

Security Terms and Definitions

Access Authority – An entity responsible for monitoring and granting access privileges for other authorized entities. SOURCE: SP 800-57

Access Control - The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities. SOURCE: FIPS 201

Administrative Safeguards - Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information. SOURCE: HIPAA

Audit – Independent review and examination of records and activities to assess the adequacy of systems controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies and procedures. SOURCE: SP 800-32

Audit Data – Chronological record of systems activities to enable the reconstruction and examination of the sequence and events and changes in an event. SOURCE: SP 800-32

Audit Trail – A record showing who has accessed an IT system and what operations the user has performed during a given period. SOURCE: SP 800-47

Authentication – The basic process of validating that someone is who they claim to be. SOURCE: HIPAA

Authentication Factors – The authentication process is usually broken down into several methods of challenge and response. 1. Something you know (account/user name, password, PIN, ID number, etc.); 2. Something you have (token, bank card, driver's license, passport, etc.) & 3. Something you are (biometrics, fingerprint, retina, DNA, signature, etc.).

Authorization – The official management decision to permit access to systems based on the implementation of an agreed-upon set of security controls. SOURCE: SP 800-37 (The granting of rights, including the ability to access specific information or resources.)

Biometric – A physical or behavioral characteristic of a human being. SOURCE SP 800-32 (A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. SOURCE: FIPS 201)

Computer Forensics – The practice of gathering, retaining, and analyzing computer-related (audit) data for investigative purposes in a manner that maintains the integrity of the data. SOURCE: SP 800-61

Federated Identity Management – The use of agreements, standards and technologies to make identity and entitlements portable across autonomous identity domains. The goal of federation is to enable transparent and secure exchange of identity information to enable disparate systems to interoperate at the security level.

Identity – A unique name of an individual person. Since the legal names of persons are not necessarily unique, the identity of a person must include sufficient additional information to make the complete name unique. SOURCE: SP 800-63

Identity Proofing – The process of providing sufficient information (e.g., identity history, credentials, documents) to a Registration Authority when attempting to establish an identity. SOURCE: FIPS 201

Information security – The protection of information and information systems from unauthorized access use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. SOURCE: SP 800-53 & FIPS 200

Password – Confidential authentication information composed of a string of characters. SOURCE: HIPAA (A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. SOURCE: SP 800-63)

Record Locator Service (RLS) – An electronic index of patient identifying (demographic) information that directs participants in a Health Information Exchange to the location of patient health information held providers as defined in section 144.335, subdivision 1 (b) and group purchasers as defined in section 62J.06, subdivision 6. SOURCE: Patient Consent/Liability subgroup

Registration Authority (RA) – A trusted entity that establishes and vouches for the identity of a subscriber to a HIE. The RA may be an integral part of a HIE, or it may be independent of a HIE, but it has a relationship to the HIE. SOURCE: Sp 800-63 (Organization responsible for assignment of unique identifiers to registered objects. FIPS 188)

Role-Based Access - Determination that the access of a workforce member to electronic protected health information is appropriate with their role or job function. SOURCE: HIPAA

Rule-Based Security Policy – A security policy based on global rules imposed for all subjects. These rules usually rely on a comparison of the sensitivity of the objects being accessed and the possession of corresponding attributes of the subjects requesting access. SOURCE: SP 800-33

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. SOURCE: SP 800-53 & FIPS 200

Security Credentialing – The process of reviewing and granting a user the appropriate role-based designation and access rights to specific health information.

Security Incident – Means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. SOURCE: HIPAA

Security Policy – A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. SOURCE: FIPS 188

Single-factor Authentication – This is when only one of the three possible factor types is used to authenticate a person for system access. The three factor types are: 1. Something you know, such as an ID and password or PIN. 2. Something you have, such as, a security fob or smart card (a physical object that must be presented to enable access). 3. Something you are, such as, personal biometric (fingerprint, retina scan, etc.), which is unique.

SNO (Sub-Network Organization) – A SNO is any group of entities (regionally or non-regionally defined) that agree to communicate clinical data with one another using a Record Locator Service (RLS), using shared policies and contractual agreements. A SNO has two sets of interfaces, one internal, which binds its member entities together, and one external, which is where traffic to and from other SNOs and outside entities comes from. SOURCE: Markle Foundation – Connecting for Health

Treatment Relationship - 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 third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another. SOURCE: HIPAA