire bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other states, or federal banking or securities regulators, the New Hampshire Affiliate also shall notify the regulator which has primary regulatory authority over such trade or commerce rather than the New Hampshire attorney general's office. The notice shall include the anticipated date of the notice to the individuals and the approximate number of individuals in New Hampshire who will be notified. The notice should not include the names of impacted or potentially impacted individuals or any personal information relating to them.

Any New Hampshire Affiliate that maintains computerized data that includes personal information that the New Hampshire Affiliate does not own shall notify and cooperate with the owner or licensee of the information of any security breach immediately following discovery, if the personal information was acquired by an unauthorized person. Cooperation includes sharing with the owner or licensee information relevant to the breach; except that such cooperation shall not be deemed to require the disclosure of confidential or business information or trade secrets.

Notification to an individual, the New Hampshire attorney general or a New Hampshire regulatory agency, or to the owner or licensee of personal information, as described above, may be delayed if a law enforcement agency, or national or homeland security agency determines that the notification will impede a criminal investigation or jeopardize national or homeland security.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** New Hampshire – Notice of Security Breach
PAGE: 2 of 4	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.NH.018
APPROVED BY: Ethics and Compliance Policy Committee	

Other Breach Notification Requirements

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 a New Hampshire Affiliate's policies promulgated thereunder.

PROCEDURE:

Personal Information

A. Notice

1. The notice required under this policy shall be provided by one of the following methods:
   a. Written notice;
   b. Electronic notice, if the New Hampshire Affiliate's primary means of communication with affected individuals is by electronic means;
   c. Telephonic notice, provided that a log of each such notification is kept by the New Hampshire Affiliate;
   d. Substitute notice, if the New Hampshire Affiliate demonstrates that the cost of providing notice would exceed $5,000, that the affected class of subject individuals to be notified exceeds 1,000, or the New Hampshire Affiliate does not have sufficient contact information or consent to provide notice pursuant to subparagraphs (A)(1)(a)-(c), above. Substitute notice shall consist of all of the following:
      i. E-mail notice when the New Hampshire Affiliate has an e-mail address for the affected individuals;
      ii. Conspicuous posting of the notice on the New Hampshire Affiliate's business website, if the New Hampshire Affiliate maintains a website; and
      iii. Notification to major statewide media; or

2. Notice shall include at a minimum.
   a. A description of the incident in general terms;
   b. The approximate date of breach;
   c. The type of personal information obtained as a result of the security breach; and
   d. The telephonic contact information of the applicable New Hampshire Affiliate.

3. If the New Hampshire Affiliate performs services that are subject to the jurisdiction of the New Hampshire bank commissioner, the director of securities regulation, the insurance commissioner, the public utilities commission, the financial institutions and insurance regulators of other states, or federal banking or securities regulators, and if it maintains procedures for security breach notification pursuant to the laws, rules, regulations, guidance, or guidelines issued by a state or federal regulator, the New Hampshire Affiliate shall be permitted to provide security breach notification in accordance with such laws, rules, regulations, guidance, or guidelines.

4. If a New Hampshire Affiliate is required to notify more than 1,000 consumers of a breach of security pursuant to this policy, the New Hampshire Affiliate shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of the notification to the consumers, the approximate number of consumers who will be notified, and the content of the notice. The notice should not include the names of impacted or potentially impacted individuals or any personal information relating to them.

B. Noncompliance

1. The New Hampshire attorney general's office has the authority to enforce violations of required security breach notifications.

2. The burden shall be on the New Hampshire Affiliate to demonstrate compliance with New Hampshire's breach notification requirements.

3. Any person injured by a New Hampshire Affiliate's violation of the New Hampshire data breach notification requirements may bring an action for damages and for such equitable relief, including an injunction, as the court deems necessary and proper. If the court finds for the plaintiff, New Hampshire law states that the plaintiff will be awarded the amount of actual damages. For willful or knowing violations, a court shall award as much as three times, but not less than two times, the amount of actual damages. Prevailing plaintiffs also shall be awarded the costs of the suit and reasonable attorney's fees, as determined by the court. Waivers of the right to these damages shall be void and unenforceable. At the court's discretion, it may grant injunctive relief to private individuals without bond.

DEFINITIONS

"Computerized data" means personal information stored in an electronic format.

"Encrypted" means the transformation of data through the use of an algorithmic process into a form for which there is a low probability of assigning meaning without use of a confidential process or key, or securing the information by another method that renders the data elements completely unreadable or unusable. Data shall not be considered to be encrypted if it is acquired in combination with any required key, security code, access code, or password that would permit access to the encrypted data.

"Person" means an individual, corporation, trust, partnership, incorporated or unincorporated association, limited liability company or other form of entity, or any agency, authority, board, court, department, division, commission, institution, bureau, or other state governmental entity, or any political subdivision of the state.

"Personal information" means an individual's first name or 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:

a. Social security number;
b. Driver's license number or other government identification number;
c. Account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

"Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.

"Security breach" means unauthorized acquisition of computerized data that compromises the security or confidentiality of personal information maintained by a person doing business in this state. Good faith acquisition of personal information by an employee or agent of a person for the purposes of the person's business shall not be considered a security breach, provided that the personal information is not used or subject to further unauthorized disclosure.

REFERENCES:

1. New Hampshire, Notice of Security Breach, Section 359-C-19
2. New Hampshire, Chapter 332-I and 332-I:5
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