DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Indiana – Disclosure of Security Breaches and Notification Process
PAGE: 1 of 6	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.IN.017
APPROVED BY: Ethics and Compliance Policy Committee	

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

PURPOSE: To provide guidance regarding workforce members' responsibility related to procedures and protocols for identifying and responding to a breach of the security of data that includes personal information. To establish the requirements for each Company-affiliated facility in Indiana to protect computerized personal information as required by Indiana Code Title 24, Sections 4.9-1-1 to 4.9-4-2.

POLICY:

Any person doing business in Indiana who owns, uses, or maintains licensed computerized data that includes personal information and becomes aware of a breach of the security of data or is notified, the database owner shall disclose the breach to an Indiana resident whose unencrypted personal information was or may have been acquired by an unauthorized person; or whose encrypted personal information was or may have been acquired by an unauthorized person with access to the encryption key if the database owner knows, should know, or should have known that the unauthorized acquisition constituting the breach has resulted in or could result in identity deception, identity theft, or fraud affecting the Indiana resident.

A database owner required to make a disclosure to more than one thousand (1,000) consumers shall also disclose to each consumer reporting agency (as defined in 15 U.S.C. 1681a(p)) information necessary to assist the consumer reporting agency in preventing fraud, including personal information of an Indiana resident affected by the breach of the security of a system.

If the database owner makes a disclosure as described above, the database owner shall also disclose the breach to the attorney general.

A person that maintains computerized data but that is not a database owner shall notify the database owner if the person discovers that personal information was or may have been acquired by an unauthorized person.

A person required to make a disclosure or notification shall make the disclosure or notification without unreasonable delay. A delay is reasonable if the delay is:

1. necessary to restore the integrity of the computer system;
2. necessary to discover the scope of the breach;
3. in response to a request from the attorney general or a law enforcement agency to delay disclosure because disclosure will impede a criminal or civil investigation; or
4. it will jeopardize national security.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Indiana – Disclosure of Security Breaches and Notification Process
PAGE: 2 of 6	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.IN.017
APPROVED BY: Ethics and Compliance Policy Committee	

The person required to make a disclosure or notification shall make the disclosure or notification as soon as possible after the delay is no longer necessary to restore the integrity of the computer system or to discover the scope of the breach, or the attorney general or a law enforcement agency notifies the person that delay will no longer impede a criminal or civil investigation or jeopardize national security.

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 Facility policies promulgated thereunder.

PROCEDURE:

A. Notifications and Disclosures

1. A database owner required to make a disclosure, shall make the disclosure using one (1) of the following methods:
   a. mail;
   b. telephone;
   c. facsimile (fax); or
   d. electronic mail, if the database owner has the electronic mail address of the affected Indiana resident.
2. If a database owner is required to make the disclosure to more than five hundred thousand (500,000) Indiana residents, or if it is determined that the cost of the disclosure will be more than two hundred fifty thousand dollars ($250,000), the database owner may elect to make the disclosure by using both of the following methods:
   a. conspicuous posting of the notice on the web site of the database owner, if a web site is maintained; and
   b. notice to major news reporting media in the geographic area where Indiana residents affected by the breach of the security of a system reside.
3. A database owner that maintains its own disclosure procedures as part of an information privacy policy or a security policy is not required to make a separate disclosure if the database owner's information privacy policy or security policy is at least as stringent as the disclosure requirements throughout this policy.
4. A database owner that maintains its own disclosure procedures as part of an information privacy, security policy, or compliance plan under:
   a. the federal USA PATRIOT Act (P.L. 107-56);
   b. Executive Order 13224;
   c. the federal Driver's Privacy Protection Act (18 U.S.C. 2781 et seq.);
   d. the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
   e. the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or
   f. the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191) is not required to make a disclosure if the database owner's information privacy, security policy, or compliance plan requires that Indiana residents be notified of a

breach of the security of data without unreasonable delay and the database owner complies with his information privacy, security policy, or compliance plan.

5. A person required to make a disclosure may elect to make all or part of the disclosure in accordance with section A1 even if the person could make the disclosure in accordance with section A2.

B. Current or Former Health Care Provider

1. A current or former health care provider who is a database owner or former database owner to which an exemption under the following applies or applied:
   a. the federal USA PATRIOT Act (P.L. 107-56);
   b. Executive Order 13224;
   c. the federal Driver's Privacy Protection Act (18 U.S.C. 2721 et seq.);
   d. the federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
   e. the federal Financial Modernization Act of 1999 (15 U.S.C. 6801 et seq.); or
   f. the federal Health Insurance Portability and Accountability Act (HIPAA) (P.L. 104-191); and;

2. Whose information privacy, security policy, or compliance plan:
   a. does not require the current or former database owner to maintain and implement reasonable procedures; or
   b. is not implemented by the current or former database owner to ensure that the personal information described in section B1a, including health records (as defined by IC 4-6-14-2.5), is protected and safeguarded from unlawful use or disclosure after current or former database owner ceases to be a covered entity under the federal Health Insurance Portability and Accountability Act (P.L. 104-191).
3. A database owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure of any personal information of Indiana residents collected or maintained by the database owner.
4. A database owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable.
5. A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act that is actionable only by the attorney general under this section.
6. The attorney general may bring an action under this section to obtain any or all of the following:
   a. an injunction to enjoin further violations of this section;
   b. a civil penalty of not more than five thousand dollars ($5,000) per deceptive act;
   c. the attorney general's reasonable costs in:
      i. the investigation of the deceptive act; and
      ii. maintaining the action.

7. A failure to comply with section B.2.c., or B.2.d., in connection with related acts or omissions constitutes one (1) deceptive act.

C. Enforcement
1. A person that is required to make a disclosure or notification in accordance with IC 24-4.9-3 and that fails to comply with any provision of this article commits a deceptive act that is actionable only by the attorney general.
2. A failure to make a required disclosure or notification in connection with a related series of breaches of the security of data constitutes one (1) deceptive act.

D. Attorney General
The attorney general may bring an action to obtain any or all of the following:
1. an injunction to enjoin future violations of IC 24-4.9-3;
2. a civil penalty of not more than one hundred fifty thousand dollars ($150,000) per deceptive act; or
3. The attorney general's reasonable cost in:
   a. the investigation of the deceptive act; and
   b. maintaining the action.

DEFINITIONS:

"Breach of the security of data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.

The term does not include the following:
1. Good faith acquisition of personal information by an employee or agent of the person for lawful purposes of the person, if the personal information is not used or subject to further unauthorized disclosure.
2. Unauthorized acquisition of a portable electronic device on which personal information is stored, if all personal information on the device is protected by encryption and the encryption key:
   a. has not been compromised or disclosed; and
   b. is not in the possession of or known to the person who, without authorization, acquired or has access to the portable electronic device.

"Database owner" means a person that owns or licenses computerized data that includes personal information.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Indiana – Disclosure of Security Breaches and Notification Process
PAGE: 5 of 6	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.IN.017
APPROVED BY: Ethics and Compliance Policy Committee	

"Doing business in Indiana" means owning or using the personal information of an Indiana resident for commercial purposes.

"Encrypted data" for the purposes of this policy, data are encrypted if the data:

1. have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or
2. are secured by another method that renders the data unreadable or unusable.

"Indiana Resident" means a person whose principal mailing address is in Indiana, as reflected in records maintained by the database owner.

"Mail" has the meaning set for in IC 231-20-15. Mail means:

1. first class, certified, or registered United States mail, postage prepaid; or
2. private carrier service, fees prepaid or billed to the sender.

"Person" means an individual, a corporation, a business trust, an estate, a trust, a partnership, an association, a nonprofit corporation or organization, a cooperative, or any other legal entity.

"Personal information" means:

1. a Social Security number that is not encrypted or redacted; or
2. an individual's first and last names, or first initial and last name, and on one (1) or more of the following data elements that are not encrypted or redacted:
   a. a driver's license number;
   b. a state identification card number;
   c. a credit card number; or
   d. a financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

   The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

"Redacted data or personal information":

1. Data are redacted for purposes of this policy if the data have been altered or truncated so that not more than the last four (4) digits of:
   a. a driver's license number;
   b. a state identification number; or
   c. an account number is accessible as part of personal information.
2. For purposes of this policy, personal information is "redacted" if the personal information has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information.

DEPARTMENT: Information Protection and Security	**POLICY DESCRIPTION:** Indiana – Disclosure of Security Breaches and Notification Process
PAGE: 6 of 6	**REPLACES POLICY DATED:**
EFFECTIVE DATE: January 1, 2022	**REFERENCE NUMBER:** IP.DP.IN.017
APPROVED BY: Ethics and Compliance Policy Committee	

REFERENCES:

1. Indiana Code Title 24, Sections 4.9-1-1 to 4.9-4-2
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