1801 Market Street, Suite 750 Philadelphia PA, 19103 www.hsxsepa.org

Glossary

Version	Approval Date	Owner
1.4	April 19, 2018	President

Disclaimer: Terms that are not specifically defined shall have the meanings ascribed to such terms in HIPAA and/or HITECH, as the case may be. Regulatory provisions are not copied or paraphrased in order to avoid conflicts or ambiguity of terms that are already legally-defined under HIPAA, HITECH or their corresponding regulations. If any term conflicts with legal definitions under HIPAA and/or HITECH, the definition ascribed to such term under the applicable law shall prevail.

A

Access Control is a formal, documented, and auditable method (whether administrative or technical in nature) for controlling access to an Information Asset. Access Control ensures that resources are only granted to those Users who are entitled to them.

Account is the bundle of access rights and privileges granted to a User, Computing Device, or System governing access to, and use of, an Information Asset.

Account Administrators are an individual, or group of individuals, who have delegated authority to act on an Information Asset Owner's behalf to administer access rights and privileges associated with an Information Asset.

Account Owner is an individual, or group of individuals, who have been officially designated as accountable for controlling access to an Information Asset. Account Owners are associated with the business functions of HSX rather than the technology functions. Account Owners are appointed by senior leadership and are typically an administrative officer or department director.

Accountable Care Organization (ACO) is a healthcare organization formed from a group of coordinated health care practitioners that ties payments to quality metrics and the cost of care. The ACO is accountable to patients and third-party payers for the quality, appropriateness and efficiency of its services. According to the Centers for Medicare & Medicaid Services (CMS) ACOs are groups of doctors, hospitals, and other health care providers, who come together voluntarily to give coordinated high-quality care to their Medicare patients. The goal of coordinated care is to ensure that patients, especially the

chronically ill, get the right care at the right time, while avoiding unnecessary duplication of services and preventing medical errors.

Admission Discharge Transfer (ADT) carry pertinent patient information that contribute to electronic clinical records. ADT systems can also be used as an alert system upon a patient's admission.

Adverse Events are Events with negative consequences (e.g., system crashes, packet floods, unauthorized use of system privileges, unauthorized access to sensitive data, execution of malware that destroys data, etc.).

Advanced Encryption Standard (**AES**) is a cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192 or 256 bits.

Aggregate Data pertaining to groups of individuals that are by definition already De-Identified. Data that are tabulated to provide information on the number of patients/members in various groups or categories, without providing individual-level information, are considered aggregate data. Aggregate Data cells must contain a sample size of more than 5 people in order to be considered to be De-Identified Data.

Thus, an example of Aggregate Data is displayed below: A Count of Patients' Primary Diagnoses by Age

	Primary Diagnosis		
Age Group	**Diabetes**	**Hypertension**	**Asthma**
20-20 years	100	200	300
30-39 years	150	250	350
40-49 years	200	300	400

American Recovery and Reinvestment Act of 2009 (ARRA) is commonly referred to as the "stimulus" bill or the "Recovery Act," it was signed into law by the President on 2/17/09. This included the enactment of the Health Information Technology for Economic and Clinical Health Act. This is unrelated to the Affordable Care Act.

Anti-Malware Software provides protective safeguards against Malware attacks.

Application is a software program that stores, accesses, and/or manipulates data or which controls a Computing Device or System.

Application Owner is an individual, or group of individuals, who have been officially designated as having management responsibility for controlling the production, development, maintenance, use and security of an Application.

Application Service is any service or function carried out to support, provision, administer, and or provide training for an Application.

Approval is the Patient's signed acknowledgment of receipt of a Health Care Provider's HIPAA Notice of Privacy Practices setting forth permissible uses and disclosures of the Patient's PHI, unless and until the Patient opts-out of the HSX HIE.

Asset see Information Asset.

Asset Inventory see Information Asset Inventory.

Asset Owner see Information Asset Owner.

Authentication is the process of confirming the correctness of the claimed identity.

Audit is an examination of the management controls within the IT infrastructure.

Audit Controls are mechanisms employed to record and examine system activity.

Auditable Events are those Events that can be tracked.

Audit Records are individual items of information in an audit trail.

Audit Trail is a record of changes. An audit trail identifies who (login) did what (create, read, modify, delete, add, etc.) to what (data) and when (date, time). An Audit Trail can potentially facilitate an internal or external audit. Audit Trail data may consist of several Audit Records.

Auditing is the process of reviewing system and User access logs to assess the appropriateness of a User's activities.

Authorized User means an individual who is also a registered Participant, or an individual designated by a Participant to use the Services *on behalf of* an approved and authorized Participant

Automated Care Team Finder (ACTF) is part of HSX's Enhanced Discharge Information case and uses payer information to identify patient's primary care providers.

B

Backup is the procedure for making copies of information in case the original information is lost or damaged.

Breach shall have the meaning given under 42 U.S.C. § 17921(1) and 45 C.F.R. § 164.402.

Business Associate is an entity or a person who is not an employee of HSX and who, on behalf of HSX, creates, receives, maintains or transmits PHI.

Business Associate Agreement (BAA) is a legally mandated agreement entered into between HSX and a Business Associate that establishes permitted and required uses and disclosures of PHI, provides obligations for the Business Associate to safeguard the

information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Business Continuity refers to the activities required to maintain vital HSX operations at an acceptable level of effectiveness and efficiency during a period of displacement or interruption of normal operations.

Business Continuity Plan (BCP) provides processes and procedures for continuing business operations under adverse conditions (e.g., storm, crime, emergency, disaster, etc.). From an IT perspective, the BCP should cover at a minimum the following events:

- Equipment failure (such as disk crash)
- Disruption of power supply or telecommunications
- Application failure or corruption of database
- Human error, sabotage or strike
- Malicious software (e.g., viruses, worms, Trojan horses) attacks
- Hacking or other security attacks
- Social unrest or terrorist attacks
- Fire
- Natural disasters (e.g., flood, earthquake, hurricanes)

Business Mobile Computing Devices are Mobile Computing Devices that are the property of HSX and are provided to support the operations of HSX. Business Mobile Computing Devices are managed by HSX and all Data they access, transmit and store is subject to audit, monitoring, and logging by HSX.

C

Certificate Authorities are entities that issue digital certificates certifying the ownership of a public key by the named subject of the certificate.

Change is defined as any addition, deletion, or alteration of any hardware, software, Network, telephony, environment, System, desktop build, or associated documentation in the HSX IT infrastructure.

Change control is **a** formal planning process to make sure only necessary changes are authorized, made, and recorded.

Change Control Board (CCB) is a group of individuals who review Change Requests and decide whether to implement the change.

Change Management is the identification and implementation of Changes to hardware, software, firmware, and documentation. Change Management workflows ensure that changes are made with minimum disruption to the organization.

Change Management Roles ensure clear ownership of the Change Management process. Change Management Roles are generic and describe Change Management responsibilities. The roles do not necessarily conform to the job titles in the organizational chart. In addition, one person might fill several roles while another role might require several people. Further, the people fulfilling the roles might be different during an Emergency.

Change Request is a formal written request for Change to any component of the HSX IT infrastructure or to any aspect of an IT service in the HSX production environment.

Chief Information Security Officer (CISO) is the most senior person in the organization responsible for establishing and maintaining the enterprise vision, strategy and programs to ensure Information Assets and technologies are adequately protected.

Clinical Activity History (CAH) is designed to pull claims clinical history Data from participating health plans claims databases for patients presenting to different care settings (e.g., hospital emergency department) leveraging ADT messages through secure methods.

Clinical Data Repository or **CDR** is designed to persist Data such as lab results, radiology reports, transcribed documents, CCD/C-CCDA's and ADT's and Clinical Activity History Summary's received from Data Supplier and Data Exchangers, including Participant. Such persisted Data will remain in the CDR subject to access and query by Data Viewers and Data Exchangers pursuant to HSX Policies and HSX approved Use Cases.

Computing Devices are the computers, Business Mobile Computing Devices, printers, Networks, online and offline storage Media and related equipment, software, and Information Assets that are owned, managed, or maintained by HSX.

Computer Security Incident Response Capability (CSIRC) see Information Security Incident Response Capability.

Confidential Data is the most restricted type of HSX sensitive Data. Confidential Data includes PHI, Social Security numbers (SSN), and personally identifiable information (PII). The full list of Confidential Data is defined in the *Data Classification Policy*.

Confidential HIV-Related Information or simply "HIV-Related Information" shall mean "any information which is in the possession of a person who provides one or more health or social services or who obtains the information pursuant to a release of confidential HIV-related information and which concerns whether an individual has been the subject of an HIV-related test, or has HIV, HIV-related illness or AIDS; or any information which identifies or reasonably could identify an individual as having one or more of these conditions, including information pertaining to the individual's contacts", as is defined in 35 P.S. 7603.

Configuration Management is the process for evaluating, coordinating, approving, disapproving, and implementing Changes to the approved operational baseline for information systems.

Contingency Plans provide the procedures necessary for recovering the operation of all or part of information systems at an existing or new location in an Emergency. See Information System Contingency Plans (ISCP).

Continuity of Care Document (CCD) and Continuity of Care Document Architecture (C-CDA) is a standardized document structured around certain technical specifications. This document is comprised of several sections, which give a snapshot of a patient's clinical information.

Continuity of Operations Plan (COOP) provides procedures and information for sustaining mission-critical business operations at an alternate site for an extended period of time. The COOP may be supported by multiple information system Contingency Plans that address recovery of impacted individual Systems once the alternate facility has been established. The COOP only addresses information system disruptions that require relocation.

Coordination or Management of Healthcare as contained in the definition of Treatment below, means the following activities which emphasize prevention, continuity of care and coordination of care on behalf of an individual patient or member to help ensure an individual patient or member receives services in a timely manner: (i) identification of special needs that a patient or member has or may have; (ii) assessment of a patient's or member's risk factors; (iii) development of a plan of care for the patient or member; (iv) referrals and assistance to a patient or member to ensure timely access to a Provider; (v) monitoring the provision of services in a patient's or member's plan of care; (vi) assisting the patient or member to ensure continuity of care; or (vii) follow up and documentation with respect to that patient or member.

Covered Entity is a

Health Plan is an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2))

Health Care Clearinghouse is a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and value-added networks and switches, that does either of the following functions:
(1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
(2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care provider means a provider of services (as defined in section 1861 of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of

the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. Who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

A Health Care Provider	A Health Plan	A Health Care Clearinghouse
This includes providers such as: • Doctors • Clinics • Psychologists • Dentists • Chiropractors • Nursing Homes • Pharmacies ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.	This includes: • Health insurance companies • HMOs • Company health plans • Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans' health care programs	This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

Credentialing is the process of assessing and confirming the qualifications of a licensed or certified health care practitioner.

Crisis Communications Plan provides procedures and information for internal and external communications in the event of a disruption. The Crisis Communications Plan also designates the specific individuals who are the only individuals with the authority for providing information to the public and answering questions.

Critical Infrastructure Protection Plan (CIP) provides procedures and information for protecting critical infrastructure components by mitigating risks and vulnerabilities.

Cross-Community Access Standard (XCA) is a method of sharing documents, within a network, across health information organizations.

Cross- Enterprise Document Sharing Registry (XDS) is a centralized system within a health information organization for maintaining information about the contents and location of a clinical document.

Cross-Enterprise Reliable Interchange (XDR) is a technical specification for Direct messaging.

Cyber Incident Response Plan provides procedures and information for identifying, mitigating, and recovering from a malicious Security Incident (e.g., unauthorized access, denial of service, virus, worm, Trojan horse, etc.).

D

Data means information provided to or through the HSX Network, including IIHI, PHI and ePHI.

Data Classification, in the context of information security, is the classification of Data based on its value, legal requirements, sensitivity, and criticality. The classification of Data helps determine what baseline security controls are appropriate for safeguarding that Data.

Data Disclosure is the sharing of Data, including PHI, outside of the HSX work force or affiliated covered entities. There are specific policies regarding Data Disclosure based on the classification of that Data, including the requirement for tracking who has seen, or is capable of seeing, specific Data elements.

Data Exchange means electronically providing or accessing Data through the HSX HIE.

Data Exchanger means a Participant that is both a Data Supplier and Data Receiver and may access Data from the HSX Network.

Data Mining is the accessing, obtaining, viewing, using of data in order to manipulate the same for competitive business intelligence, or some other personal business benefit

Data Misuse shall mean the unauthorized acquisition, access, use or disclosure of Data by a Participant or Authorized User in a manner inconsistent with the Use Cases, the Permitted purposes and/or the HSX Policies. The term "Data Misuse" does not include a Breach or Security Incident described in the Business Associate Agreement (BAA).

Data Owner is an individual, or group of individuals, who have been officially designated as accountable for specific Data that is transmitted, used, and stored on a System or Systems. Data Owners are associated with the business functions of HSX rather than the technology functions. Data Owners are appointed by senior leadership, and are typically an administrative officer or department director.

Data Receiver is an organization, such as a hospital, physician practice, clinical laboratory, pharmacy, governmental agency or other entity, that has entered into an agreement allowing them to receive Data that is Pushed through the HSX HIE and into such Data Receiver's electronic medical record (EMR) or other similar Data-collection repository, or is specifically made available to such Data Receiver for limited viewing. A Data Receiver also may, but is not required to be, a Data Supplier.

Data Sharer is an organization, such as a hospital, physician practice or other eligible entity, that has entered into a Participation Agreement (or an equivalent) and will, in accordance with the terms of such agreement and all applicable laws, make Data maintained in such Data Sharer's EMR available for access by other Participants through the HSX HIE and also has the authority to access and Pull Data from the HSX HIE that is made available by other Participants.

Data Supplier is an organization, such as a hospital, physician practice, clinical laboratory, pharmacy claims aggregation company, governmental agency or other entity, that has entered into a Participation Agreement (or an equivalent) and will, in accordance with the terms of such agreement, and all applicable laws, transmit Data to the HSX HIE and make it available for access by authorized Participants through the HSX HIE. A Data Supplier may also be a Data Receiver; however, a Data Supplier shall not have authority to fully access and Pull other Participant's Data through the HSX HIE, unless such Participant is registered as a full Data Sharer.

Data Use and Reciprocal Support Agreement (DURSA) is a comprehensive, multi-party trust agreement that is entered into voluntarily by public and private organizations (eHealth Exchange Participants) that desire to engage in electronic health information exchange with each other as part of the eHealth Exchange.

Data User see User.

De-Identified Data can be De-Identified one of two different ways:

1. The Safe Harbor Method of De-Identification, which removes the 18 identifiers as listed. In reference to zip code, the first three digits of the zip code may be provided if the geographic unit formed by the combining the zip code with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code the geographic units containing 20,000 or fewer people is changed to 000 (See Reference Section #1).

OR

2. The Expert Determination Method where HSX will apply the appropriate statistical or scientific principles to ensure that the information is not individually identifiable. The application of The Expert Determination Method ensures the risk of the information being used alone or in combination with other reasonably available information by an anticipated recipient to identify an individual who is a subject of the information is very small. HSX will document the methods and results of the analysis that justify such determination (See Reference Section #1). HSX will use the techniques to de-identify and reduce the probability to re-identify Data as per the

Office for Civil Right's Guidance for the De-identification of Protected Health Information and https://www.ncbi.nlm.nih.gov/books/NBK285994/.

Demilitarized Zone (DMZ) is a physical or logical sub Network that sits between the internal and external Network, usually the Internet. DMZs provide sub Network segmentation based on security requirements or policy. DMZs provide a transit mechanism from a secure source to an insecure destination or from an insecure source to a more secure destination.

Demographic Information includes name, address and dates of service.

Designated Record Set is a group of records maintained by or for a covered entity that is:

- The medical records and billing records about individuals maintained by or for a covered health care provider;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Used, in whole or in part, by or for the covered entity to make decisions about individuals.

The term **record** means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a covered entity.

Differential Backup is a cumulative Backup of all changes made since the last Full Backup, i.e., the differences since the last Full Backup. The advantage is a quicker recovery time, requiring only a Full Backup and the last Differential Backup to restore the entire Data repository.

Direct, Direct Secure Messaging or **DSM** is designed to allow authorized Participants to send or receive encrypted health information which may include Data directly to or from known, trusted recipients using the direct specifications promulgated by the Office of the National Coordinator of Health Information Technology, from time to time.

Direct Trust is a non-profit and self-regulatory entity created to help implement best practices and rules needed to securely send Direct messages between its members. Currently, the Direct Trust network serves over 33,000 healthcare organizations.

Disaster is a sudden Event, such as an accident or a natural catastrophe, which causes great damage or loss of life.

Disaster Recovery is the process of rebuilding operations and infrastructure after the Disaster is over.

Disaster Recovery Plan (DRP) covers physical disruptions to service that deny access to the primary infrastructure for an extended period of time. The DRP includes procedures for establishing operations at an alternate site during an Emergency. The DRP is supported by

multiple Contingency Plans that address recovery of individual Systems at the alternate site.

Discharge Information is designed to permit Participant hospitals to send a continuity of care document with discharge information from their electronic health record to patient's primary care provider and health plan using secure methods. An enhancement to the Discharge Information Use Case is the Automated Care Team Finder ("ACTF"). ACTF is designed to leverage Participant health plans databases to assist with identifying a patient's primary care provider through Participant hospitals sending an ADT message with a discharge method to HSX which sends these to the patient's participating health plan. The participating health plan sends back information designating the primary care provider based upon their attribution model. HSX routes the discharge information to the primary care provider.

Disclosure is the release, transfer, access, or divulging of PHI in any manner outside of the entity holding the information.

Domain Name System (DNS) is a system for naming computers and Network services that is organized into a hierarchy of domains. DNS naming is used in TCP/IP Networks, such as the Internet, to locate and identify computers and services through user-friendly names.

E

Electronic Healthcare Network Accreditation Commission (EHNAC) is an independent organization that promotes accreditation in the healthcare industry. This organization aims to achieve quality and trust for healthcare information exchange through adoption and implementation of standards.

Electronic Health Record (EHR) is the Patient's collective or aggregated record of information comprised of information in separate EMRs maintained by multiple Health Care Providers.

Electronic Medical Record (EMR) is an electronic system used to enter, maintain and store patient clinical information, including such information as required under applicable state law and federal regulations, and maintained by a single Health Care Provider who, for purposes of these HSX HIE Policies, is a Participant in the HSX HIE.

Electronic Media see Media.

Electronic PHI (ePHI) means PHI that is transmitted by or maintained in electronic media.

Emergency is a serious, unexpected, and often dangerous situation requiring immediate action.

Emergency Change typically occurs during a Security Incident and requires an immediate response to mitigate a production System outage. Emergency Changes must be done in accordance with the Incident Response Plan.

Emergency Operations Plan (EOP) is the document that describes the response to a situation that has overwhelmed, or may overwhelm, the ability to provide services. Communications, Incident Command, Clinical Activities and Capacity Management, Resources and Assets, Staffing, Safety, Security and Utilities responses are included.

Emergency Plan (EP) provides coordinated first-response procedures for minimizing loss of life and injury in the event of a physical threat (e.g., fire, bomb threat, chemical release, domestic violence, medical emergency, etc.). The EP includes procedures for sheltering-in-place as well as evacuating.

Encounter Notification Services (ENS) is designed to provide a list of real-time patient encounters to participants via secure methods. HSX will receive ADT messages from applicable HSX Data Exchangers or Suppliers when patients are admitted, discharged or transferred from a Participant hospital or other care setting. HSX will generate a real time encounter notification alerting subscripting Participants of such admission, discharge or transfer for their patients or members.

Encryption is the process of encoding information in such a way that only authorized parties can read it. Encryption does not of itself prevent interception, but denies the message content to the interceptor.

Enterprise Data is any information that is created or used as part of HSX's operations. Enterprise Data is further classified based on its value, legal requirements, sensitivity, and criticality to the organization.

Event is an observable occurrence in a System or Network (e.g., user connects to file share, server receives request for web page, user sends email, firewall blocks connection attempt).

External Audit is a review of the records of system activity performed by an entity not owned by or affiliated with the same entity using the system being reviewed.

External Networks shall mean statewide, nationwide or other health information exchange networks, including but not limited to the PA Patient and Provider Network (P3N) (defined in § 3.4) which enables the secure exchange of health information among authorized parties, all in accordance with the HSX Policies.

F

False Positive is an alert that incorrectly indicates that malicious activity is occurring.

Firewall is a logical or physical part of a computer System or Network that is designed to block unauthorized access to Data.

Founding Member shall mean each one of the Founding Hospital/HealthSystem Members and Founding Health Plan Members that have executed the founding member Participation Agreement

Full Backup is a complete Backup of everything. The advantage is fast restoration since you only need one set of Backup Data. The disadvantage is that the Backup process is slow and requires significant storage capacity.

G

Governance relates to processes and decisions that seek to define actions, grant power and verify performance.

H

Health Care Operations (HCO) of a Covered Entity, provided that if the Covered Entity is requesting or accessing Protected Health Information of another Covered Entity in order to perform its own HCO then (i) the requesting Covered Entity has an established Treatment relationship with the individual who is the subject of the Protected Health Information; (ii) the purpose of the request is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance; and (iii) the Covered Entity's Authorized User is requesting the Protected Health Information for its Covered Entity's own use.

Healthcare Provider as defined by state law [Pennsylvania eHealth Information Technology Act] is a person licensed by the Commonwealth to provide healthcare or professional clinical services. This term includes:

- A healthcare practitioner, as defined in Section 103 of the Act of July 19, 1979 (P.L.130, No.48), known as the Health Care Facilities Act.
- A healthcare provider, as defined in Section 103 of the Health Care Facilities Act.
- A public health authority.
- A pharmacy.
- A laboratory.
- A person that provides items or services described in Section 1861(s) of the Social Security Act (49 Stat. 620, 42 U.S.C. 1395x(s)).
- A provider of services, as defined in Section 1861(u) of the Social Security Act (49 Stat. 620, 42 U.S.C. 1395x(u)).

In connection with the HSX HIE, the Health Care Provider will be either a Data Supplier or Data Receiver (or both), or a Data Sharer, as well as a Participant (at entity-level) or Authorized User (at user-level).

Health Information Exchange (HIE) is an interoperable system that electronically moves and exchanges PHI between approved participating Healthcare Providers or health information organizations in a manner that ensures the secure exchange of PHI to provide care to patients.

Health Information Organization (HIO) brings together healthcare stakeholders within a defined geographic area and governs eHIE among them for the purpose of improving healthcare in that community.

Health Information Service Provider (HISP) is an organization that manages security and transport for health information exchange among healthcare entities or individuals using the DIRECT standard for transport. HSX provides services for some of its members.

Health Information Technology for Economic and Clinical Health (HITECH) set meaningful use of interoperable EHR adoption in the health care system as a critical national goal and incentivized EHR adoption. The "goal is not adoption alone but 'meaningful use' of EHRs — that is, their use by providers to achieve significant improvements in care."

Health Insurance Portability and Accountability Act (HIPAA) is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) collectively with the Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Part 160 and Part 164, Subpart E (Privacy Rule), and the HIPAA Security Standards, 45 C.F.R. Part 160 and Part 164, Subpart C (Security Rule), as amended by the Health Information Technology for Economic and Clinical Health Act and regulations promulgated thereunder (collectively, "HITECH"). The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information, and help the healthcare industry control administrative costs.

Health Level Seven International (HL7) is a not-for-profit standards developing organization which provides a secure framework for the exchange, integration, sharing and retrieval of electronic health information.

Healthcare Operations (HCO) of a Covered Entity, provided that if the Covered Entity is requesting or accessing Protected Health Information of another Covered Entity in order to perform its own HCO then (i) the requesting Covered Entity has an established Treatment relationship with the individual who is the subject of the Protected Health Information; (ii) the purpose of the request is for those Health Care Operations listed in paragraphs (1) or (2) of the definition of Health Care Operations in 45 C.F.R. § 164.501 or health care fraud and abuse detection or compliance; and (iii) the Covered Entity's Authorized User is requesting the Protected Health Information for its Covered Entity's own use.

Healthcare Provider as defined by state law [Pennsylvania eHealth Information Technology Act] is a person licensed by the Commonwealth to provide healthcare or professional clinical services. This term includes:

- A healthcare practitioner, as defined in Section 103 of the Act of July 19, 1979 (P.L.130, No.48), known as the Health Care Facilities Act.
- A healthcare provider, as defined in Section 103 of the Health Care Facilities Act.
- A public health authority.
- A pharmacy.
- A laboratory.
- A person that provides items or services described in Section 1861(s) of the Social Security Act (49 Stat. 620, 42 U.S.C. 1395x(s)).
- A provider of services, as defined in Section 1861(u) of the Social Security Act (49 Stat. 620, 42 U.S.C. 1395x(u)).

HIPAA BAA shall mean the Business Associate Agreement executed between HSX and its members/participants. See "Business Associate Agreement (BAA)" definition.

HITRUST https://hitrustalliance.net is an organization providing third party certification for privacy and security programs and services. The certifiable framework (CSF) provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management. Developed in collaboration with healthcare and information security professionals, the HITRUST CSF rationalizes healthcare-relevant regulations and standards into a single overarching security framework. Because the HITRUST CSF is both risk- and compliance-based, organizations can tailor the security control baselines based on a variety of factors including organization type, size, systems, and regulatory requirements.

HSX Board shall mean the Board of Trustees of HSX, a nonprofit corporation further described in the bylaws of HSX.

HSX Executive Committee is a governing and decision-making body for HSX.

HSX Network shall mean the community-wide health information system that supports the operation of a secure Internet-based authenticated peer-to-peer computer system and search engine as well as other services for patient health, demographic, and related information that assists its Authorized Users in locating, and facilitates the sharing and aggregation of, patient Data held by multiple potentially unaffiliated health care and health care related organizations with unique health information applications that interface with the Internet, or other applications, and allows Participants the ability to authenticate and communicate securely in order to provide access to and improve the coordination, continuity and quality of patient care.

HSX Policies shall mean the written policies and procedures that apply to and govern HSX, and its Participants and Authorized Users and that are adopted pursuant to HSX Board processes. The **HSX Policies** shall be contained on the website of HSX at http://www.hsxsepa.org.

HSX Systems and Services: Includes the following but is not an exhaustive list of HSX capabilities and can be found on the HSX website https://www.healthshareexchange.org/hsx-approved-policies:

- Automated Care Team Finder (ACTF)
- Clinical Activity History (CAH)
- Clinical Data Repository (CDR)
- Encounter Notification Service (ENS)
- Health Plan Quality Reporting
- Population Health Reporting
- Urgent Patient Activity Liaison (UPAL)

I

Identified Data will be considered Identifiable Data when information provided about an individual person includes any of the following HIPAA patient identifiers:

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, precinct, zip code).
3. All elements of dates related to an individual (birthday, admission date, discharge date, date of death, exact age if over 89)
4. Telephone Numbers
5. Fax Number
6. Device identifiers and serial numbers
7. Email addresses
8. Web Universal Resource Locators (URLs)
9. Social Security numbers
10. Internet Protocol (IP) addresses
11. Medical record numbers (MRN)
12. Biometric identifiers including finger and voice prints
13. Health plan beneficiary numbers

14. Full-Face photographs and any comparable images
15. Account numbers
16. Certificate/license numbers
17. Vehicle identifiers and serial numbers including license plate numbers
18. Any other unique identifying number characteristic or code except the unique code assigned by the investigator to code the data.

Thus, an example of identified individual patient Identified Data is displayed below (by virtue of the information provided in the first 3 columns):

Identified Individual Patient Data Example			
Patient Name	**Age**	**Residential Zip code**	**Primary Diagnosis**
John Doe	34	19183	Asthma
Minnie Mouse	76	19232	Alzheimer's Disease
Test Patient	51	19333	Type II Diabetes
Donald Duck	49	19445	Hypertension

Any combination of De-Identified and Identified individual Data will be considered Identified Data except in the application of the Expert Determination Method of De-identification.

Impact Analysis (IA) is a process that identifies and evaluates the potential effects (financial, life / safety, regulatory, legal / contractual, reputation and so forth) of natural and man-made events on business operations. An IA determines what levels of impact to a System are tolerable. An IA further identifies mitigation options, mitigation steps for each option, and related expenses to support emergency management decisions.

In Production describes the act or process of creating a product or fulfilling a service. In the context of HSX, in production may mean that a member hospital is in the process of establishing the technical connections that will be tested in order to "go live"/ benefit from HSX services.

In Test describes an organization that has successfully connected to HSX, but data feeds are being tested for accuracy and reliability before going live.

Incident see Security Incident.

Incident Response is a structured and organized response to any Adverse Event or Security Incident that threatens HSX's IT assets, including Systems, Networks and telecommunications Systems. Incident Response is also the mitigation of violations of security policies and recommended practices. Incident Response is an action plan for dealing with intrusions, cyber-theft, denial of service attacks, fire, floods, and other security-related Adverse Events. Incident Response is typically comprised of a six step process (Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned).

Incident Response Team (IRT) is a group of professionals trained and chartered to respond to Security Incidents. The IRT provides both an investigative and problem-solving component. The IRT includes managers with the authority to act, technical resources with the knowledge and expertise to rapidly diagnose and resolve problems, and communication experts that provide external communications.

Incremental Backup is a copy of all files that have changed since the last Backup of any type (Full, Differential, and Incremental). The advantage is fast Backup and least storage requirements. The disadvantage is that restoration is slow, and requires several sets of Backup Data to fully restore all of the Data.

Indicator is a sign that a Security Incident may have occurred or may be currently occurring.

Individual Data is data pertaining to an individual person.

Information Assets are elements of software and hardware and associated Data that are found in HSX's operating environment. Information Assets include, but are not limited to:

- Enterprise Data (e.g., PHI, business Data, intellectual property, etc.)
- Servers
- Workstations (desktops, laptops, notebooks)
- Network devices (switches, routers, firmware, firewalls)
- Peripherals (printers, scanners, monitors)
- Software/ applications (purchased, licensed or leased)
- Biomedical equipment
- Mobile devices (smart phones, tablets, USB storage drives)
- Telecommunication equipment (VOIP phones)

Information Asset Inventory is the identification, recording, and documenting of Information Assets maintained by HSX.

Information Asset Owner is the individual or organizational unit that has management responsibility for controlling the production, development, maintenance, use and security of Information Assets. Information Asset Owners are associated with the business functions of HSX rather than the technology functions. Information Asset Owners are

appointed by senior leadership, and are typically an administrative officer or department director. Depending on the type of Information Asset, the Information Asset Owner may be a Data Owner, an Application Owner, a System owner, etc.

Information Security Incident Response Capability (ISIRC) is a capability set up for the purpose of responding to Security Incidents.

Information Services are any service or function carried out to support, provision, administer, and / or provide training for with respect to an Information Asset (e.g., email, database services, etc.).

Information Systems are a subset of Information Assets that includes information technology hardware and software/applications, but does not include Data.

Information System Contingency Plans (ISCP) provides procedures for the recovery of a System following a disruption. The ISCP provides the information necessary for System recovery, including roles and responsibilities, inventory, assessment procedures, recovery procedures, and testing. The ISCP can be activated at the current location or at an alternate location.

Interface Engine (IE) describes hardware and software that allow different computer systems to access and exchange information.

Internal Audit is an in-house review of the records of system activity.

Internal Use Only Data represents data classified as Tier 2: Internal Use Only Data according to the data classification scheme defined in *the Data Classification Policy*.

Intrusion Detection System (IDS) is a device or software application that monitors Network or System activities for malicious activities or policy violations and produces reports to a management station.

Intrusion Prevention System (IPS) is a device or software application that monitors and reports Network or System activities similar to an Intrusion Detection System (IDS), but also possesses the ability to block unauthorized access.

Involuntary Termination is characterized by the employer taking the decision to terminate the employment relationship. In certain cases, Involuntary Termination can be caused by death or by an accident leaving the individual unable to continue employment.

IT Infrastructure includes, but is not limited to, hardware, software, firmware, Network, telephony, applications, Data, platforms, middleware services, computing facilities, and systems management. IT Infrastructure also applies to the design, configurations, parameters, and documentation of those components.

L

Least Privilege means giving an Account or a process the least amount of permissions necessary to perform their intended function.

Live describes an organization that has successfully tested data feeds with HSX and consequentially, is able to exchange valuable clinical information and experience the benefits of HSX.

M

Malware, short for malicious software, is any software used to disrupt computer operations, gather sensitive information, or gain unauthorized access to private computer systems. Malware includes Viruses, Worms, Trojan Horses, ransomware, Spyware, adware, scareware, and other malicious programs.

Master Patient Index (MPI) is a tool and database that enables centralized management of patient demographics and identifiers.

Meaningful Use (MU) is a program, regulated under the Centers for Medicare and Medicaid Services, that offers incentives to providers to adopt electronic health record technology with the goals of improved care, quality and efficiency, and reduced healthcare costs.

Media includes fixed Media such as internal hard disks, flash drives, and solid state drives as well as Removable Media such as USB flash drives, portable external hard drives, removable hard drives, flash memory cards, CDs, and magnetic tapes. Media is covered by the HIPAA Security Rule.

Media Access Control (MAC) Address is a unique identifier assigned to Network interfaces for communications on the physical Network segment. MAC addresses are used as a Network address for most IEEE 802 network technologies, including Ethernet.

Medical Emergency A medical emergency means that you have symptoms that could place your health in serious jeopardy including damage to organs or bodily functions.

Member is a party that has entered into a Participation Agreement and has registered with the HSX HIE as a specific Member User Type.

Message Integrity is the authenticity, validity, and certainty of origin of a transmitted message. Message Integrity deals with methods that ensure that the contents of a message have not been tampered with and altered.

Minimum Necessary: The HIPAA Privacy Rule stipulates that covered entities limit the amount of information disclosed to the minimum necessary to achieve the specified goal

[45 CFR 164.514(d)(1)]. This requirement does not apply if the disclosure is required by law, authorized by the individual, or for treatment purposes.

When Using or Disclosing PHI, or when requesting PHI from another health care provider or health organization, HSX shall limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

Mitigate: To make less severe or intense.

Mobile Code is software transferred between Systems, e.g., transferred across a Network, and executed on a local system without explicit installation by the recipient. Examples of mobile code include scripts (JavaScript, VBScript), Java applets, ActiveX controls, Flash animations, Shockwave movies (and Xtras), and macros embedded within Microsoft Office documents.

Mobile Computing Devices are lightweight, easily transportable devices capable of connecting to HSX Networks and/or accessing HSX Confidential Data. Mobile Computing Devices include, but are not limited to, Smart Phones (e.g., iPhones, Androids), tablets (e.g., iPads, Slates), and Blackberry devices. Mobile Computing Devices may be HSX owned (see Business Mobile Computing Devices) or personally-owned, and may be fully or partially managed by HSX.

Multi-Factor Authentication (MFA) requires using two or more forms of identification to authenticate a user. Single factor authentication, which is commonly used, employs a unique username and password combination. For more security, multi-factor authentication adds at least one more form of authentication, such as a physical token or biometrics.

N

Need-to-Know means restricting access to Confidential Data to only those who have a specific need based on their job responsibilities. In order to safeguard patient privacy, Users shall receive access only to the minimum functions and privileges required for performing their jobs.

Need-To-Share means restricting access to Confidential Data to only the information that is required for sharing.

Network is any system of IT hardware, software, frequency spectrum, cable and physical surroundings that enables devices to interconnect and share information. Network includes all communications cabling, equipment and infrastructure devices, including but not limited to the following: telecommunications switches, data networking switches and routers, Wireless Access Points, cellular distributed antenna systems, cellular repeaters

and/or bi-directional amplifiers, cellular macro sites, cable and satellite television reception and distribution equipment.

Network Administrator is an individual, or group of individuals, who have delegated authority to administer a Network, including controlling access to the Network and configuring the Network and the devices of which it is comprised. It is the responsibility of the Network Administrator to understand the business needs of Network Users and to facilitate appropriate access to the Network.

Network Diagram is a graphical representation of the Network. Network Diagrams document and detail the current state of connectivity regarding the Network's physical, logical, system-specific, application-specific, and/or other aspects of network hardware, software, frequency spectrum, cabling and connectivity, signaling types, ports, and protocols.

Network Owner is an individual or organizational unit responsible for operating and maintaining the physical HSX infrastructure which comprises the Network, including responsibility for establishing the procedures to be used for maintenance and upgrades.

Non-exceptional Use Case (non-permitted) is exceptional use of Protected Health Information for otherwise non-Permitted Purposes (i.e. pay-for-performance; benchmarking, analytics and comparative purposes; and/or research) may be granted on a case-by-case basis upon review and approval of HSX with Notice to Data-Contributing Participants for each and every non-Permitted Purpose.

Notice of Privacy Practices (NPP) is a printed advisory given to patients that explains the health care office's use of the patient's protected health information (PHI).

O

Office of the National Coordinator of Healthcare IT is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and electronic exchange of health information.

Operating System is the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.

Output Data Validation is the process of ensuring that a program operates on clean, correct and useful Data, and that the resulting output Data is correct, meaningful, and secure.

P

PA eHealth Partnership Authority (Authority) improves healthcare delivery and healthcare outcomes in Pennsylvania by enabling the secure exchange of electronic health information (eHIE).

Paper Media includes any physical piece of paper that may be photocopied or easily removed from HSX facilities. Paper Media is covered by the HIPAA Privacy Rule.

Participant means, in general, a person or entity that has entered into a binding agreement with HSX setting forth the terms and conditions of access to and use of the HSX Network after such person or entity is approved as an authorized Participant of HSX, and shall include each Founding Member

Participant Agents acting as agents for Participants who are payors in connection with the completion and reporting of Data to CMS for HEDIS and Star reimbursement purposes or for other Permitted Purposes contained in approved Use Cases.

Participant Type means the category of Participant to which a particular Participant is assigned based upon that Participant's relationship to the HSX Network and other Participants, and includes classification of such Participant as either a Data Supplier, Data Receiver, Data Viewer, or Data Exchanger, as more specifically described in the HSX Policies.

Participation Agreement is an agreement which sets forth the terms and conditions pursuant to which a Participant may supply, receive or share Data through the HSX HIE.

Password is a string of characters that allows access to a computer, interface, or System.

Patient is an individual who has received or will receive treatment or health care services from a Health Care Provider.

Payment can be defined as activities related to being paid for services rendered. These include eligibility determinations, billing, claims management, utilization review, etc. Payment also includes using debt collection and location agencies

Pennsylvania eHealth Authority is a predecessor organization to the Pennsylvania eHealth Partnership.

Pennsylvania eHealth Collaborative (PAeHC) is a predecessor organization to the Pennsylvania eHealth Authority.

Pennsylvania Health Information Exchange (PHIX) is a predecessor organization to the Pennsylvania eHealth Collaborative.

Pennsylvania eHealth Partnership is the Commonwealth of Pennsylvania Department of Human Services (DHS) Health Information Exchange regulatory body. The Pennsylvania eHealth Partnership is responsible, under Pennsylvania Act 76 of 2016 http://www.legis.state.pa.us/cfdocs/legis/li/uconsCheck.cfm?yr=2016&sessInd=0&act=76 , for

the creation and maintenance of Pennsylvania's secure health information exchange, known as the PA Patient & Provider Network, or P3N. This includes certification of Health Information Organizations (HIO) connecting to the P3N "hub," maintenance of the patient opt-out and opt-back-in registry, and administration of grant programs to facilitate connections of health care providers to HIOs. The eHealth Partnership also works within DHS and across selected state agencies to facilitate health care provider reporting to various state registries, including immunization, laboratory reporting, cancer, syndromic (disease) surveillance, and clinical quality measurement.

Pennsylvania Patient and Provider Network (P3N) is the PA eHealth Partnership operated network that supports the ability of certified healthcare participants to exchange information within and beyond Pennsylvania's borders.

Persist is to retain as in storing data.

***Permitted Purposes** is the ways that are authorized by the participation agreement to exchange and share information between the covered entities.

Permitted Use is the permitted purposes for which Data received through the HSX HIE may be accessed and used. Any use of Data that is not set forth as a Permitted Use under the policies shall be, for purposes of the HSX HIE, considered a Prohibited Use.

Personally-Owned Mobile Computing Devices are Mobile Computing Devices that are purchased with non-HSX funds.

Personal Health Record (PHR) means an electronic, universally available, resource of health information that may originate from either a Health Care Provider or the Patient, but is controlled and managed exclusively by the Patient.

Personal Representative is a person or persons designated by a patient to receive PHI or an individual who has legal authority to receive another individual's PHI. In clarification, a health care provider may disclose PHI to a designated Personal Representative when the patient is not physically able to personally disclose their PHI to the Personal Representative, or the patient has requested their health care provider to disclose PHI to their Personal Representative. Should a legitimate need arise, and patient designation or legal authority is not possible, an individual may be designated as the Personal Representative based on the professional judgment of the healthcare provider.

Population Health refers to an approach to improving the health outcomes of an entire population. As noted above, populations might be defined based on where they receive care, how they are insured, their diagnoses (e.g., people with hypertension or diabetes), where they reside, or other personal or demographic attributes. Population Health analyses might inform improvements in clinical care, community/social services, and public health. The health of individuals and populations is shaped by not only by the healthcare they receive but also by the social determinants of health. Consideration of

circumstances in patients' communities can be used to create best practices for prevention, treatment, and healthy living.

Population Health Management for a targeted group of patients or members for which the HSX Member/Participant has treatment and/or payment responsibility through a recognized Accountable Care Organization or Patient Centered Medical Home for population-based activities relating to: (i) improving overall health of the targeted group, (ii) reducing health care costs, (iii) protocol development, (iv) case management and care coordination of the group, (v) contacting of health care providers and patients with information about treatment alternatives targeted at a certain group; and (vi) related functions that do not include treatment of the individual. Population Health Management activities focus on the specified patient population or group, but necessarily could extend to the conducted on an individual patient/member.

Precursor is a sign that an attacker may be preparing to cause a Security Incident.

Primary Care Provider (PCP) is an individual provider through whom a patient receives primary care services.

Privacy Officer is the individual responsible for ensuring the HSX's compliance with privacy requirements under HIPAA, HITECH and other applicable privacy laws. The HSX Privacy Officer is the primary contact for all notifications regarding potential or actual privacy violations in connection with the HSX HIE.

Privilege refers to the access permissions granted to a specific User within a System.

Program Source Code is code written by programmers using a programming language (e.g., Java). The programming language provides a series of instructions the programmers use to create the program. All the instructions a programmer uses to build the program are known as Program Source Code.

Prohibited Uses are any access or use of Data through the HSX HIE for any reason or purpose other than a Permitted Use. Prohibited Uses may include, but are not necessarily limited to, manipulating, aggregating, integrating, compiling, merging, reorganizing, regenerating, transferring or otherwise using or disclosing Data for any purpose except treatment and other Permitted Uses specifically allowed under these polices.

Protected Health Information (**PHI**) shall have the meaning given to such term under HIPAA and 45 C.F.R. 160.103 and means any information, transmitted or recorded in any form or medium, that: (a) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; and that (b) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual). Protected Health Information includes ePHI.

Provider means Physicians or Non-Physician Professionals and Participant's agents on behalf of Physicians or Non-Physician Professionals who are employed by, under contract with or members of the medical staff of a Participant. "Physician" means an individual legally licensed to provide healthcare services to patients and includes a doctor of medicine or osteopathy, a doctor of dental surgery or dental medicine, a doctor of podiatric medicine, a doctor of optometry and chiropractor. "Non-Physician Professional" means an individual who is licensed, certified or otherwise designated to assist Physicians in providing healthcare services to patients and includes, but is not limited to, a nurse practitioner, physician assistant, therapist, psychologist, pharmacist, technician, nurse, dietician, patient care coordinator and social worker.

Provider Directory is a listing of providers with a Direct email address enabling the lookup of other Providers based on name, organizational association or specialty.

Psychotherapy Notes are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or who is analyzing the contents of conversations during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record.

Psychotherapy Notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis and progress to date.

Public Health – Public Health activities shall have the same meaning as set forth in 45 C.F.R 164.512(b) of HIPAA, including the use and disclosure of PHI under this use case to or by a Public Health Authority that is authorized by law to collect or receive such PHI for the purpose of preventing or controlling disease, injury, or disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of a Public Health Authority, to an official of a foreign government agency that is acting in collaboration with a Public Health Authority.

Public Health Authority – Public Health Authority shall have the same meaning assigned to such term under 45 C.F.R 164.501 of HIPAA, which is limited to "an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate".

Public Health Gateway (PHG) provides a secure, single point of entry for critical public health data, including electronic lab reporting, syndromic (disease) surveillance, cancer reporting, immunization registry, and clinical quality measurement.

Q

Query is a system search for PHI about a patient by an authorized User conducted through the HSX HIE on a Need-to-Know basis.

R

Record Locator Service (RLS) is a Cross-Enterprise Document Sharing (XDS) Registry. A RLS allows patient information to be aggregated from connected providers – this information can then be queried.

Reference Information Model (RIM) is an object model which is the cornerstone of the HL7 development process that identifies the life cycle a message or groups of messages will carry.

Regional Health Information Organization (RHIO) is used to denote a type of health information organization that connects stakeholders from a particular geographic region in order to improve the quality and cost of healthcare. Stakeholders may include, but are not limited to: payers, health systems, laboratories, and public health entities.

Remote Access is the ability to gain access to HSX's Network from outside the Network perimeter. Common methods of communication from the remote computer to HSX's Network includes, but is not limited to, Citrix and Outlook Web Access (web-based Secure Socket Layer (SSL) portals), HSX Private Networks (VPNs), and other methods which employ Encrypted communication technologies.

Removable Media are devices external to HSX Computing Devices that may be utilized for the storage and/or transfer of Enterprise Data, and which may be removed from HSX facilities. This includes, but is not limited to USB flash drives, portable external hard drives, removable hard drives, flash memory cards (e.g., SD cards, XSD), CDs, DVDs, floppy disks, and magnetic tapes. Removable Media is covered by the HIPAA Security Rule.

Request for Change (RFC) is a declarative document containing the details of an emergency or non-emergency call to an adjustment of a system. HealthShare Exchange of Southeastern Pennsylvania, Inc. requires an online form to be completed in order make a request for change.

Requester is an individual, team, or entity seeking a change pertaining to the existing system.

Research the purpose of Research is to generate or contribute to generalizable knowledge outside the scope of providing the participating institution information that is needed to assess or improve the health of the individuals or populations they serve. Data collected exceeds requirements for care of the study participants or extend beyond the scope of the

activity. Generalizable knowledge means new information that has relevance beyond the population or program from which it was collected, or information that is added to the scientific literature. Knowledge that can be generalized is collected under systematic procedures that reduce bias, allowing the knowledge to be applied to populations and settings different from the ones from which it was collected.

Resilience is the ability to quickly adapt and recover from any known or unknown changes to the business environment.

Risk Management is a continuous process that allows the organization to balance the operational and economic costs of protective measures while achieving gains in protecting the IT Systems and Data that supports organizational goals and objectives. Risk Management encompasses:

- Risk Assessment
- Risk Treatment
- Risk Monitoring and Review

Risk Management Plan is a document that a project manager prepares to foresee risks, estimate impacts, and define responses to issues. The Risk Management Plan also contains a risk assessment matrix.

Roll Back Plan documents the actions to take to restore service if the Change fails.

S

Secure Access is a Network technology that hosts applications on central servers and allows users to interact with them remotely or stream and deliver them to user devices for local execution.

Security Incident is an Adverse Event or group of Adverse Events in an information System or Network or the threat of the occurrence of such an Event. A Security Incident is also a violation, or imminent threat of violation, of information security policies, acceptable use policies, or standard security practices.

Examples of Security Incidents include:

- Loss of a Computing Device, e.g., laptop or portable device
- Compromise of information integrity
- Inadvertent disclosure of Confidential Data
- Loss of system availability
- Denial of service
- Misuse of service, Systems or information
- Hacking, attempts to steal passwords, or other malicious activity

- Damage to Systems from malicious code attacks (e.g. viruses, Trojan horses, logic bombs, etc.)

***Self Pay** is the patient right to request that information not be shared with Health Plan when the healthcare services were paid for by the patient and not using a Health Plan benefit.

Senior Leadership is the Board of Trustees and Officers responsible for making executive-level decisions.

Service Level Agreement (**SLA**) is a contract with a Third Party that specifies in measurable terms the services to be provided.

The Sequoia Project previously known as HealtheWay is a non-profit organization that aims to reduce interoperability barriers for HIEs on a national scale. This organization facilitates the groundwork and provides services for collaboration and analysis of government policies and standards affecting HIEs.

Signature is a recognizable, distinct pattern in Network traffic associated with an attack, such as a binary string in a Virus or a particular set of keystrokes used to gain unauthorized access to a System.

State Law means the laws of the State of Pennsylvania unless specifically stated otherwise.

Social Engineering is an attempt to trick someone into revealing information (e.g., a password) that can be used to attack Systems or Networks.

Source Code see Program Source Code.

Spyware is a type of Malware software that enables a hacker to obtain covert information about another's computer activities by transmitting Data covertly from their hard drive.

Stateful Packet Inspection is a Firewall architecture that works at the Network layer. Stateful Packet Inspection examines both the header information and the contents of the packet up through the application layer in order to determine more than just information about its source and destination. The Firewall is programmed to distinguish legitimate packets from different types of connections.

Static IP Address is a permanent numeric identification assigned by the Network Administrator to a node in a TCP/IP network. Static IP Addresses are used for shared resources such as web servers and webcams.

Super Protected Data (SPD) is information related to mental health, substance abuse, or HIV/AIDS, cannot be legally exchanged without explicit patient authorization.

System is a collection of hardware, software, Data, people and procedures that work together to produce quality information.

System Administrator is an individual, or group of individuals, who have delegated authority to administer a System, including controlling access to the System and configuring the System and the devices of which it is comprised. It is the responsibility of the System Administrator to understand the business needs of System Users and facilitate appropriate access to the System.

System Owner is an individual, or group of individuals, who have been officially designated as having management responsibility for controlling the production, development, maintenance, use and security of a System.

T

Telework (telecommuting) allows an individual to use technology to work from home or from an alternate worksite. Telework arrangements do not change salary, benefits, job responsibilities, leave policies, or other terms of employment.

Third Party is any entity external to HSX with which HSX is sharing Enterprise Data or from which HSX is obtaining products or services.

Threat is a potential for violation of security, which exists when there is a circumstance, capability, action, or Adverse Event that could breach security and cause harm.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a Participant; consultation between health care providers relating to a patient or member; or the referral of a patient or member for health care from one health care provider to another.

Treatment, Payment, or Operations (TPO) describes that the HIPAA Privacy Rule permits disclosure of PHI only for TPO or when regulatory exception applies (e.g. public health reporting).

Trojan Horse is a Malware program designed to breach the security of a computer system while ostensibly performing some innocuous function.

U

Urgent Care Care is a walk-in clinic designed to treat illness and injury that requires immediate care; but care that is not significant enough for an emergency room visit.

Urgent Patient Activity Liaison (UPAL) is designed to provide a real-time look-up capability of an individual patient's emergency healthcare activity in the event of a regional crisis or emergency situation impacting healthcare services for a large number of citizens. This service can be invoked for HSX staff to locate the institution to which patients have been

admitted, discharged or transferred and to share that information with the patient's next of kin and other family members.

Use Cases means the specific narratives offered by HSX to meet Participant needs using the HSX Network or External Networks. Use Cases shall be approved through HSX Board Use Governance processes.

User is any person or entity that uses HSX Information Assets.

User Authentication is the process of validating the professional credentials and identity of a User in order to gain authorized access to the HSX HIE systems/applications.

User Authorization is the process of determining whether a particular User within has the right to access PHI through the HSX HIE, and is subject to role-based access requirements that take into account an individual's specific job function.

V

***Value Based Payment Service** is a service that HSX offers to the Participant that addresses sharing of information between covered entities under the auspicious of Value Based program entered in between entities.

Virtual Private Network (VPN) is a networking technology that enables a host computer to send and receive Data across shared or public Networks as if it were a private Network with all the functionality, security and management policies of the private Network.

Virus is a piece of code that is capable of copying itself and typically has a detrimental effect, such as corrupting the System or destroying Data. Viruses spread to other machines by the actions of Users, such as opening infected email attachments.

Voluntary Termination is characterized by mutual agreement between the employee and HSX regarding the terms and timing of the departure. Voluntary Termination can include retirement.

Vulnerability is a weakness in a System, application, or Network that is subject to exploitation or misuse.

Vulnerability Management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities, especially in software and firmware. Vulnerability Management is integral to computer security and network security.

W

Wireless Access Point is a device that allows wireless devices to connect to a wired Network using Wi-Fi or related standards. The Wireless Access Point usually connects to a

router (via a wired Network) as a standalone device, but it can also be an integral component of the router itself.

Worm is a standalone Malware program that replicates itself in order to spread to other computers. Often a worm uses a computer Network to spread itself, relying on security failures on the target computer to access it. Unlike a computer Virus, a Worm does not need to attach itself to an existing program.

WPA (Wi-Fi Protected Access) is a security protocol for wireless 802.11 Networks from the Wi-Fi Alliance.