

DHS Information Security Glossary

ACCESS TO INFORMATION	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system resource.
ACCESS LEVELS	<p>1) In security, the level of authority required from an entity to access a protected resource. Note: An example of access level is the authority to access information at a particular security level.</p> <p>2) The hierarchical portion of the security level used to identify sensitivity of information-system (IS) data and the clearance or authorization of users. Access level, in conjunction with the nonhierarchical categories, forms the sensitivity label of an object. (INFOSEC) -Telecom Glossary 2K</p>
ACCESS RIGHTS	The privilege to use computer information in some manner. For example, a user might be granted read access to a file, meaning that the user can read the file but cannot modify or delete it. Most operating systems have several different types of access privileges that can be granted or denied to specific users or groups of users. (Webopedia)
ADMINISTRATIVE SAFEGUARDS	Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect confidential and/or sensitive information and to manage the conduct of DHS' workforce in relation to the protection of that information.
APPLICATION	An application is any program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of application programs include word processors; database programs; Web browsers; development tools; drawing, paint, and image editing programs; and communication programs.
AUDIT TRAILS	A data security system should maintain detailed logs of who did what and when and also if there are any attempted security violations. Logs provide information that allows the system auditor to determine who initiated the transaction, the time of the day and date of entry, the type of entry, what fields were affected, and the terminal used.
AUTHENTICATION	The validation of the user's identity.
AVAILABILITY	Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.

DHS Information Security Glossary

CCERT	Los Angeles County's Computer Emergency Response Team that has responsibility for response and reporting of Information Technology (IT) security incidents.
CERT	Computer Emergency Response Team that has responsibility for response and reporting of IT security incidents within an organization.
COMPUTER SYSTEM	Any equipment or interconnected system or subsystems of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information; including computers; ancillary equipment; software, firmware, and similar procedures; services, including support services; and related resources.
CONFIDENTIALITY	Assurance that data is protected against unauthorized disclosure to individuals, entities or processes.
CONTINGENCY PLAN	A plan for emergency response, backup procedures, and post-disaster recovery. Synonymous with disaster plan and emergency plan.
CONTINGENCY PLANNING	A planned response to high impact events to maintain a minimum acceptable level of operation.
DATA	A collection of observations of fact.
DATABASE	A collection of interrelated data, often with controlled redundancy, organized according to a schema to serve one or more applications; data is stored so that it can be used by different programs without concern for the data structure or organization. A common approach is used to add new data and to modify and retrieve existing data.
DCERT	Departmental Computer Emergency Response Team. The Department's CERT that has responsibility for response and reporting of IT security incidents.
DEVICE	Any equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
DHS INFORMATION RESOURCES	Los Angeles County Department of Health Services' computer systems. See definition of <i>computer systems</i> above.
DISASTER RECOVERY	A plan for the restoration of lost data, or the reconciliation of conflicting or erroneous data, after a system failure due to natural or manmade disaster.

DHS Information Security Glossary

DISO	Los Angeles Department of Health Services' Information Security Officer
ELECTRONIC INFORMATION SYSTEMS	An automated set of methods, software, and hardware that operates as a whole to accomplish a prescribed task with regard to data.
ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)	<p>1) Individually identifiable health information:</p> <p>(1) Except as provided in paragraph (2) of this definition, that is:</p> <ul style="list-style-type: none"> (i) Transmitted by electronic media; (ii) Maintained in electronic media; <p>(2) Protected health information excludes individually identifiable health information in:</p> <ul style="list-style-type: none"> (i) Education records (ii) Employment records held by a covered entity in its role as employer. <p>2) Protected Health Information that is transmitted by electronic media or is maintained in electronic media. This does not include health information contained in employment records held by DHS in its role as employer.</p>
ENCRYPTION	The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission, or when it is stored on a transportable magnetic medium. (Microsoft Press Computer Dictionary)
EPHI	See, Electronic Protected Health Information
FACILITY	<p>Facility encompasses all hospital/MACC and Public Health organizational units within LA DHS.</p> <p>Hospital/MACC includes the associated cluster sites that it governs.</p> <p>Recognized Facilities are; HDHS, KDMC, HUCLA, LAC+USC, OVMC, RLMC, PH, and HSA.</p>
FACILITY CHIEF INFORMATION OFFICER (Facility CIO)	A Chief Information Officer in a DHS Facility.
FACILITY INFORMATION SECURITY COORDINATOR (FISC)	A person with the responsibility for information security in a DHS Facility.

DHS Information Security Glossary

FACILITY PRIVACY COORDINATOR/OFFICER	A person with the responsibility for privacy in a DHS Facility.
GUIDELINES	General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.
HYBRID ENTITY	A single legal entity that acts as provider and health care plan.
ILLEGAL ACCESS AND DISCLOSURE	Activities of employees that involve improper systems access and sometimes disclosure of information found thereon, but not serious enough to warrant criminal prosecution.
INCIDENT	An occurrence or event that interrupts normal procedure or precipitates a crisis.
INFORMATION	Any communication or reception of knowledge, such as facts, data, or opinions; including numerical, graphic, or narrative forms, whether oral or maintained in any other medium, including computerized databases, paper, microform, or magnetic tape.
INFORMATION TECHNOLOGY (IT)	A term that encompasses all forms of technology used to create, store, exchange, and use information in its various forms (business data, personal health information, voice conversations, still images, motion pictures, multimedia presentations, and other forms, including those not yet conceived).
INFORMATION TECHNOLOGY ASSETS/RESOURCES	See definition of computer system above.
INTEGRITY	Assurance that data is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.
INTEGRITY CONTROL	The mechanism or procedure that assures data or information is protected against unauthorized, unanticipated, or unintentional modification and/or destruction.
INTERNET	A worldwide electronic system of computer Medical Centers which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.
LOCAL AREA MEDICAL CENTER (LAN)	A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the

DHS Information Security Glossary

	<p>Medical Center (Microsoft Press Computer Dictionary)</p> <p>Local Area Medical Centers commonly include microcomputers and shared (often-expensive) resources such as laser printers and large hard disks. Most modern LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger Medical Centers.</p>
MALICIOUS SOFTWARE	<p>The collective name for a class of programs intended to disrupt or harm systems and Medical Centers. The most widely known example of malicious software is the computer virus; other examples are Trojan horses and worms.</p>
MEDIA	<p>Hard copy (including paper), PC/workstation diskettes, and other electronic forms by which data is stored, transported, and exchanged. The need to protect information confidentiality, integrity, and availability applies regardless of the medium used to store the information. However, the risk exposure is considerably greater when the data is in an electronically readable or transmittable form compared to when the same data is in paper or other hard copy form.</p>
MODEM	<p>Modem is short for modulator/demodulator, a communications device that enables a computer to transmit information over a standard telephone line. Modems convert digital computer signals into analog telephone signals (modulate) and the reverse (demodulate). (Microsoft Press Computer Dictionary)</p>
MEDICAL CENTER	<p>A group of computers and associated devices that are connected by communications facilities. A Medical Center can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A Medical Center can be as small as a LAN consisting of a few computers, printers and other devices, or it can consist of many small and large computers distributed over a vast geographic area. Small or large, a computer Medical Center exists to provide computer users with a means of communicating and transferring information electronically. (Microsoft Press Computer Dictionary)</p>
MEDICAL CENTER INFORMATION SECURITY OFFICER (ISO)	<p>LAC+USC Specific: Person responsible for all aspects of Medical Center Information Security Policy compliance.</p>
PASSWORDS	<p>A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM)</p> <p>Passwords are most often associated with user</p>

DHS Information Security Glossary

	<p>authentication. However, they are also used to protect data and applications on many systems, including PCs. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).</p>
PERIODIC	Recurring from time to time; intermittent.
PERSONNEL SECURITY	Personnel security refers to the procedures established to ensure that each individual has a background which indicates a level of assurance of trustworthiness which is commensurate with the value of resources which the individual will be able to access.
PHI	See Protected Health Information
PHYSICAL SECURITY	The application of physical barriers and control procedures as preventive measures and countermeasures against threats to resources and sensitive information.
POLICY	A high-level statement of departmental beliefs, goals, and objectives and the general means for their attainment for a specified subject area.
PROCEDURES	Define the specifics of how the policy and the supporting standards and guidelines will actually be implemented in an operating environment.
PROTECTED HEALTH INFORMATION (PHI)	<p>PHI means individually identifiable information relating to past, present and future physical or mental health or condition of an individual, provision of health care to an individual, or the past, present or future payment for health care provided to an individual.</p> <p>Protected health information excludes individually identifiable health information in Education records and Employment.</p> <p>The term PHI, as used in the IT security policies 935 series, refers to electronic Protected Health Information.</p>
RISK	<p>The potential for harm or loss. Risk is best expressed as the answers to these four questions:</p> <ul style="list-style-type: none"> (1) What could happen? (What is the threat?) (2) How bad could it be? (What is the impact or consequence?) (3) How often might it happen? (What is the frequency?)

DHS Information Security Glossary

	<p>(4) How certain are the answers to the first three questions? (What is the degree of confidence?)</p> <p>The key element among these is the issue of uncertainty captured in the fourth question. If there is no uncertainty, there is no “risk” per se.</p>
RISK ASSESSMENT	The identification and study of the vulnerability of a system and the possible threats to its security.
RISK MANAGEMENT	The process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.
SAFEGUARDS	Administrative, physical and technical actions or measures, and policies and procedures to protect Protected Health Information (PHI) and other confidential information.
SECURITY	All of the safeguards in an information system, including hardware, software, personnel policies, information practice policies, disaster preparedness, and the oversight of all these areas. The purpose of security is to protect both the system and the information it contains from unauthorized access from outside and from misuse from within. Through various security measures, a health information system can shield confidential information from unauthorized access, disclosure and misuse, thus protecting privacy of the individuals who are the subjects of the stored data. (HIPAA Security Standard)
SECURITY LEVEL DESIGNATION	A rating based on the sensitivity of data (i.e., the need to protect data from unauthorized disclosure, fraud, waste, or abuse), and the operational criticality of data processing capabilities (i.e., the consequences where data processing capabilities to be interrupted for some period of time or subjected to fraud or abuse). There are four security level designations for data sensitivity and four security level designations for operational criticality. The highest security level designation for any data or process within an information system is assigned for the overall security level designation.
SECURITY VIOLATION	An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources. This includes, but is not limited to, unusual or apparently malicious break-in attempts (either local or over a Medical Center), virus or Medical Center worm attacks, or file

DHS Information Security Glossary

	or data tampering, or any incident in which a user, either directly or by using a program, performs unauthorized functions.
SENSITIVE DATA	Data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission (e.g., proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.).
SENSITIVE INFORMATION	Any information that, if lost, misused, accessed or modified in an improper manner, could adversely affect the county interest, the conduct of county programs, or the privacy to which individuals are entitled.
SEPARATION OF DUTIES	Separation of duties refers to the policies, procedures, and organizational structure that help ensure one individual cannot independently control all key aspects of a process or computer-related operation. Independent control would enable the individual to conduct unauthorized actions or gain unauthorized access to assets or records without detection. Strict controls involving the maintenance or use of IT assets would ensure that no individual has the ability to both perpetrate and conceal an accidental or intentional breach of IT security.
SIGNIFICANT CHANGE	A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, changing from batch to online processing, adding dial-up capability, and increasing the equipment capacity of the installation. (DHHS Definition)
STANDARDS	Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to be meaningful and effective.
VULNERABILITY	A condition or weakness in (or absence of) security procedures, technical controls, physical controls, or other controls that could be exploited by a threat.
WIDE AREA MEDICAL CENTER (WAN)	1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM)

DHS Information Security Glossary

	2) A WAN is a communications Medical Center that connects geographically separated areas (Microsoft Press Computer Dictionary).
WORKFORCE MEMBER	Employees, volunteers, trainees and other persons whose conduct in the performance of work for the department, its offices, programs or facilities, is under the direct control of the department, office, program or facility, regardless of whether they are paid by the department.
WORKSTATION	A workstation is a computer built around a single-chip microprocessor. Less powerful than minicomputers and mainframe computers, workstations have nevertheless evolved into very powerful machines capable of complex tasks. Technology is progressing so quickly that state-of-the-art workstations are as powerful as mainframes of only a few years ago, at a fraction of the cost. (Microsoft Press Computer Dictionary)
WORM	A worm is a program that propagates itself across computers, usually by spawning copies of itself in each computer's memory. A worm might duplicate itself in one computer so often that it causes the computer to crash. Sometimes written in separate segments, a worm is introduced surreptitiously into a host system either for fun or with intent to damage or destroy information.

RESOURCE ACRONYMS

CMS (Centers for Medicare & Medicaid Services)
 DHHS (U.S. Department of Health and Human Services)
 FISCAM (Federal Information Security Controls Audit Manual)
 HIPAA (Health Insurance Portability and Accountability Act of 1996)
 INFOSEC (National Information Systems Security Glossary)