Vermont Information Technology Leaders

HIPAA COMPLIANCE POLICIES AND PROCEDURES

Appendix:

Glossary of Terms

APPENDIX: GLOSSARY OF TERMS

Primary Source: CMS Information Systems Security Policy, Standards and Guidelines Handbook, version 1.0, February 19, 2002, with substantial additions and modifications.

ACCESS CONTROL A security mechanism used to grant users access to a system, based upon the identity of the user, and prevent access to unauthorized users. The user is commonly pre-defined to the system by the systems administrator with a User-id and password.

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.

ANTI-MALWARE Programs and systems used to combat, remove, and/or prevent system damage and/or security breaches caused by malicious software. (See MALICIOUS SOFTWARE)

APPLICATION SYSTEM Computer system written by or for a user that applies to the user's work; for example, a payroll system, inventory control system, or a statistical analysis system.

ASSETS These include information, software, personnel, hardware, and physical resources (such as the computer facility).

ASSET VALUATION The value of an asset consists of its intrinsic value and the near-term impacts and long-term consequences of its compromise.

AUDIT CONTROL is two-fold in that it is:

1. An independent review and examination of system records, operational procedures, and system activities to ensure compliance with established policies, procedures, and

2. A record of system activities that is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction, from its inception to output of final results.

AUTHENTICATION is:

1. The corroboration that an entity (User, Process, etc.,) is the one claimed.

2. A communications/network mechanism to irrefutably identify authorized users, programs, and processes, and to deny access to unauthorized users, programs, and processes.

AVAILABILITY Assurance that there exists timely, reliable access to data by authorized entities, commensurate with mission requirements.

BACKUP The process of creating exact copies of data in storage that can be used to restore lost data in contingency circumstances. Also, the information so copied.

BIOMETRICS identifies a human from a measurement of a physical feature or repeatable action of the individual (e.g., hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand written signature).

CERTIFICATION A technical evaluation with system owner's concurrence of a sensitive application and/or system to see how well it meets security requirements.

CHECKSUM is a count of the number of bits in a transmission unit that is included with the unit so that the receiver can determine whether the same number of bits arrived. If the counts match, it's assumed that the complete transmission was received.

COMPUTER SECURITY The concepts, techniques, technical measures, and administrative measures used to protect the hardware, software, and data of an information processing system from deliberate or inadvertent unauthorized acquisition, damage, destruction, disclosure, manipulation, modification, use, or loss.

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.

CONSEQUENCE (or IMPACT) ASSESSMENT An estimation of the degree of overall, aggregate harm or loss that could occur, e.g., lost business, failure to perform the system's mission, loss of reputation, violation of privacy, injury, or loss of life.

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 INTEGRITY ASSURANCE TECHNOLOGIES The technological means of assuring that information stored in electronic systems has not been altered or destroyed in an unauthorized fashion. For example, hardware-based data integrity assurance technologies may include error-correcting memory or duplicated storage systems; software-based data integrity assurance technologies may include mathematical checksums or other programmatic means of detecting anomalies in stored information.

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.

DIGITAL SIGNATURE An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters, such that the identity of a signer and the integrity of the data can be verified.

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.

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.

FIREWALLS Hardware and software components that protect one set of system resources (e.g., computers, networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

GUIDELINES General statements that are designed to achieve the policy's objectives by providing a framework within which to implement procedures.

HACKER A person who secretively invades others' computers, inspecting or tampering with the programs or data stored on them.

HANDHELD COMPUTING DEVICE A portable computing device, such as a personal digital assistant (PDA, Palm Pilot, Pocket PC and the like), wireless communicator (such as a Blackberry, Treo, or the like), or other device that may be used to retain and/or transmit information.

HIPAA The Health Insurance Portability and Accountability Act of 1996, under which the HIPAA Security Rule (and other HIPAA rules) is created.

HIPAA SECURITY RULE Published in the United States Federal Register as 45 CFR Parts 160, 162, and 164. Health Insurance Reform: Security Standards; Final Rule. February 20, 2003. Washington, DC.

INFORMATION SYSTEMS FACILITY An organizationally defined set of personnel, hardware, software, and physical facilities, a primary function of which is the operation of information technology. IS Facilities range from large centralized computer centers to individual standalone workstations.

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.

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. Also see PERSONAL OR PRIVATE INFORMATION.

INFORMATION SYSTEMS SECURITY (INFOSEC) The protection afforded to information systems to preserve the availability, integrity, and confidentiality of the systems and information contained in the systems. Protection results from the application of a combination of security measures, including crypto-security, transmission security, emission security, computer security, information security, personnel security, resource security, and physical security.

INTEGRITY Assurance that data 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.

INTRUSION DETECTION The use of programs and/or systems, and their monitoring, to detect attempts at improper system usage or information access and potential security breaches.

INTRUSION PREVENTION The use of programs and/or systems, and their monitoring, to prevent attempts at improper system usage or information access and potential security breaches.

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. Local area networks commonly include microcomputers and shared (often-expensive) 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.

MAJOR APPLICATION (MA) An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, modification of, or unauthorized access to the information in the application. Note: All applications holding electronic protected health information require some level of protection. Certain applications, because of the information in them, however require special management oversight and should be treated as major.

MALICIOUS SOFTWARE, aka "MALWARE" The collective name for a class of programs intended to disrupt or harm systems and networks. The most widely known 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 protection 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.

MISUSE OF ORGANIZATION PROPERTY The use of computer systems for other than official business that does not involve a criminal violation, but is not permissible under organization policies.

MITIGATION See Risk Mitigation.

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).

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, wired or wireless. 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.

NIST The National Institute of Standards and Technology, which (among many duties) creates standards and guides to be used in meeting various Federal requirements such as HIPAA and FERPA. NIST documents are frequently cited in the preamble to the HIPAA Security Rule.

PASSWORDS A confidential character string used to authenticate an identity or prevent unauthorized access. 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).

PATCHES Vendor-supplied system and software updates designed to correct faults or vulnerabilities in installed systems and devices.

PERIMETER SECURITY The use of technical means to protect the boundaries of systems and networks used to maintain or transmit personal or private information. Such means may include the use of firewalls and devices to detect or prevent unauthorized intrusion into systems and networks.

PERSONAL OR PRIVATE INFORMATION Information that is protected under applicable standards and regulations, such as payment cardholder information under the Payment Card Industry (PCI) Data Security Standard, protected health information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), or any other information that the unauthorized use or release of which would violate applicable standards or regulations, or which would jeopardize the confidentiality, integrity, or availability of proprietary information.

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 information resources which the individual will be able to access.

PHI An abbreviation for Protected Health Information (see below).

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 enterprise 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) The health information concerning health treatment of an individual and payment for such services. Virtually all health information held by a HIPAA covered entity is protected by HIPAA in some manner.

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 question. If there is no uncertainty, there is no "risk" per se.

RISK ANALYSIS A process whereby cost-effective security / control measures may be selected by balancing costs of various security control measures against the losses that would be expected if these measures were not in place.

RISK ASSESSMENT The identification and study of the vulnerabilities of a system and the possible threats to its security.

RISK MANAGEMENT The total process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk, including identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost/benefit analysis, selection, implementation and testing, security evaluation of safeguards, and overall security review. It encompasses the incorporation of the processes and results from both risk analysis and risk mitigation.

RISK MITIGATION The process of reducing the probability and / or consequences of an adverse risk event to an acceptable threshold.

SAFEGUARD ANALYSIS An examination of the effectiveness of the existing security measures, actions, devices, procedures, techniques, or other measures that reduce a system's vulnerability to a threat and identification of appropriate new security measures that could be implemented on the system.

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 without 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.

SECURITY INCIDENT HIPAA Definition: Attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or interference with operations in an information system. FIPS (Federal Information Protection Standard) Publication 200 Definition: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

SECURITY-RELATED EVENT An attempt to change the security state of the system (e.g., change discretionary access controls, change the security level of the subject, change user password, etc.). Also included are attempts to violate the security policy of the system (e.g., too many attempts to log on, attempts to violate the mandatory access control limits of a device, attempts to downgrade a file, etc.).

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 APPLICATION An application of information technology that requires protection because it processes sensitive data, or because of the risk and magnitude of loss or harm that could result from improper operation, deliberate manipulation, or delivery interruption of the application.

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 of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an

organization to accomplish its mission, proprietary data, and records about individuals requiring protection under PCI, HIPAA, or other regulation.

SIGNIFICANT CHANGE A physical, administrative, or technical modification that alters the degree of protection required. Examples include adding a LAN, changing from batch to on-line processing, adding dial-up capability, and increasing the equipment capacity of the installation.

STANDARDS Mandatory activities, actions, rules, or regulations designed to provide policies with the support structure and specific direction they require to meaningful and effective.

SYSTEM OWNER/MANAGER The official who is responsible for the operation and use of an application system.

SYSTEM SECURITY PLAN A basic overview of the security and privacy requirements of the subject system and the organization's plan for meeting those requirements.

TELECOMMUNICATIONS A general term for the electronic transmission of information of any type, including data, television pictures, sound, and facsimiles, over any medium such as telephone lines, microwave relay, 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.

TROJAN HORSE A computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. Also a destructive program disguised as a game, a utility, or an application. When run, a Trojan horse does something devious to the computer system while appearing to do something useful.

USER The person who uses a computer system and its application programs to perform tasks and produce results.

VIRUS A program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed 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.

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) A group of computers and other devices dispersed over a wide geographical area that are connected by communications links. A WAN is a communications network that connects geographically separated areas.

WORKFORCE The collection of employees, trainees, contractors, and volunteers whose conduct, in the performance of work or services for the organization, is under the direct control of such entity, whether or not they are paid by the entity.

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.

WORLD-WIDE WEB (WWW or WEB) The collection of electronic pages, (documents) that are developed in accordance with the HTML (hyper text markup language) Web format standard and may be accessed via Internet connections.

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.