

DHHS POLICIES AND PROCEDURES

Section VIII: Privacy and Security
Title: Security Manual
Chapter: Glossary
Current Effective Date: 11/21/05
Revision History:
Original Effective Date:

Purpose

To provide to the Department of Health and Human Services (DHHS) divisions/offices definitions of key security terms used in the departmental security policies, procedures and standards developed and published by DHHS Privacy and Security Office (PSO) and the North Carolina Office of Information Technology Services (ITS). This document is not intended to be an exhaustive list of ITS security terms; however, the document should provide the user with the basic, key terms required for the interpretation of the DHHS ITS security policies, procedures, standards, and guidelines. ITS also maintains a glossary that is available at the State Chief Information Officer web site:

http://www.scio.state.nc.us/SITPoliciesAndStandards/Statewide_Information_Security_Manual.asp.

Policy

DHHS shall use the authorized definitions in interpreting and/or implementation of the security policies, procedures and standards

Implementation

The following are key terms found in the DHHS and ITS security policies, procedures, and standards.

A

Access – A specific type of interaction between a subject (e.g., user) and an object (e.g., data) that results in the flow of information from one to the other. The ability or the means necessary to read, write, modify or communicate data/information or otherwise make use of any computer or information system resource.

Accessibility – The ability to obtain use of a computer system resource, or the ability and means necessary to store data or communicate with a system.

Access Control – A feature or technique used to permit or deny use of the components of a system, including hardware, software, and/or procedures that restrict access to devices and services.

Access Control List (ACL) – A mechanism that implements access control for a system resource by listing the identities of the entities (i.e., users, groups, processes or devices) that are permitted to access the resource.

Accountability – The property that enables activities to be traced to individuals (or entities) that may then be held responsible for their actions.

Account Management – The review of one (1) or more user accounts to determine if the status of an account has changed. User access privileges to information resources are typically reviewed on a periodic basis to see if they are still applicable.

Accreditation – Accreditation is the official authorization for the operation of a system and is based on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the management or operating authority and indicates that due care has been taken for security. Essentially, accreditation involves acceptance of the system.

Administrative Security – The management methodologies, policies, processes, standards, procedures, and controls established to protect the infrastructure (i.e., data, hardware/software assets, property, and personnel).

Agency – Any department, institution, commission, committee, board, division, bureau, office, officer, or official of the state. The term does not include a state entity excluded from coverage under N.C. General Statutes (G.S.) 147-33.80, unless that state entity elects to be covered under N.C.G.S. 147-33.81.

Annualized Loss Expectancy – The expected yearly dollar value loss from the system or activity due to attacks or threats. Generally calculated by taking the value of a single such loss by a given threat or event, and multiplying by the expected number of events over the period of a year.

Anti-virus Software – Software that protects a personal computer (PC) from infection by viruses and worms, which are small, sometimes destructive, self-propagating programs that are usually transmitted via the Internet, email, or disks. Infected computers can lose data and spread viruses/worms to other computers.

Application – A collection of software [components](#) used to perform specific types of user-oriented work on a computer. Computer [software](#) that performs a business function (e.g., Microsoft Word).

Application Security – The technical architecture and controls implemented to limit user access and protect the confidentiality, integrity, and availability of data for an application in the production environment.

Assessment – An evaluation. The following security-related assessments are referred to in the DHHS policies:

- Threat assessment – evaluates what events could occur in a given environment.
- Risk assessment – examines how likely security incidents are to occur in the given environment and how much damage these incidents would cause.
- Vulnerability assessment – identifies security weaknesses and examines how well existing countermeasures reduce the risk of a security incident.

Asset Management – Specific standards for the management of the networks, information systems, and applications that store, process, and transmit information assets. This does not

replace the asset management process used by the DHHS Office of the Controller to create a comprehensive list of equipment and software owned (e.g., hardware) by the department.

Assurance – A measure of confidence that the security features and architecture of a system can accurately mediate and enforce the DHHS security policies.

Attack – The act of trying to bypass security controls on a computer system, information system, or network.

Audit – The process of generating, recording, and reviewing a chronological record of transactions in an information system to verify the activity in the system. An examination of the systems, programming and datacenter policies and procedures to determine the efficiency of computer operations and adherence to the DHHS Security Policies.

Audit Controls – The mechanisms employed to record and examine system activity.

Audit Trail – A chronological record of information system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results. It includes data collected and potentially used to facilitate a security audit and includes the who, what, and when.

Authentication – The act of verifying the identity of a system entity (e.g., a user or a computer or information system) and the entity's eligibility to access information.

Authorization – The process of determining what types of activities are permitted. The process of granting a user access to information, an information system or an application. Often access privileges are granted based on the role the user has in relation to the organization and/or the system to be accessed.

Authorized User – One who has been authenticated to a system and has been granted rights of access based on the user's policy attributes. A person, computer or information system, application, or defined group that has been authenticated to a system and granted access only to those resources to which he/she/it has been granted permission to use.

Availability – The probability that a given resource will be usable during a given time period. Availability is the need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

B

Backdoor – A hidden software or hardware mechanism that can be triggered to permit computer or information system or network protection mechanisms to be circumvented.

Backup – The process of making a duplicate copy of data for archiving purposes or for protecting against damage or loss.

Banner – The initial message given by a system to prompt login or identify a connection.

Best Practices – The processes, practices, and systems identified in public and private organizations that perform exceptionally well and are widely recognized as improving an organization's performance and efficiency in specific areas.

Biometrics - Unique, measurable physical or behavioral characteristics of a human being for automatically recognizing or verifying identity.

Business Associate – A person, organization, or agency that provides specific functions, activities, or services that involve the use, creation, or disclosure of individually identifiable health information for, or on behalf of, a HIPAA covered health care component. Examples of business associate functions are activities such as claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice

management, and repricing; and legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

- **DHHS Internal Business Associate** – A non-covered unit within the same division or unit in another DHHS division that performs HIPAA covered functions for, or on behalf of, a covered health care component.
- **DHHS External Business Associate** – Another state government department or public/private contractor that performs HIPAA covered functions for, or on behalf of, a covered health care component.

Business Continuity Plan (BCP) – A collection of procedures and information which is developed, compiled and maintained in readiness for use in the event of an emergency or disaster.

Business Impact Analysis (BIA) – Management level analysis, which identifies the impacts of losing organizational resources. The BIA measures the effect of resource loss and escalating losses over time, in order to provide senior management with reliable data upon which to base decisions on risk mitigation and continuity planning.

Business Owner – The person at the local level, i.e., division, central office, or facility, who is responsible for information system business processes at that particular level.

C

Certification – The comprehensive evaluation of the technical and non-technical security features of a system and other safeguards made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Change Control – A management tool to provide control and traceability for all changes made to the system. Also known as change management.

Client-Server – Computers networked in a configuration where the client is the requesting machine and the server is the supplying machine. Processing may take place on either the client or the server but it is transparent to the user.

Common Vulnerabilities and Exposures (CVE) – The CVE is an important defensive information system, community wide effort. CVE is the result of a collaborative effort of the CVE Editorial Board, which includes representatives of over 20 security-related organizations. The MITRE Corporation maintains and moderates CVE. Vulnerabilities are assigned a specific CVE number for tracking.

Confidentiality – Confidentiality is the need to ensure that information is disclosed only to those who are authorized to view it.

Configuration Management – The management of security features and assurances through control of changes made to a computer or information system's hardware, software, firmware, documentation, test cases, test fixtures, and test documentation throughout the development and operational life of a system.

Content Filtering – Controlling access to a network by analyzing the contents of the incoming and outgoing packets and either letting them pass or denying them based on a set of rules.

Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. The plan describes the necessary steps to take in order to ensure the continuity of core business functions.

Control – Any protective action, device, procedure, technique or other measure that reduces exposure.

Covered Entity – One of the following organizations that is subject to HIPAA regulations:

- A health plan;
- A health care clearinghouse; or
- A health care provider who transmits any health information in electronic form in connection with a transaction that is subject to the Health Insurance Portability Accountability Act (HIPAA) of 1996.

Covered Functions – Those functions of a covered entity or the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

Covered Health Care Component – An agency or a portion of an agency within DHHS (a hybrid entity) that performs a HIPAA covered function and is thereby considered a covered health plan, health care clearinghouse, or a health care provider; OR, a DHHS agency or portion of an agency that performs a covered function for, or on behalf of, a DHHS covered health care component and is thereby considered an internal business associate.

Cryptography – A technology that scrambles data to prevent unauthorized individuals from reading the data. A cryptographic key is a sequence of numbers and characters used in scrambling and unscrambling the data. The principles, means and methods for rendering information unintelligible and for restoring encrypted information to intelligible form.

D

Data Custodian – The individual or individuals that are responsible for the storage and safeguarding of information.

Data Integrity – The property that data meet, having the both expectation of quality and that the data can be relied upon.

Data Owner – DHHS is the owner of all data utilized to conduct the business of DHHS.

Data Security – The implementation of controls that maintain confidentiality, ensure integrity and enable the availability of information.

Data Use Agreement – Refers to a documented arrangement between a covered health care component and another entity concerning the permitted uses and disclosures of a limited data set of individually identifying health information that will be received by the entity from the covered entity. Entities that receive limited data sets can only use the information for the purposes of research, public health, or health care operations.

Database – A stored collection of related data needed by organizations and individuals to meet their information processing, storage, and retrieval requirements.

Data Authentication – The corroboration that data have not been altered or destroyed in an unauthorized manner. Examples of how data corroboration may be assured include the use of a check sum, double keying, a message authentication code, or digital signature.

Decryption – A technique used to recover the original plaintext from the ciphertext in an intelligible form.

Denial of Service Attack – An assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted. Unlike a virus or worm, which can cause severe damage to databases, a denial of service attack interrupts network service for some period.

Department – The DHHS.

Digital Certificate – A certificate identifying a public key to its subscriber that corresponds to a private key held by that subscriber. It is a unique code that typically is used to enable the authenticity and integrity of the communicated data to be verified.

Digital Signature – A process by which a private key is used to scramble information. A digital signature is a hash of a message that uniquely identifies the sender of the message and proves the message hasn't changed since transmission.

Disaster Recovery Plan (DRP) – A plan and preparations directed towards the resumption of business and the recovery of computer systems after catastrophic loss of important computer systems. A disaster recovery plan is generally concerned with longer time frames than a business continuity plan.

Disclosure – The release, transfer, provision of access to, or divulging in any other manner of protected health information outside the entity holding the information.

DMZ (Demilitarized Zone) – Commonly referred to as the network segment between the Internet and the private network. It controls access to external services while limiting access to the private network.

DNS (Domain Name System) – A hierarchical database that enables names to be resolved into Internet Protocol (IP) addresses (and vice versa).

Due Care – The diligence which a person would normally exercise under a given set of circumstances. That degree of care that a reasonable person can be expected to exercise in carrying out their duties.

E

Electronic Protected Health Information (ePHI) – The HIPAA Privacy Rule governs the use and disclosure of PHI in any form; the Security Rule applies to electronic PHI. Security Rule compliance efforts start where the Privacy Rule left off. A term used in the HIPAA Privacy Regulations that has the same meaning as ‘individually identifiable health information.’ The term ‘individually identifiable health information’ was used in the DHHS Privacy Policies to describe any information, including demographic information that has the potential of tying the identity of a client to his/her health information. Examples include medical record number, account number, SSN, dates of service (e.g., dates of admission, discharge, and appointment dates), and patient demographic data (e.g., address, date of birth, date of death, gender, and email address). Although some divisions/offices within DHHS possess ePHI that does not fall under the auspices of HIPAA due to the definitions of covered entities, there are covered entities within DHHS, such as DMA, that do possess ePHI. DHHS policies require that all divisions/offices follow the DHHS security policies.

Electronic Storage Media – Materials used to store data in electronic form, including floppy disks, magnetic tape, CD-ROMs and computer hard drives.

Electronic Mail (E-Mail) – The capability to compose, address, and send messages electronically over a network.

Emergency Mode Operation – Access controls in place that enable an agency to continue to operate in the event of fire, vandalism, natural disaster, or computer system failure.

Encryption – The conversion of data into a form that cannot be readily understood by unauthorized people, to ensure that only the intended recipient is allowed to read the data. The process of transforming a message, or plaintext into apparently random noise, or ciphertext, such that the message can be extracted by those in possession of an appropriate key, but is difficult or impossible to extract by unauthorized parties.

Enterprise – All state agencies, departments, institutions, commissions, committees, boards, divisions, bureaus, offices, officers, and officials of the state. The term does not include any state agency excluded from coverage under this Article by G.S. §147-33.80, unless they elect to participate in the information technology programs, services, or contracts offered by the ITS.

Environmental Infrastructure – The physical environment surrounding an information system including electrical power, fire detection and suppression, and heating, ventilation, and air conditioning (HVAC).

Exposure – A particular weakness or vulnerability to a specific attack.

Extended Workforce – Contractors, volunteers, trainees, students, and other persons whose conduct, in the performance of work for a DHHS agency that maintains individually identifying health information, is under the direct control of such entity, whether or not they are paid by that agency. Extended workforce members must follow DHHS and agency policies and procedures.

External Business Associate – A public/private contractor or a state government department or agency outside of DHHS that performs activities for, or on behalf of, a DHHS covered health care component that involves the use or disclosure of individually identifiable health information. For example, the NC Office of the Attorney General in the Department of Justice provides legal services, a covered function, for DHHS agencies.

F

Facility Information Security Official (FISO) – Staff identified within each DHHS division/office facility that is delegated the role, responsibility and authority as outlined in the respective security policies. The FISO serves as the primary point of contact and liaison between the division/office information security official.

Facility Security Plan – A plan to safeguard the premises and buildings (exterior and interior) from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering or theft.

Family Educational Rights Privacy Act (FERPA) – A federal law [20 United States Code (USC) § 1232g; 34 Code of Federal Regulations (CFR) Part 99] that sets forth the rights of a student’s parents and of students, and the correlating duties of education agencies and institutions regarding education records. The law applies to all schools that receive funds under an applicable program of the United States Department of Education.

File Transfer Protocol (FTP) – A TCP/IP protocol specifying the transfer of text or binary files across the network.

File Integrity Checkers – A file integrity checker computes and stores a checksum (?) for every file to be protected and establishes a database of the checksums. It provides a tool for system administrators to recognize when changes were made to files, particularly authorization changes.

Firewall – A term used for software or devices used to control access from one network, usually external, to another internal network. A secured system passing and examining traffic between an internal trusted network and an external untrusted network such as the Internet. Firewalls can be used to detect, prevent, or mitigate certain types of network attack.

G

Gateway – A network point that acts as an entrance to another network.

Guideline – A best practice or recommended approach for DHHS divisions/offices to use when implementing a policy.

H

Health Information – Any information, whether oral or recorded in any form or medium, that:

- Is created, maintained, or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
- 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 services to an individual.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) – HIPAA is a federal law (Public Law 104-191, also known as the Kennedy-Kassenbaum Bill) that focuses on improving access to health insurance. Additional intents were to limit fraud and abuse and simplify health care administration. Within the legislation, specific requirements are required of health care providers, clearinghouses, and service providers for the standardization of electronic transaction, and the privacy and security of “protected health information”.

I

Identification and Authentication – Methods to determine a user’s identity, verify that it is correct and establish accountability.

Information Processing Resources – Electronic computing and communications hardware, software, networks, and information.

Information Security Official (ISO) – Staff identified in each DHHS division/office who are delegated the roles, responsibilities and authorities as outlined in the DHHS Security Organization manual. The division/office security official serves as the primary point of contact between the division/office and the DHHS Privacy and Security Office (PSO).

Information System – Information System is defined as an interconnected set of information resources under the same direct management control that shares common functionality. A

system normally includes hardware, software, information, (and the interconnections, including wireless technology, between components) data, applications, communications, and people.

Incident (also ITS Security Incident) – A violation of DHHS computer security policies, acceptable use policies, or standard computer security practices. An adverse event where a North Carolina information technology resource is accessed or used without authorization; attacked or threatened with attack, or used in a manner inconsistent with established policy with the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information.

Individually Identifiable Health Information (IIHI) – A subset of health information that is collected from a client, including demographic information, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse;
- 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
 - Identifies the individual; or
 - There is a reasonable basis to believe the information can be used to identify the individual.

NOTE: According to the HHS Office of Civil Rights (OCR), the identification of a health care provider/facility is considered to be indicative of the provision of health care services; therefore, if an individual identifier for a DHHS client is combined with the name of a health care provider; such information is considered individually identifiable health information.

Integrity – Integrity is the need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete.

Internal Business Associate – A DHHS division or office or component within a DHHS division or office that performs activities for or on behalf of a DHHS covered health care component that involves the use or disclosure of individually identifiable health information. An internal business associate can be in the same or different agency as the covered health care component. For example, the central billing office in the DHHS Office of the Controller is an internal business associate of the DMH/DD/SAS facilities because the central billing office provides a billing service for those facilities.

Internal Review or Audit – The in-house review of the records of system activity (for example, logins, file accesses, security incidents) maintained by the department or divisions/offices.

Intrusion Detection – The process of monitoring the events occurring in a system or network, by detecting signs of security problems. The purpose of intrusion detection software (IDS) is to detect unauthorized access or misuse of a computer system.

Intrusion Prevention – The ability to prevent or stop unauthorized invasion, access or entry to servers, files, or computer systems before the security event is executed.

Intrusion Protection – Intrusion protection provides the ability to detect, prevent, respond to, and manage security threats in real time. Effective intrusion protection isn't one security

product or method. Intrusion protection should encompass (1) Network-based intrusion protection, (2) Host-based intrusion detection and prevention, and (3) Decoy-based (or "honeypot") technology.

ISO (International Organization for Standardization) 17799 – An internationally recognized security standard that establishes general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ITS is moving forward with adoption of these standards as a cornerstone to their security program.

J

(Left Blank Intentionally)

K

(Left Blank Intentionally)

L

Least Privilege - Least Privilege is the principle of allowing users or applications the least amount of permissions necessary to perform their intended function.)

Local Area Network (LAN) – A communication network that serves several users within a specified geographic area. It is typically made up of servers, workstations, a network operating system and a communications link.

Log – A record of information or events usually arranged in temporal sequence, i.e., the order in which they occur.

M

Mainframe – A computer with extensive capabilities and resources that can share facilities with other computers and support simultaneous users.

Malicious Software – Software, for example, a virus, designed to damage or disrupt a system.

Malware – Short for "malicious software," malware refers to software programs designed to damage or do other unwanted actions on a computer system. Common examples of malware include viruses, worms, Trojan horses, and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it.

Modem Security – Software programs that detect the use of unauthorized modems that might be used to bypass security measures.

N

National Institute of Standards and Technology (NIST) – Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life. The organization publishes computer security standards and guidelines on the Computer Security Resource Center web site at <http://csrc.nist.gov>.

NCID- North Carolina Identity (NCID) is the ITS enterprise approach for application access authorization and account management.

Network – A system or interconnected computers and the communications equipment used to connect them. Networks can interconnect with other networks and contain subnetworks.

Network Management – The discipline that describes how to monitor and control the managed network to ensure its operation and integrity and to ensure that all communication services are provided in an efficient manner.

Network Mapping – The use of a port scanner to identify all active hosts connected to an organization's network, the network services operating on those hosts (e.g., file transfer protocol and hypertext transfer protocol), and the specific application running the identified service.

Network Security – The protection of all network resources from perceived risks. The architecture, standards and technical controls required to protect the confidentiality, integrity and availability of data transmitted over the network.

Non-Repudiation – The assurance that a party cannot later deny originating data. Non-repudiation is the ability for a system to prove that a specific user and only that specific user sent a message and that it hasn't been modified.

North Carolina Integrated Information Network (NCIIN) – Refers to a web of interoperable networks, within the state, that transmits data, text, images, voice, and video. The NCIIN is also referred to as the state network.

O

Object Reuse – The reassignment and reuse of a storage medium that once contained data. To be properly reused, storage media must contain no residual data (or magnetic remanence).

Operating System – Software that controls the execution of computer programs and provides services such as scheduling and input/output control.

Owner – Individual that has responsibility for specific data, data types, or systems. The owner has the responsibility for determining the sensitivity of data and taking adequate steps to protect that data.

P

Packet – Data unit that is routed from source to destination in a packet-switched network. A packet contains both routing information and data.

Password – A character string used to authenticate an identity. A confidential numeric and/or character string used in conjunction with a user ID to verify the identity of the individual attempting to gain access to a computer system.

Password Authentication – Access is authenticated following the “User ID and Password Protection Standard”, using at least six-character passwords. All passwords shall be encrypted in storage and in transit where supported by the application and/or system.

Password Cracking – A process by which a program is used to identify weak password usage.

Patch – A quick modification of a program, which is sometimes a temporary fix until the problem can be solved more thoroughly. A security vulnerability or a loophole in a system may be fixed with a patch.

Penetration Testing – A live test of the effectiveness of security defenses by simulating the actions of attackers. Part of security testing in which evaluators attempt to circumvent the security features of a system.

Pharming – The act of misdirecting the user to fraudulent sites or proxy servers without their knowledge. The user may type a legitimate URL into the address bar of the browser, but the hijacking occurs through malicious techniques.

Phishing – The act of sending an email message to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information to be used for fraudulent purposes such as identify theft. These techniques are referred to as social engineering and technical subterfuge and are used to steal personal identity data.

Physical Access Testing – The performance of one or more tests to determine the effectiveness of physical access controls.

Physical Security – The physical and environmental design, standards and controls required to protect people, property and information assets in the workplace.

Port – An interface point between the CPU and a peripheral device.

Policy – A governing principle or directive that establishes the security requirement(s) for an organization. Note: DHHS management has issued a set of security policies that are published in a security manual located at <http://info.dhhs.state.nc.us/olm/manuals/dhs/pol-80/man/index.htm>.

Privacy – The state of being free from unsanctioned intrusion.

Privacy of health information refers to the legal right to, or public expectation of, confidentiality in the collection and sharing of an individual’s identifying health information. Privacy problems exist wherever individually identifiable health information that is collected and stored is disclosed for purposes other than that for which it was gathered or against the express wishes of the client. The challenge in health information privacy is to share data for valid purposes (e.g., state mandated health reporting, health screening, and disease registries), while protecting the individually identifiable health information from improper use. In the majority of cases, individuals should retain the right to decide to whom and under what circumstances their individually identifiable health information will be disclosed.

Procedure – A set of interrelated steps and instructions to be specifically followed in order to implement the policy and standard.

Process – A series of steps, actions or operations used to bring about a desired result.

Protected Health Information (PHI) – A term used in the HIPAA Privacy Regulations that has the same meaning as ‘individually identifiable health information.’ The term ‘individually identifiable health information’ is used in the DHHS Privacy Policies to

describe any information, including demographic information that has the potential of tying the identity of a client to his/her health information.

Protocol – A standardized, formal description of message formats and the associated rules computers must follow to exchange those messages. A set of rules and formats that permits entities to exchange information

Public Access – Open access to information resources. Some North Carolina state web pages and applications are accessible to the public via the internet.

Public Key Infrastructure (PKI) – A PKI (public key infrastructure) enables users of a public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates. The functions required to issue and manage the public key certificates needed for authentication. A Public Key Infrastructure consists of all the supporting services required to issue and manage digital certificates.

Public Records – All documents, papers, letters, maps, books, photographs, films, sound recordings, magnetic or other tapes, electronic data-processing records, artifacts, or other documentary material, regardless of physical form or characteristics, made or received pursuant to law or ordinance in connection with the transaction of public business by any agency of North Carolina government or its subdivisions.

Q

(Left Blank Intentionally)

R

Recovery Time Objective (RTO) – The amount of time allowed for the recovery of a business function or resource after a disaster occurs.

Remote Access – The ability of a resource to access the state’s network via an external network connection. Remote access generally occurs from remote locations such as homes, hotel rooms, and off-site offices; however it could also occur locally within an agency’s physical facilities.

Removable Storage Device – Disk drives, flash drives, or other means that store information which can be removed and stored remotely.

Resource Access Control Facility (RACF) – RACF is also known as IBM secure way security server. RACF is primary mainframe security software.

Risk – An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result; the likelihood that vulnerability may be exploited or that a threat may be harmful.

Risk Assessment – The process used to determine risk management priorities by evaluating and comparing the level of risk against predetermined acceptable levels of risk. A process that systematically identifies valuable system resources and threats to those resources, and quantifies loss exposures (i.e., loss potential) based on estimated frequencies and costs of occurrence.

Risk Management – The systematic application of management policies, procedures and practices to the tasks of identifying, assessing, treating and monitoring risk. The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources.

Router – A switching device that connects two (2) LAN segments or network layers, which use similar or different architectures, at the reference model network layer. The combination of hardware and software that links LANs and WANs together

S

Safeguard – Any protective measure or control that is prescribed to meet the security requirements specified for a system. Safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Security Architecture – A plan and set of principles that describe (a) the security services that a system is required to provide to meet the needs of its users, (b) the system elements required to implement the services, and (c) the performance levels required in the elements to deal with the threat environment. A complete system security architecture includes administrative security, communication security, computer security, emanations security, personnel security, and physical security. A complete security architecture needs to deal with both intentional, intelligent threats and accidental kinds of threats. See also security policy.

Security Work Group (SWG)- The DHHS Security Work Group consists of assigned representatives from dhhs divisions/offices. The group serves in an advisory capacity to the DHHS PSO in formulating information technology security policies, standards, guidelines and procedures for dhhs.

Segregation/Separation of Duties – A control that prevents errors or irregularities by assigning responsibility so that persons are not in a position to be the sole checker or verifier of their own work.

Service Level Agreement (SLA) – A contract agreement that defines the minimum performance measures at or above which service is considered acceptable.

Screen Lock - A special application, that cannot be opened without a password, that locks access to the computer every time either a mouse and computer keyboard are idle for a specified period of time or when specific combinations of keys are depressed simultaneously by the user.

Screen Saver – A special application that starts when activated by the user or every time the mouse and keyboard are idle for a specified period of time, which hides any information displayed on a computer monitor.

Secure Sockets Layer (SSL) – A widely used means for securely communicating between a web browser and web server. SSL works by using a public key to encrypt data that are transferred over the SSL connection.

Sniff – A surveillance technique used to detect or explore network traffic.

Spam – Unsolicited bulk commercial electronic mail.

Spoof – Attempt by an unauthorized entity to gain access to a system by posing as an authorized user. Also, sending messages or e-mail under a false identity.

Standard – The specification that establishes an approved methodology or technology that is to be implemented.

Switches – Devices that bridge two separate networks to form a logical network (e.g. joining an ethernet and token network). Switches have large number of ports and operate at faster speeds than other devices such as bridges.

System – An assembly of components (hardware, software, procedures, human functions and other resources) united by some form of regulated interaction to form an organized whole. A group of related processes.

System Administrator – An individual responsible for maintaining a multi-user computer system, including a local-area network (LAN).

System Development Life Cycle (SDLC) – A methodology used to develop, maintain, and replace information systems. Typical phases in the SDLC are: analysis, design, development, integration and testing, implementation, etc.

System Owner – The manager or agent responsible for the business use of the information or application.

T

TCP/IP – “Transmission control protocol/internet protocol,” the suite of communication protocols used to connect hosts on the internet. TCP establishes a virtual connection between a destination and a source and enables the exchange of streams of data. IP specifies the format of packets and the addressing scheme.

Third Party Contractors – Non-state employees, such as vendors, suppliers, individuals, contractors, and consultants, including their employees and agents, responsible for providing goods or services to the state.

Threat – Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

Threat Analysis – The examination of all actions and events that might adversely affect a system or operation

Threat Source – Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability

Time out – A parameter related to an event designed to occur at the conclusion of a predetermined elapsed time.

Trojan Horse – A destructive program that masquerades as a benign application. It contains purposefully hidden malicious or damaging code. It may appear to be useful software but will actually do damage once installed or run on the computer. When activated, the results can vary. Trojans may change the desktop (such as adding icons), delete files, destroy information or create a backdoor on the computer to give unauthorized users access to the system, possibly allowing confidential or personal information to be compromised.

U

User / Normal User – An individual or application that accesses the state network. A person, system, application or defined group that has been authenticated to an ITS system and granted access only to those resources to which he has been granted authorization.

User ID – A unique symbol or character string that is used by a system to identify a specific user. The identifier by which a person or entity is recognized.

Update – Vendor-provided changes to software for either improved functionality or repair of known bugs or defects.

User Access – Access to applications by users for non-administrative purposes.

User Account – An established relationship between a user and a computer, network or information service. User accounts require a username and password, and a set of permissions.

V

Virtual Private Network (VPN) – A secure, private network that operates within a public network. VPNs enjoy the security of a private network via access control and encryption.

Virus – A destructive program or piece of code that is loaded onto a computer without the knowledge of the user and which runs against one’s wishes. Viruses spread from computer to computer using a variety of methods, with the ability to replicate themselves. They typically attach themselves to a program and modify it. Viruses may transmit themselves across networks and attempt to bypass security systems.

Voice Over IP – The technology used to transmit voice conversations over a data network using the internet protocol. The data network involved might be the internet itself, or a corporate intranet, or managed networks used by local or long distance carriers and ISPs.

Vulnerability – A weakness in an information system and procedures including technical, organizational, procedural, administrative, or physical weaknesses.

Vulnerability Assessment – A measurement of vulnerability which includes the susceptibility of a particular system to a specific attack and the opportunities available to a threat agent to mount that attack; an evaluation of the current security posture which is intended to reveal security-related control strengths and control weaknesses.

Vulnerability Scanners – Tools used to identify not just the hosts and open ports but any associated vulnerabilities. Most vulnerability scanners probe for a finite number of problems and attempt to provide information on mitigating discovered vulnerabilities.

W

Waiver – Authorization to operate either using a new, atypical approach or while not in compliance with a defined standard.

Wide Area Network (WAN) – A data telecommunications network typically extending a LAN outside a building, over common carrier lines, to link to other LANs that are geographically dispersed. Point-to-point wireless access points may be used in lieu of common carrier lines.

Worm – A worm is similar to a virus. A worm spreads from computer to computer but unlike a virus, has the ability to infect other computers, etc., without the help of a person. The biggest danger of a worm is its ability to replicate itself on the system without one’s knowledge. One example would be for a worm to send a copy of itself to everyone listed in an e-mail address book.

Workforce – Employees, volunteers, contractors, vendors and other persons whose conduct, in the performance of DHHS, is under the direct control of the department or divisions/offices, whether or not they are paid or via contract.

X

(Left Blank Intentionally)

Y

(Left Blank Intentionally)

Z

(Left Blank Intentionally)

Enforcement

For enforcement questions or clarification on any of the information contained in this policy, please contact DHHS security officer (DHHS.Security@ncmail.net). For general questions about department-wide policies and procedures, contact the [DHHS Policy Coordinator](#)