COUNTY OF LOS ANGELES
Public Health

SUBJECT:	**PUBLIC HEALTH INFORMATION TECHNOLOGY AND SECURITY POLICY**	**PAGE**	1
		OF	16

POLICY No.: 1000	**EFFECTIVE DATE:** 04/15/09
APPROVED BY:	**SUPERSEDES:** DHS Policy No. 935

PURPOSE: To provide direction for the development and implementation of data security policies and procedures and to identify the data security officials and their responsibilities.

POLICY: The Department of Public Health (Public Health) is responsible for securing all electronic data, including Protected Health Information and other confidential information, while complying with the security requirements of all applicable regulatory, compliance and accreditation sources, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated there under, including the Security Standards for Electronic Protected Health Information at 45 Code of Federal Regulations (CFR) Parts 160 and 164, Medicare, Medi-Cal and JCAHO.

The term Public Health, as used in the Information Technology (IT) security policies 1000 series, refers to electronic Protected Health Information (ePHI).

Public Health must develop data security policies and procedures to ensure the security of Protected Health Information and other confidential information, and the hardware and systems used to obtain, utilize, and maintain such information.

All Public Health workforce members must comply with provisions of the Public Health data security policies. Any workforce member who fails to comply will be subject to disciplinary action in accordance with Public Health Policy No. 1201, Disciplinary Action for Failure to Comply with Privacy Policies and Procedures, Public Health Policy No. 741, Disciplinary Action, Civil Service Rule 18.031 and the Public Health Employee Evaluation and Discipline Guidelines.

Non-DPH County workforce members, contractors and agencies that violate the security policies and procedures are subject to sanctions or penalties imposed pursuant to the applicable contract or memorandum of understanding (MOU) and/or federal, state, local law.

To ensure compliance with the provisions of this policy, the following responsibilities have been designated to the following data security officials:

Departmental Information Security Officer (DISO)

A. Public Health must designate a DISO who is responsible for the development, implementation and maintenance of Public Health data security policies, procedures, and guidelines.

B. The DISO will assist Public Health managers and/or designated staff in the risk analysis and management process.

C. The duties of the DISO include, but are not limited to the following:

1. Chair the Departmental Information Security Steering Committee (DISSC).

2. Provide information security related technical, regulatory, and policy leadership.

3. Facilitate the development and implementation of the Public Health information security policies and procedures.

4. Coordinate information security efforts across the Facilities/Programs within Public Health in alignment with Countywide security policies.

5. Direct continuing information security training and education efforts.

6. Represent Public Health at the County Information Security Steering Committee (ISSC).

7. Report to the Public Health Chief Information Officer (CIO).

8. Ensure Public Health is in compliance with all laws, rules and regulations as it relates to the proper handling of data and electronic media.

9. Recommend new security standards as technology changes.

10. Coordinate Public Health-wide security software and hardware purchasing and licensing.

11. Review and approve data security implementation and risk management efforts.

D. The DISO or designee must review and approve the Risk Analysis Report.

E. The DISO or designee must review and approve the Public Health Facility/Program Master Security Management Report, Public Health Policy No.1001, Security Management Process: Risk Management.

F. The DISO must assist Public Health Facility/Program System Managers/Owners in implementing the access authorization procedures and determining the appropriate technical access controls.

G. The DISO or designee will coordinate the Departmental Computer Emergency Response Team (DCERT).

H. The DISO or designee and DCERT are responsible for determining the appropriate level of response to a security incident.

The DISO or designee must represent the department at the County Computer Emergency Response Team (CCERT) as the primary department CERT member (DCERT).

Facility/Program IT Director and/or Program Director

The duties of the Facility/Program IT Director, Program Director, and/or designee must include:

A. Management responsibility over all systems within their facility.

B. Ensure that Public Health Facility/Program System Managers/Owners conduct risk assessments for their data resources and information systems in accordance with Public Health procedures.

C. Create and periodically update the Facility/Program Master Security Management Report.

D. Ensure that Public Health Facility/Program System Managers/Owners develop plans to implement the Facility/Program Master Security Management Report's recommended safeguards and actions.

E. Ensure that Public Health Facility/Program System Managers/Owners establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.

F. Work with Public Health Facility/Program System Managers/Owners, Public Health managers and supervisors and Public Health Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

G. Ensure that Public Health Facility/Program System Managers/Owners authorize access to information resources under their control on a "need to know basis" for carrying out the essential job functions of the workforce members.

H. Ensure that Public Health Facility/Program System Managers/Owners implement procedures for establishing Public Health workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.

I. Ensure that Public Health Facility/Program System Managers/Owners implement procedures that modify a user's right of access to a workstation, transaction, program, process, or other mechanism, when such modification is necessary to align the workforce members' access with the workforce members' essential job functions.

J. Ensure that the Public Health Facility/Program System Managers/Owners respond to security incidents and emergency situations in a manner authorized and directed by the DISO or designee and DCERT

Facility/Program Information Security Coordinator (FPISC)

Each Public Health Facility/Program within Public Health must designate a FPISC responsible for working with the DISO in the implementation and maintenance of the data security policies, procedures and guidelines.

The duties of the FPISC include, but are not limited to the following:

A. Manage information security within the facility

B. Coordinate the development, implementation, and update of facility specific information security policies

C. Represent the Facility/Program at the DISSC

D. Assist the Facility DCERT member in responding to and documenting security incidents

E. Coordinate the implementation of the Public Health information security policies

F. Monitor Risk Management effectiveness

G. Report to the Facility/Program IT Director and/or Program Director

Departmental Information Security Steering Committee (DISSC)

The DISO and the FPISC will designate the members of the DISSC that must develop the appropriate security strategies for Public Health, taking into consideration the balance between heightened security and the Department's need to carry out its mission.

The DISSC's responsibilities are as follows:

A. Along with the DISO develop, review, recommend and update information security policies and procedures.

B. Develop, review, and recommend best practices, standards, and guidelines.

C. Develop, review, and recommend security awareness and training program.

D. Coordinate Inter-Facility communication and collaboration.

E. Recommend compliance self-evaluation.

F. Review compliance and audit documentation and ensure recommendations are implemented in a timely manner.

Public Health Facility/Program System Managers/Owners

Public Health Facility/Program System Managers/Owners security responsibilities include, but are not limited to, the following:

A. Establish rules for system use and protection of the Public Health and other confidential information as required in Public Health Policy No. 1201 Public Health Privacy and Security Compliance Program.

B. Work with Public Health Facility/Program IT Director and/or Program Director to develop and implement the Public Health Policy No. 1001, Security Management Process: Risk Management.

C. Establish, document, and implement procedures for reviewing information systems activity, including but not limited to audit logs, problem logs, system access reports, change control logs, and security incident reports.

D. Work with Public Health Facility/Program IT Director, Program Manager or designee, Public Health managers and supervisors and Public Health Human Resources to develop workforce security procedures and to coordinate those activities necessary to implement the workforce security procedures.

E. Implement procedures for establishing Public Health workforce member access to electronic information, for example, through access to a workstation, transaction, program, process, or other mechanism, that is both necessary and appropriate for the job functions of the workforce member.

F. Ensure that each workforce member with access has signed an acknowledgment of Public Health Policy No. 1016, Acceptable Use Policy for County Information

Technology Resources that defines their responsibility for protecting the confidentiality, integrity and availability of all Public Health information resources and identifying restrictions for utilizing those resources.

G. Determine the sensitivity and criticality of the resources for which they are responsible and develop, implement and maintain the Contingency Plan (CP) that commensurate with the criticality.

H. Ensure that appropriate physical safeguards and technical security policies are implemented.

J. Define the system's security requirements in a System Security Documentation.

K. Train and communicate to the workforce member the proper procedures for protecting the Public Health and other confidential information.

Public Health Human Resources (HR)

The security responsibilities of the Public Health Human Resources must include:

A. Work with Public Health Facility/Program System Managers/Owners to ensure proper workforce clearance procedures are implemented. Refer to Public Health Policy No. 723, Criminal Records Background Check/ Fingerprinting Policy.

B. Ensure that each new workforce member receives and signs acknowledgment of Public Health Policy No. 1016, Public Health Acceptable Use Policy for County Information Technology Resources during the new-hire orientation and that each workforce member completes the acknowledgment during the annual Performance Evaluation process. Signed acknowledgments will be filed in the workforce member's official personnel folder.

Workforce Managers and Supervisors

The security responsibilities of workforce managers and supervisors must include:

A. Determine workforce members' access rights and levels based on the workforce members' job responsibilities and authorize workforce members' access to electronic data systems, the Internet and Intranet systems.

B. Supervise the activities of Public Health workforce members in relation to the use and disclosure of electronic data.

C. Provide authorization and supervision to workforce members and others who need to be in areas where confidential and sensitive information may be accessed and take appropriate safeguards to ensure those who may be exposed

to confidential or sensitive information are made aware of the policies protecting that information.

D. Identify and supervise workforce members who work with confidential and/or sensitive information or who work in locations where confidential and/or sensitive information might be accessed.

Workforce Member

The security responsibilities of all Public Health workforce members must include:

A. Complying with the provisions of all relevant data security policies and procedures. Including but not limited to Public Health Policy No. 1201, Privacy and Security Compliance Program, Public Health Policy No. 1016, Acceptable Use Policy for County Information Technology Resources, and Public Health Policy No. 1008, Workstation Use and Security.

B. Reporting any and all suspected and actual breaches of information security to the Public Health DCERT.

DEFINITIONS:

Terms used in this policy and subsequent Public Health data security policies and procedures are included in the Public Health Information Security Glossary (Attachment I).

AUTHORITY: 45 code of Federal Regulations (CFR) Parts 160 and 164
Health Insurance Portability and Accountability Act of 1996 (HIPAA) Public Law 104-91
Board of Supervisor's Policies:
6.100 Information Technology and Security Policy

REFERENCE: Board of Supervisors Policies:
6.101 Use of County Information Technology Resources
6.102 Countywide Antivirus Security Policy
6.103 Countywide Computer Security Threat Response
6.104 Use of Electronic Mail (e-mail) by County Employees
6.105 Internet Usage Policy
6.106 Physical Security
6.107 Information Technology Risk Assessment
6.108 Auditing and Compliance
6.109 Security Incident Reporting
6.110 Protection of Information on Portable Computing Devices
6.111 Information Security Awareness Training
6.112 Secure Disposition of Computing Devices

ATTACHMENT I

PUBLIC HEALTH 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	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. 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
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 Protected Health Information and confidential and/or sensitive information and to manage the conduct of Public Health's workforce in relation to the protection of that information.
APPLICATION	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 identify of the user.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

AVAILABILITY	Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.
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.
PUBLIC HEALTH INFORMATION RESOURCES	Los Angeles County Department of Public Health's computer systems. See definition of *computer systems* 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.
DISO	Los Angeles Department of Public Health's 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.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)	1) Individually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; (2) Protected health information excludes individually identifiable health information in: (i) Education records (ii) Employment records held by a covered entity in its role as employer. 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 Public Health in its role as employer.
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	Facility encompasses all locations where there are Public Health Programs, Offices, Clinics, or administrative offices.
FACILITY CHIEF INFORMATION OFFICER (Facility CIO)	A Chief Information Officer in a Public Health Facility.
FACILITY INFORMATION SECURITY COORDINATOR (FISC)	A person with the responsibility for information security in a Public Health Facility.
FACILITY PRIVACY COORDINATOR/OFFICER	A person with the responsibility for privacy in a Public Health 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.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

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 networks which provides communications and resource sharing services to government employees, businesses, researchers, scholars, librarians and students as well as the general public.
LOCAL AREA NETWORK (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 network (Microsoft Press Computer Dictionary) Local Area Networks commonly include microcomputers and shared resources such as laser printers and large hard disks. Most modem LANs can support a wide variety of computers and other devices. Separate LANs can be connected to form larger networks.
MALICIOUS SOFTWARE	The collective name for a class of programs intended to disrupt of harm systems and networks. The most widely know example of malicious software is the computer virus; other examples are Trojan horses and worms.
MEDIA	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.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

MODEM	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)
NETWORK	A group of computers and associated devices that are connected by communications facilities. A network can involve permanent connections, such as cables or temporary connections made through telephone or other communications links. A network 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 network exists to provide computer users with a means of communicating and transferring information electronically. (Microsoft Press Computer Dictionary)
PASSWORDS	A confidential character string used to authenticate an identity or prevent unauthorized access. (FISCAM) Passwords are most often associated with user 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).
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.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

PROTECTED HEALTH INFORMATION (PHI)	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. Protected health information excludes individually identifiable health information in education records and employment. The term PHI, as used in the IT security policies 1000 series, refers to electronic Protected Health Information.
RISK	The potential for harm or loss. Risk is best expressed as the answers to these four questions: (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?) (4) How certain are the answers to the first three questions? (What is the degree of confidence?) The key element among these is the issue of uncertainty captured in the fourth questions. If there is no uncertainty, there is no "risk" per se.
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)

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

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 network), virus or network worm attacks, or file 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.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

SYSTEM	A set of integrated entities that operate as a whole to accomplish a prescribed task.
SYSTEM LIFE CYCLE	The period of time beginning when the software product is conceived and ending when the resultant software products are no longer available for use. The system lifecycle is typically broken into phases, such as requirements, design, programming and testing, installation, and operations and maintenance. Each phase consists of a well-defined set of activities whose products lead to the evolution of the activities and products of each successive phase.
SYSTEM MANAGER/OWNER	The person who is responsible for the operation and use of a system.
SYSTEM SECURITY PLAN	A basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements.
TECHNICAL SAFEGUARDS	The technology and the policy and procedures for its use that protect confidential and/or sensitive information and control access to it.
TELECOMMUNICATIONS	A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such a telephone lines, microwave delay, satellite link, or physical cable.
THREAT	An entity or event with the potential to harm the system. Typical threats are errors, fraud, disgruntled employees, fires, water damage, hackers, and viruses.
THREAT IDENTIFICATION	The analysis of recognized threats to determine the likelihood of their occurrence and their potential to harm assets.
USER	The person who uses a computer system and its application programs to perform tasks and produce results. (FISCAM) Any organizational or programmatic entity that utilizes or receives services from a facility. A user may be either internal or external to the agency organization responsible for the facility, but normally does not report to either the manager or supervisor or director of the facility or to the same immediate supervisor.
VIRUS	A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executable when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. A self-propagating Trojan horse, composed of a mission component, a trigger component, and a self-propagating competent.

ATTACHMENT I

PUBLIC HEALTH INFORMATION SECURITY GLOSSARY

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 NETWORK (WAN)	1) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. (FISCAM) 2) A WAN is a communications network 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)