Policy Title:	Privacy and Data Protection Policy	Document Number:	
Accountable Role:	Privacy Officer	**Governance:**	DHIN Management
Accountable Person:	Jeff Reger	**CEO Signature:**	Janice L Lee Janice L Lee (Sep 1, 2020 18:30 EDT)
Effective Date:	8/15/2020	**Document Review Period:**	Annual Sep 1, 2020
Communication Plan	Email, SharePoint, Annual Training	**Communication Period:**	Upon revision

Revision History

Name	***Date***	***Reason***
Elise Scheidel	7/22/2020	Draft for review.

Contents

I. Scope

This policy is applicable to all employees, participants and users of DHIN and its utilities. It contains Patient/Consumer Privacy Rights to which employees, users and member organizations shall uphold as agreed to in the DHIN End User Data Use Agreement and Business Associate Agreements. This policy provides references to regulations adhered to by DHIN for purposes of protecting individually identifiable data and protected health information.

II. Purpose

The purpose of this document is to provide policy and guidance for protecting patient data from unauthorized access and disclosure and enabling secure reliable access to individually identifiable information for healthcare treatment, payment or operations. Information about patient rights regarding the use and disclosure of their personal health information is also provided.

III. Statutory and Regulatory References

DHIN shall commit to conducting business in keeping with its core organizational values and established policies in compliance with all applicable laws and regulations. In particular, DHIN is committed to compliance with the regulatory requirements established by the Department of Health and Human Services under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) regarding the privacy of protected health information (PHI), also known as the "Privacy Rule" and all subsequent Privacy Rule updates, as well as all state-level regulatory compliance requirements that apply to its area of operations.

a. Federal Regulation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI).

b. State Statutes and Regulation

Title 16, Chapter 103 of the Delaware Code established the Delaware Health Information Network (DHIN) and requires DHIN to ensure the privacy and appropriate treatment of patient healthcare information. Pursuant to that statutory mandate and associated regulations, DHIN is required to disclose patient specific health information only in accordance with the patient’s consent or best interest to those having a need to know. In fulfilling this obligation, DHIN shall disclose patient specific health information only for Treatment, Payment and Operations purposes (as those terms are defined in HIPAA) to individuals and organizations that have an approved relationship with the patient, as required to comply with (or assist our Data Sending Organization Participants in complying with) directives from relevant law or in accordance with authorizations provided by the patient.

IV. Roles and Responsibilities

The CEO shall appoint a Privacy Officer who is a direct report to the CEO to be accountable for DHIN's individual Privacy and Data Protection Program. The Privacy Officer shall have expert knowledge of data protection law and practices and the ability to fulfill required tasks. [1]

V. Policy

a. Data Protection Applied to Covered Information

1. Handling Protected and Sensitive Information

DHIN shall explicitly identify and ensure the implementation of security and privacy protections for the transfer of organizational records, or extracts of such records, containing sensitive personal information to a state or federal agency or other regulatory body that lawfully collects such information.[2]

Where required by law, DHIN shall obtain consent from the individual prior to emailing, faxing, communicating by telephone or otherwise disclosing protected information (PII or PHI) about the individual to any external party. [3]

DHIN shall classify data according to its sensitivity and specify protections to be applied to that data type. *See* Data Classification and Document Management Policy.

DHIN shall ensure that data is retained and securely disposed of in accordance with legal and regulatory requirements, specific organizational needs and privacy practices. *See* Data Classification and Document Management Policy.

2. Protecting Data at Rest

To ensure data protection of covered information, DHIN shall at minimum, render the data unusable, unreadable, or indecipherable anywhere it is stored, which includes: personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs. Any exceptions to this policy shall require authorization by DHIN management and be documented.[4]

The information system must protect the confidentiality and integrity of information at rest. DHIN shall encrypt ePHI via current, generally accepted, encryption algorithms.

[1] 1901.06d1Organizational.1

[2] 1911.06d1Organizational.13

[3] 1902.06d1Organizational.2

[4] 1903.06d1Organizational.3456711

DHIN shall implement full-disk encryption wherever protected information is stored. Logical access shall be independent of O/S access and decryption keys shall not be tied to user accounts. If DHIN determines there is a situation where encryption will not be applied because it is not reasonable or appropriate, DHIN shall document its rationale for the decision or use alternative compensating controls other than encryption, provided the method is approved and reviewed annually by the Security Officer.

b. Patient/Consumer Privacy Rights

1. Public Information and Contacting the DHIN Privacy Officer

DHIN shall ensure that the public has access to information about its privacy activities and is able to communicate with its senior privacy official. Access to information shall be available through DHIN's website, and DHIN's Privacy Officer may be reached through the DHIN Service Desk. [5]

2. Notification from Data Contributing Organization Participants

DHIN data contributing organizations are contractually responsible to include information about DHIN within their notice of privacy practice (NPP) documentation to their patients/consumers, if such notices are required by relevant law. Content shall:

- Inform patients that they provide clinical results to the ordering provider through the agency of DHIN and that DHIN makes this information accessible to other healthcare organizations with appropriate rights to access data.
- Inform patients of their right to restrict access to their data held by DHIN. (See section Patient/Consumer Non-Disclosure.) DHIN shall make available to data contributing members the tools necessary to respond to patient inquiries about DHIN.
- Inform patients about electronic exchange of health information. Electronic exchange applies to delivery and query of information through DHIN for the purposes of treatment, payment or operations,
- Inform patients that DHIN patient/consumer information shall not be sold or disclosed for any activity that may support marketing to the individual; nor is individual information provided and/or used for mailing lists.

3. Inform patients of the permitted uses to which data may be put under the terms of contractual agreements between DHIN and Data Sending Organization DHIN Oversight of Data Contributing Organization Participant Notifications

When engaging in a new relationship with a data contributing organization that is a health care provider, DHIN shall review the data contributing organizations' Notice of Privacy Practice (NPP) for completeness and clarity of notification.

4. Audit Reporting for Patients/Consumers

DHIN shall ensure that patients/consumers are provided the means and opportunity to request an audit report that identifies which DHIN user(s) has accessed their individually

[5] 19134.05j1Organizational.5

identifiable health information through DHIN. Audit reports will not contain any personal health information. Specific procedures have been established to respond to requests for audit reports. DHIN shall retain requests for disclosure as organizational records for a period of six years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting. [6]

5. Disclosure Compliance with Law

DHIN shall ensure that disclosures remain consistent with all applicable federal and state laws and regulations and information shall not be used for any unlawful discriminatory purpose. Violations of privacy are subject to immediate termination of access to DHIN systems up to and including legal action in accordance with DHIN's policy and with all applicable federal and state laws and regulations. Pursuant to Title 16 § 10307, inappropriate access is a criminal offense subject to prosecution and penalties under the Delaware Criminal Code or federal law.

6. Patient/Consumer Non-Disclosure "Opt-Out"

Patients/consumers may request non-disclosure of their data through DHIN. This process is known as "Opting-Out". DHIN shall document restrictions in writing and retain a paper or an electronic copy of the request as an organizational record for a period of six years. 7

DHIN will enable Opt-Out requests with the following limitations:

- The patient cannot opt-out of DHIN being the contracted agent of the hospital, lab or other data contributing organization to deliver the result or report to the ordering provider.
- Nor can they opt-out of any reporting that is required by law or regulation such as immunizations or certain communicable diseases being reported to Public Health.
- Nor can they opt-out of their information being stored electronically in a database, as that is how business is conducted today. Their data remains in the DHIN data repository, but it is masked so that it is not discoverable upon query by a user of DHIN information systems
- The State of Delaware Newborn Screening Program enables an exception to DHIN's Opt-Out limitations for newborn screening combined metabolic and hearing results data. The Division of Public Health manages delivery or non-delivery of the results to DHIN per its patient/parental Refusal Form process.

[6] 1909.06c1Organizational.5

[7] 1907.06c1Organizational.3

7. Amendment of Data

In accordance with HIPAA, patients/consumers are provided the means to challenge and amend their individually identifiable health information. DHIN is a steward, not the owner, of the data in its repository. Any amendments to data must come from the source system of the data sender. Requests to amend data shall be made to the data contributing organizations; DHIN does not have the authority or access to amend individually identifiable health information. If a patient/consumer makes a request directly to DHIN to have their data amended, DHIN will facilitate placing the patient in contact with the appropriate individual in the data sending organization.

VI. Associated HITRUST CSF 9.3 Control Statements

Footnote	Baseline ID	Control Statement
1	1901.06d1Organizational.1	The organization has formally appointed a qualified data protection officer, reporting to senior management, and who is directly and fully responsible for the privacy of covered information.
2	1911.06d1Organizational.13	Records with sensitive personal information are protected during transfer to organizations lawfully collecting such information.
3	1902.06d1Organizational.2	When required, consent is obtained before any PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to the organization.
4	1903.06d1Organizational.3456711	The confidentiality and integrity of covered information at rest is protected using an encryption method appropriate to the medium where it is stored; where the organization chooses not to encrypt covered information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO.
5	19134.05j1Organizational.5	The public has access to information about the organization's security and privacy activities and is able to communicate with its senior security official and senior privacy official.
6	1909.06c1Organizational.5	The organization documents and maintains accountings of disclosure as organizational records for a period of six years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting.
7	1907.06c1Organizational.3	The organization documents restrictions in writing and formally maintains such writing, or an electronic copy of such writing, as an organizational record for a period of six years.