Policy: Access to Individually Identifiable Health Information

Policy Number: 0901 Original Effective Date: 03-17-2009	Current Revision Effective Date: 03-17-2011 Current Review Date: n/a

A. Background

A.1. The Delaware Health Information Network, (DHIN) is a public/private partnership created to facilitate the electronic exchange of health information between health care entities. DHIN provides fast, secure and reliable exchange of health information among health care facilities and clinicians across the state. DHIN is *not* a medical database or an electronic medical record. It is a mechanism to facilitate the movement and delivery of patient health information among those with a need to know. The design and implementation of DHIN include state-of-the-art security precautions to safeguard personal health information.

B. Purpose

B.1. The purpose of this policy is to:

B.1.1. Provide information about patients'/consumers' rights regarding the use and disclosure of their personal health information.

B.1.2. Maintain an appropriate level of security to protect patient data from unauthorized access and disclosure. This policy defines the access controls and parameters necessary to achieve this protection and to ensure the secure and reliable operation of DHIN.

C. Scope

C.1. This policy is applicable to all users and member organizations of DHIN. All users of DHIN, senders and receivers of data, have signed and agreed to the DHIN Data Use Agreement and Business Associate Agreement. This policy does not supersede or replace any Health Insurance Portability and Accountability Act (HIPAA) privacy and security policies in use by individual DHIN users and member organizations.

C.2. All participating DHIN hospitals' privacy policies have been reviewed and are inclusive of electronic exchange of health information. This applies to delivery and query of information through DHIN for the purposes of treatment, payment or operations/administrative actions.

D. Definitions

D.1. *Access Controls* – system level security that grants authorization to view personal health information in DHIN.

D.2. *Auditing* – the logging and monitoring of all system activity, including: user log-in identification, user name, user organization, date and time, patient account that was accessed, and type of records viewed by user.

D.3. *Health Care Provider*—health professionals licensed in Delaware with the authority to order or prescribe clinical tests and diagnostics, including physicians as defined by Title 18, Section 1861(r) of the Social Security Act, and clinical medical professionals who are licensed to diagnose and treat patients under the supervision of such physicians.

D.4. *Data Contributing Organizations* – those health care facilities that send clinical data (e.g. lab results) to health care providers/clinicians through DHIN.

D.5. *Users* – those who enroll in DHIN to receive clinical results and reports. DHIN users are clinicians and their designated staff, who must agree to maintain the privacy and security of the information they obtain from DHIN. DHIN users receive clinical results and reports free of charge and, when available, may also query DHIN for clinical history.

D.6. *Member Organizations* – those who are sending data into the health information exchange as well as those who benefit from the system, such as health plans and employers. Member Organizations have a responsibility to DHIN both financially as well as to ensure accurate delivery of data into the system for consumption by DHIN users for the delivery of clinical care.

D.7. *User Roles* – rules defined by DHIN and assigned to users, determining an individuals' level of access to personal health information through DHIN.

D.8. *User Authentication* – requirements for users to gain authorized access to the DHIN application.

D.9. *Query* – allows an authorized user who has an established relationship with a patient to search for clinical information for that patient available through DHIN on a need to know basis.

D.10. *Expanded Query Access* – allows a user to temporarily extend their access rights under defined parameters to view clinical information available through DHIN on a need to know basis.

D.11. *Need to Know* – in order to safeguard patient/consumer privacy, DHIN users shall receive access only to the minimum functions and privileges required for performing their jobs.

D.12. *Individually Identifiable Health Information* –a subset of health information, including demographic data and past, present, or future health condition information collected from an individual that is created or received by a health care provider participating in DHIN.

D.13. *HIPAA* – the Health Insurance Portability and Accountability Act (HIPAA) designed to help protect privacy of a patient/consumer's protected health information

E. Patient/Consumer Privacy

E.1. **Notice to Patient/Consumers Regarding DHIN**

E.1.1. Patient/consumer privacy is of critical importance. DHIN complies with state and federal laws, including HIPAA, as applicable. With the assistance of Delaware's privacy officers, hospitals, legal counsel and the DHIN consumer advisory committee, DHIN has established a policy that considers the patients' rights and expectations while balancing the need for health care providers to have information that enables them to make informed decisions and ultimately provide better quality health care services.

E.1.2. DHIN users shall implement appropriate procedures to (1) inform patients that they use DHIN, and (2) inform patients of their right to non-participation in DHIN.

E.1.3. DHIN shall make available to users tools necessary to respond to patient inquiries about DHIN.

E.2. **Uses and Disclosures of Individually Identifiable Health Information**

E.2.1. Disclosure of Individually Identifiable Health Information. DHIN patient/consumer information is not sold or disclosed for any activity that may support marketing to the individual nor is individual information provided and/or used for mailing lists.

E.2.2. Query Access. Only users enrolled in DHIN who have an established relationship with a patient will have access to that patient's information available through DHIN. Emergency care personnel will have access to DHIN whereby they can access patient records in emergency care situations on a need to know basis.

E.2.3. Expanded Query Access. Users may expand their access to patient information by requesting to establish a relationship with a patient in DHIN. Users are required to log a reason for the relationship and set a defined time period for access, not to exceed six (6) months. Refer to the Expanded Query Access (Section F.6) for specific details related to this function.

E.2.4. Audit Reporting. Patients/consumers are provided the means and opportunity to request an audit report that identifies which DHIN user(s) has accessed their individually identifiable health information through DHIN. Audit reports will not contain any personal health information. Specific procedures shall be established to respond to requests for audit reports.

E.2.5. Compliance with Law. All disclosures of individually identifiable health information through DHIN and the use of such information obtained from users of DHIN shall be consistent with all applicable federal and state laws and regulations and shall not be used for any unlawful discriminatory purpose. Violations of privacy are subject to immediate termination of access to DHIN up to and including legal action in accordance with DHIN's privacy policy and with all applicable federal and state laws and regulations. Pursuant to the DHIN Statute, inappropriate access is a criminal offense that could be a Class D felony punishable by eight (8) years imprisonment, fines and penalties for each offense.

E.3. **Patient/Consumer Non-Participation**

E.3.1. Patients/consumers may decide not to participate in DHIN.

E.3.2. Non-participation will result in personally identifiable health information not being available to users (including emergency personnel) upon a query or expanded query.

E.3.3. Patients/consumers may choose to participate in the system again at any time.

E.3.4. DHIN will develop specific procedures to process non-participation requests, as well as requests to begin participating again.

E.3.5. Users should adopt procedures for notifying DHIN of requests from patients/consumers not to participate. DHIN shall respond in a timely manner and according to the procedures that are established.

E.4. **Amendment of Data**

E.4.1. In accordance with HIPAA, patients/consumers are provided the means to challenge and amend their individually identifiable health information. 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.

F. Information Security

F.1. **Access Controls**

F.1.1. Only authorized users are granted access to DHIN, and users are limited to specifically defined, documented and approved levels of access rights.

F.1.2. Access control to DHIN is achieved via identifiers that are unique to each user and provide individual accountability and enable tracking.

F.1.3. Access rights are based on user roles and job responsibilities. The health care provider enrolled in DHIN is responsible for creating staff accounts and assigning user roles to those who work for them. Users should be granted access to information on a need to know basis. That is, users should only receive access to the minimum functions and privileges required for performing their jobs.

F.1.4. Users will be required to acknowledge and accept the Terms and Conditions of Use statement prior to logging into the application.

F.1.5. Users will be held responsible for all actions conducted under their sign-on.

F.1.6. Any user accessing the DHIN application must be authenticated. The level of authentication will correspond appropriately to the designated access rights.

F.1.7. When a user is inactive for a period of time, defined by DHIN and consistent with HIPAA, the application will automatically time-out. Users will then be required to log on again to continue usage. This minimizes the opportunity for unauthorized

users to assume the privileges of the intended user during the authorized user's absence.

F.2. **User Authentication**

F.2.1. To obtain access to the DHIN application, an authorized user must enter his/her unique user identification and supply an individual user password.

F.2.2. To obtain a new password from DHIN, users must be able to provide the answers to unique questions selected and answered by the user at the time of set-up.

F.2.3. All users will be required and prompted to change their passwords at a time interval defined by DHIN and consistent with HIPAA.

F.2.4. Passwords must be promptly changed if it is suspected of being disclosed to unauthorized parties.

F.2.5. At the time a user is no longer associated with or employed by a member organization, the member organization is required to terminate the user's access to DHIN.

F.3. **User Roles**

F.3.1. DHIN will define, document and maintain user roles created in the application and establish a process for periodic review.

F.4. **Access Rights**

F.4.1. Users will be defaulted to have access only to their organization's data. Only pre-defined and approved users will be allowed to obtain expanded access to individually identifiable health information through DHIN.

F.4.2. Expanded Query Access is an access level that enables a user to temporarily expand their standard security rights to view patient information available through DHIN on a need to know basis. Refer to Section F.6 "Expanded Query Access" for information specific to this function.

F.5. **Audit Controls**

F.5.1. DHIN logs and monitors all system activity, including: user log-in identification, user name, user organization, date and time, patient account that was accessed, and type of records viewed by user. Audit reports do not contain personal health information.

F.5.2. DHIN shall audit access to individually identifiable health information on a regular and scheduled basis to ensure appropriate use of the system. Procedures shall be established to define this process.

F.5.3. Patients/consumers are provided the means and opportunity to request an audit report of who has accessed their health information through DHIN. DHIN shall establish specific procedures to respond to patient requests for audit reports in a timely manner.

F.6. **Expanded Query Access**

F.6.1. User Requirements

F6.1.1. The right of a user to obtain expanded query access is established by the DHIN user roles.

F6.1.2. If expanded query is utilized, the user must indicate a reason, from a pre-populated list of options, as to why they have expanded their access rights.

F6.1.3. Each time expanded query is utilized, the user must also indicate the period of time in which they need to have access to the patient's data, from one time to a period of time not to exceed six (6) months.

F.6.2. Auditing

F6.2.1. DHIN logs and monitors all expanded query access activity, including: user log-in identification, user name, user organization, date and time, patient account that was accessed, the reason the user utilized expanded query, time period for which access was established, and the type of records viewed by user.

F6.2.2. Patients/consumers are provided the means and opportunity to request an audit report of who has accessed their health information through DHIN, including utilization of expanded query. Audit reports do not contain personal health information. DHIN shall establish specific procedures to respond to patient requests for audit reports in a timely manner.