At Delaware Health Information Network (DHIN), data is our business. With cyber threats and the organized targeting of healthcare data on the rise, the safety and security of that patient data is paramount.

Protecting this data requires a multi-pronged approach, consisting of physical, procedural and legal safeguards, as well as a “toothy” enforcement policy.

**Federal and State Regulations**

Key to DHIN’s data protection policies and procedures is the Health Insurance Portability & Accountability Act (HIPAA), which mandates that DHIN applies policy, procedure and annual assessments to fulfill obligations as a Business Associate to Covered Entities.

Additionally, DHIN adheres to requirements put forth by the National Institutes of Standards and Technology, as well as other applicable federal and state laws and regulations.

These regulations govern DHIN’s legal and procedural protections of PHI.

**Privacy and Security Program**

A cybersecurity plan is only as good as an organization’s ability to execute it. A comprehensive program for safeguarding DHIN’s data – and responding to threats - is key to our ability to protect it.

*Risk assessments and continuous improvement*

As the sanctioned provider of health information exchange for the State of Delaware, DHIN provides safeguards for PHI as the Business Associate for Delaware’s covered entities receiving information exchange services from DHIN.

This responsibility includes annual risk assessments, which alternate between external and internal reviews, with the goal of identifying risks and vulnerabilities.

DHIN responds to assessment findings with remediation and corrective action plans, as needed, and employs an employee education and awareness program for continuous improvement activities.

*Risk management – system design, access constraints, system reviews and user audits*

DHIN is required to implement and maintain appropriate safeguards to protect the health information we receive on behalf of Covered Entities and to prevent its unauthorized use or disclosure. Risk management includes:

1. Organizational safeguards, designed to prevent conflict of interest and to detect control failures

DHIN is required to keep updated organizational charts and job descriptions, with auditing responsibilities assigned to those independent of the audited tasks

1. User audits

DHIN routinely audits user access to our systems, both those with and without individually identifiable health information. Audit logs are stored for at least three years, per records retention schedules, and meet both State and HIPAA regulations for information contained therein.

Additionally, all DHIN users are notified that our systems are monitored, and disclosure reporting expectations are shared with DHIN’s Business Associates and Covered Entities, as well.

*Enforcement*

DHIN employs a formal sanctions process for personnel who fail to comply with information security policies and procedures. Each DHIN employee is required to read, acknowledge and comply with DHIN’s privacy, security and data access to PHI expectations. Violations are sanctioned accordingly, up to and including criminal charges.

**Privacy and Security Components**

Perhaps most critical to DHIN’s data protection efforts are the components that impact DHIN’s operations as a health information exchange.

*Policy and Procedure Documentation*

DHIN follows a comprehensive set of policies and procedures designed to safeguard patient data. These are reviewed annually and approved versions made available to all employees and contractors.

*Employee Privacy and Security Education Oversight*

Employee education and oversight is key to a privacy and security program. Each employee and contractor is responsible for reviewing and acknowledging DHIN’s policies and procedures related to protection of data.

*Technology Software/Hardware Maintenance*

The information technology business requires that DHIN’s technology partners and solutions meet the privacy and security requirements outlined above. Maintaining software and hardware technology includes embedded secure coding, with thorough testing protocols and defined change control.

External protections include encryption, anti-viral and anti-spyware monitoring. Multi-factor authentication is required for all external connections to DHIN’s network, and access to the internal network is restricted.

DHIN’s asset management inventory provides a comprehensive view of all software and hardware components, whether maintained by DHIN or its subcontractors.

*Business Associates Oversight*

Oversight of DHIN’s subcontractors is an expectation of privacy and security management. DHIN’s subcontractors are held to the same standards for protection of patient data as DHIN. Specialized agreements are put in place prior to DHIN granting access to data and are monitored and enforced by DHIN executive management.

*DHIN Information Systems User Oversight*

As outlined above, each Business Associate is required to sign a Data Use Agreement prior to accessing DHIN data. The agreement specifies user account management protocols, registration and de-registration and password management. Again, these agreements are monitored and enforced by DHIN executive management.

*Business Continuity / Disaster Recovery*

Data delivery timeliness and the ability to recover from disaster are critical to DHIN’s ability to serve as Delaware’s health information exchange. As such, DHIN developed and routinely tests our business continuity and disaster recovery plans, knowing that our services are imperative to the delivery of healthcare in the state.

*Data Classification and Document Management*

Classifying data is the first step to determining application of security levels and access controls. Once data is classified, document handling procedures, records retention and safeguard controls follow. DHIN’s data classification and management policies follow federal guidelines and requirements.

*Physical Environment*

Today’s physical environment is more than just an office – remote offices, shared equipment and even supplies like printers are factored into security controls. 24/7 badge access, security system and monitored reception area are present at DHIN’s main office, with additional safeguards in place for remote access.

Because safety never takes a holiday, as the saying goes, DHIN is ever-vigilant with monitoring cybersecurity threats and assessing our ability to both prevent and react to a threat.