

DEFINITIONS:

A.

ACTIVITY LOG, AUDIT LOG OR AUDIT TRAIL is a series of internal records of computer events, about an operating system, an application, or user activities. A computer system may have several audit logs, each devoted to a particular type of activity.

ADMINISTRATOR or **SYSTEM ADMINISTRATOR** or **SECURITY ADMINISTRATOR** means the individuals responsible for the technical administration of information assets, including networks, systems, applications, and databases.

APPLICATION LEVEL FIREWALLS

Application firewalls are hosts running proxy servers. The proxy applications are software components running on the firewall.

- a. Permits no traffic directly between networks.
- b. Performs elaborate logging and auditing of traffic passing through.
- c. Performs logging and access control.
- d. Can be used as network address translators, can mask the origin of the initiating connection.
- e. Can have a negative impact on performance and may make the firewall less transparent (impact outgoing traffic).

AS/400 or **Application System/400** refers to IBM's midrange business computer system platform for business applications.

ASSET means any item that is purchased by, owned by, leased to, contracted by, operated by, used by, controlled by, given to, supplied by, or in any other manner connected to Tenet. This includes everything from pens and paper to mainframe computing systems and other information assets.

- a. **TENET INFORMATION ASSETS** means, without limitation, confidential information, proprietary information, Protected Health Information, and Personally Identifiable Information owned or maintained by Tenet, as well as computers, networks, electronic files, records, services hardware, and software, regardless of type or media and that is owned, leased, operated, used or controlled by or on behalf of Tenet.

AUDIT TRAILS System, network and application logs, maintenance documents, and any other documentation that would help establish a trail of responsibility in an investigation.

AUTHORIZATION A written document signed by the Patient (or the Patient's Personal Representative) that contains the elements and statements required by state and federal law and grants specific permission to Use and/or Disclose PHI for a purpose that requires such written permission (e.g., a purpose other than Treatment, Payment, or Health Care Operations).

AVAILABILITY means the process of ensuring that systems and data are accessible to authorized users when they need it.

B.

BACKGROUND CHECK A background check is a complete check of an individual's criminal, civil, and financial status. This includes but is not limited to: local and federal criminal conviction records, lawsuit records, credit bureau records, driver's license records, and military records.

BASTION HOSTS A host sitting behind a firewall (router) which is a highly secured and heavily defended. This host is very resistant to attack.

BREACH means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of the protected health information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

BREACH NOTIFICATION RULE means the HIPAA privacy regulations set forth at 45 CFR part 164, Subpart D.

BUSINESS ASSOCIATE or **BA** means a person or entity (not an employee) who, on behalf of Tenet,

- a. Creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
- b. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or on behalf of Tenet, where the provision of the service involves the disclosure of individually identifiable health information from Tenet.

BUSINESS USE means activities that directly or indirectly support the business of Tenet.

C.

CARDHOLDER DATA includes the primary account number (PAN) along with any of the following data types: cardholder name, expiration date or service code. A service code is a three- or four-digit number on cards that use a magnetic-stripe.

CARDHOLDER DATA ENVIRONMENT (CDE) is the computer system or networked group of IT systems that processes, stores and/or transmits Cardholder Data or sensitive payment

authentication data. A CDE also includes any component that directly connects to or supports this network.

CENSUS REPORT/FACILITY DIRECTORY A publication that contains a patient's PHI such as name, location in the facility (room number), patient's general condition, and religion. This information is routinely used by facility staff members and is commonly made available in response to public inquiries.

CERTIFICATE AUTHORITY An entity responsible for the creation, distribution, tracking and revoking of cryptographic keys or digital certificates.

CHANGE CONTROL Configuration management. The function of tracking changes to assets. This encompasses, without limitation, changes to hardware, software, and networks.

CHIEF INFORMATION SECURITY OFFICER or **CISO** means the person within Tenet responsible for developing and implementing the Information Security program, which includes procedures and policies designed to protect enterprise communications, systems and assets from both internal and external threats.

COMPLIANCE INCIDENT MANAGEMENT SYSTEM (CIMS) means the internal system employed to document the investigation process of a Potential Compliance Matter from intake to resolution.

CLASSIFIED Any information, regardless of its format or media, that is "NON-PUBLIC" or has been assigned a security classification such as **PROPRIETARY** or **CONFIDENTIAL**

CLIENTS / CUSTOMERS Any individual, groups of individuals, companies, organizations, etc. which do business with Tenet.

CLOSED RECORDS Medical records of patients who have been discharged or released from the facility.

CLOUD STORAGE refers to the practice of using a network of remote servers hosted on the internet to store, manage, and process data, rather than a local server or personal computer.

The **COMMON RULE** is the Federal Policy for the Protection of Human Subjects codified in Title 45 CFR 46 (Public Welfare) Subparts A, B, C and D. The current U.S. system of protection for human research subjects is heavily influenced by the Belmont Report, written in 1979 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. The Belmont Report outlines the basic ethical principles in research involving human subjects.

CONFIDENTIAL INFORMATION means information that is protected above the **PROPRIETARY** level. **CONFIDENTIAL** information is the most sensitive business information intended strictly for use within and between Tenet and authorized third parties. Unauthorized disclosure of this information could adversely impact Tenet, its stockholders, its

business partners, its patients and/or its customers. **CONFIDENTIAL INFORMATION** shall have the same meaning as Proprietary Information.

CONFIDENTIALITY is the degree to which the privacy or secrecy of something can be trusted.

CONFIGURATION MANAGEMENT See Change Control.

COPYRIGHT *“A body of legal rights that protect creative works from being reproduced, performed, or disseminated by others without permission. The owner of copyright has the exclusive right to reproduce a protected work; to prepare derivative works that only slightly change the protected work; to sell or lend copies of the protected work to the public; to perform protected works in public for profit; and to display copyrighted works publicly. These basic exclusive rights of copyright owners are subject to exceptions depending on the type of work and the type of use made by others.”*

“The term work used in copyright law refers to any original creation of authorship produced in a tangible medium. Thus, works that can be copyrighted include literary pieces, musical compositions, dramatic selections, dances, photographs, drawings, paintings, sculpture, diagrams, advertisements, maps, motion pictures, radio and television programs, sound recordings, and-by special legislation passed by the Congress of the United States in 1980-computer software programs.”

“Copyright does not protect the idea or concept; it only protects the way in which an author has expressed an idea or concept. If, for example, a scientist publishes an article explaining a new process for making a medicine, the copyright prevents others from substantially copying the article, but it does not prevent anyone from using the process described to prepare the medicine. In order to protect the process, the scientist must obtain a patent.”

From Microsoft Encarta 96 Encyclopedia

COVERED FUNCTIONS Those functions of a Covered Entity that make the entity a Health Plan, Health Care Provider or Health Care Clearinghouse.

A **COVERED ENTITY** is a Health Plan, a Health Care Clearinghouse, or a Health Care Provider that transmits any health information in electronic form in connection with a transaction covered by the HIPAA Regulations.

CYBERSECURITY Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

CYBERSECURITY INCIDENT RESPONSE PLAN or **PLAN** means the plan developed by the CISO, in collaboration with Tenet’s Chief Information Officer and the Tenet Law

Department, to respond to various incidents that may impact negatively the security, confidentiality, integrity or availability of Tenet Information Assets.

CYBERSECURITY INCIDENT RESPONSE TEAM or **CIRT** means those Tenet employees designated with certain responsibilities in connection with the Cybersecurity Incident Response Plan and as identified therein.

D.

DATA is, without limitation, information of any kind that is collected, stored, transmitted, and/or printed. (E.g. A software program such as a spreadsheet, with no information added, has no data. When information is added, it contains data).

DATA CENTER A central location containing computer assets including, but not limited to, servers, magnetic storage devices, and network devices. This data center could service a single building or department, or serve a large geographical area.

DATA COMMUNICATION EQUIPMENT refers to networking and telecommunication computer hardware devices used to establish, maintain and terminate communication network sessions between a data source and its destination.

DATA USE AGREEMENT is. An agreement between the Covered Entity and the limited data set recipient that establishes the permitted uses and disclosures of information within the limited data set. 164.514 (e) (1)

DE-IDENTIFIED INFORMATION Health information that does not identify a patient and with respect to which there is no reasonable basis to believe that the information can be used to identify a patient.

DEMOGRAPHIC INFORMATION The patient's name, address and other contact information (such as phone number, e-mail address, etc.), age, gender, and insurance status.

DESIGNATED RECORD SET A group of records maintained by or for the facility that is:

- a. The medical records and billing records about patients maintained by or for the facility,
- b. The enrollment, payment, claims adjudication and case or medical management record systems maintained by or for a Health Plan, or
- c. Used, in whole or part, by or for the facility to make decisions about patients.

For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for the facility; the term "record" includes (a) patient information originated by another Health Care

Provider and used by the facility to make decisions about the patient, and (b) tracings, photographs, videotapes, digital and other images that may be recorded to document care of the patient.

DIGITAL CERTIFICATE A cryptographic signature used to provide irrefutable evidence of origin.

A **DISCLOSURE** means the release, transfer, provision of access to, or divulging of information in any other manner outside the Tenet Facility holding the information.

DUAL-HOMED GATEWAY A dual homed gateway runs proxy software and has two network interfaces. One interface for each network (outside, inside). All traffic passing through is blocked.

E.

ELECTRONIC MEDIA Means the mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media.

ELECTRONIC PROTECTED HEALTH INFORMATION or **ePHI** means protected Health Information that is created, received, maintained, or transmitted in electronic form by or on behalf of a covered entity.

EMANCIPATED MINOR typically means a minor who is to be treated as an adult for purposes of this policy. An emancipation order allows a minor to consent to “medical, dental or psychiatric care, without parental consent, knowledge or liability.” You should consult Regional Operations Counsel for the definition in your state.

ENCRYPTION The transformation of plaintext (words) into cipher text (unintelligible) by cryptographic techniques to protect data from disclosure during network transmissions.

EXTRANET A network connection between two companies. This does not have to be a geographical separation. If a company data center houses not only their own systems, but also those of a client, and a 10-foot cable separates the two systems, that cable constitutes an external connection.

F.

FACILITY A hospital, clinic, laboratory, office, site or building that is owned, leased, used or affiliated with Tenet.

FACILITY DIRECTORY/CENSUS REPORT See Census Report/Facility Directory.

FACILITY LEADERSHIP or FACILITY MANAGEMENT means the individuals responsible for the management at a Tenet Facility, including, but not limited to, the CEO, CFO, CIO, ISD, CNO, COO, Compliance Officer, Privacy and Security Compliance Officer, or their designated appointees.

FILE, DATA or OBJECT ADMINISTRATOR An individual delegated the authority and responsibility with respect to a file, set of files, or discreet data, too:

- a. Determine classification.
- b. Determine access authority.
- c. Assign custody.
- d. Specify physical controls over input and output.
- e. Determine the need for alternative processing capabilities.
- f. Monitor compliance with control requirements.

FINANCIAL REMUNERATION means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect remuneration does not include any payment for treatment of an individual.

FIREWALL A device or series of devices that separate and secure a company's internal networks from external networks, or, in some cases, sensitive internal networks from general internal networks.

FIRST SERVICE DELIVERY The first service delivery to a patient occurs on the date of the first Treatment encounter between a patient and a Health Care Provider. The first Treatment encounter may be face-to-face, telephonic or electronic. A conversation or encounter between a Health Care Provider and a patient, which only concerns a Payment or administrative issue is not the occurrence of a first service delivery.

G.

GROUP HEALTH PLAN A Group Health Plan is any plan, including insured and self-insured plans, established or maintained by an employer or by an employee organization, or by both, for the purpose of providing for its participants (e.g., current or former employees of the employer) or their beneficiaries, and to the extent that the plan provides medical care, that:

- a. Has 50 or more participants; or
- b. Is administered by an entity other than the employer that established and maintains the plan.

GROUP HEALTH PLAN SPONSOR The employer is the plan sponsor in the case of a plan maintained by a single employer; the organization is the plan sponsor in the case of a plan

maintained by an employee organization; and the plan sponsor is the association, committee, joint board of trustees or other group representing the plan participants in the case of a plan established by two or more employers.

GUIDELINES Procedures that show a ‘best practices’ approach to an issue, but do not mandate compliance. Reasons for non-compliance and alternative solutions shall be documented.

H.

HARDWARE The physical part of a computer system including the machinery and equipment.

A **HEALTH CARE CLEARINGHOUSE** is a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches that does either of the following functions:

- a. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
- b. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

HEALTH CARE OPERATIONS means any of the following activities of the Covered Entity to the extent that the activities are related to covered functions:

- a. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of Health Care Providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- b. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, Health Plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as Health Care Providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- c. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for

health care (including stop-loss insurance and excess of loss insurance), in accordance with the restrictions of applicable law;

- d. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- e. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- f. Business management and general administrative activities of the entity, including, but not limited to:
 - i. Management activities relating to implementation of and compliance with the requirements of this subchapter;
 - ii. Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.
 - iii. Resolution of internal grievances;
 - iv. The sale, transfer, merger, or consolidation of all or part of a Covered Entity with another Covered Entity, or an entity that following such activity will become a Covered Entity and due diligence related to such activity; and
 - v. Consistent with the requirements of applicable law, creating de-identified health information or a limited data set, and fundraising for the benefit of the Covered Entity.

A **HEALTH CARE PROVIDER** is a provider of services (as defined in the Medicare statute), a provider of medical or health services (as defined in the Medicare statute), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

HEALTH INFORMATION is broadly defined and includes any health information that pertains to a particular individual.

The **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996** or **HIPAA** was enacted by the U.S. Congress and signed by President Bill Clinton in 1996. Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the

establishment of national standards for the privacy and security of health data. The Administrative Simplification provisions also address electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

A **HEALTH PLAN** is an individual or group plan that provides, or pays the cost of, medical care. A Health Plan *includes* the following, singly or in combination:

- a. A Group Health Plan;
- b. A health insurance issuer;
- c. An HMO;
- d. Part A or Part B of the Medicare program;
- e. The Medicaid program;
- f. An issuer of a Medicare supplemental policy;
- g. An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy;
- h. An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers;
- i. The health care program for active military personnel under title 10 of the United States Code;
- j. The veterans' health care program under 38 U.S.C. chapter 17;
- k. The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS)(as defined in 10 U.S.C. 1072(4));
- l. The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.;
- m. The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.;
- n. An approved state child health plan under title XXI of the Act, providing benefits for child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.;

- o. The Medicare + Choice program;
- p. A high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; and
- q. Any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care.

A Health Plan *excludes* the following:

- a. Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and
- b. A government-funded program:
 - 1. Whose principal purpose is other than providing, or paying the cost of, health care; or
 - 2. whose principal activity is:
 - i. the direct provision of health care to persons; or
 - ii. the making of grants to fund the direct provision of health care to persons.

HEALTH PROFESSIONAL An individual who:

- a. has undergone formal training in a health care field;
- b. holds an associate or higher degree in a health care field, and holds a state license or state certificate in a health care field; and
- c. has professional experience in providing direct patient care.

HIGHLY CONFIDENTIAL INFORMATION means the subset of PHI that: (1) is maintained in psychotherapy notes; (2) is about mental illness, mental retardation and developmental disabilities; (3) is about alcohol or drug abuse or addiction; (4) is about HIV/AIDS testing, diagnosis or treatment; (5) is about communicable disease(s), including venereal disease(s); (6) is about genetic testing; (7) is about child abuse and neglect; (8) is about domestic abuse of an adult; or (9) is about sexual assault.

The **HIPAA PRIVACY RULE** (45 C.F.R. Part 160 and in Subparts A and E of 45 C.F.R. Part 164) establishes regulations for the use and disclosure of all Protected Health Information (PHI) including paper and electronic.

The **HIPAA SECURITY RULE**(45 C.F.R. Part 164, Subpart C) complements the Privacy Rule. The Security Rule deals specifically with Electronic Protected Health Information (ePHI). It lays

out three types of security safeguards required for compliance: administrative, physical, and technical.

HOST (or router) BASED AUTHENTICATION This authentication takes place when the firewall is a router and is using IP addresses to allow or disallow access. This configuration is vulnerable to "IP Spoofing" attacks.

HYBRID OR COMPLEX GATEWAY This is the combination of different types of firewalls. If those firewalls are set up in parallel, they do not complement each other (they do not increase the security of the network). The vulnerabilities on one firewall could allow an intruder to bypass the other firewalls. If they are set up in series, the features of each are combined to present a more complete protection package.

I

IN LOCO PARENTIS means a person or institution acting in lieu of a parent.

“INCIDENTAL DISCLOSURE” means the possible disclosure of PHI due to exposure to information while performing a service for Tenet that does not directly involve access, use and disclosure of PHI. Examples include, janitorial service, non-patient care employees/vendors in the patient room or waiting area.

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI) Information, including demographic information, that:

- a. Is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse,
- b. Relates to the past, present, or future physical or mental condition of a patient, the provision of health care to a Patient, or the past, present or future payment for the provision of health care to a Patient, and
- c. Identifies the patient or with respect to which there is a reasonable basis to believe the information can be used to identify the patient.

INFORMATION ASSET OR RESOURCE OR ASSET Without limitation, any computer, network, electronic file, record, service, hardware, software, regardless of type or media, that is purchased by, owned by, leased to, contracted by, operated by, used by or controlled by Tenet. This is to include ALL data residing in, or generated by those resources regardless of its format or storage device.

INFORMATION PRIVACY AND SECURITY INCIDENT means an event or situation that poses a threat to the integrity, confidentiality, or availability of information or systems. These incidents violate corporate policies and may violate local, state and federal laws or regulations. The direct result of Information Privacy and Security Incidents may include information disclosure, modification, destruction, or denial of system services. Indirect results of Information Privacy and Security Incidents may include loss of business, loss of computing capacity,

violation of privacy, civil lawsuits, loss of public confidence, or adverse consequences to other computing assets.

INFORMATION SECURITY means the protection of data against loss, modification, or unauthorized disclosure during its input to, storage in, or processing by a computing resource or at any point thereafter. The protection of computing resources from physical or logical damage, or any other act or occurrence that could decrease or degrade system availability.

INFORMATION SECURITY OFFICER The person designated by Tenet to be responsible for the development and implementation of the information security policies and procedures of Tenet.

An **INSTITUTIONAL REVIEW BOARD** or **IRB** is a board, committee, or other group formally designated by an institution to review bio-medical research involving humans as subjects, to approve initiation of and conduct periodic review of such research.

INTEGRITY means the degree to which something is free from corruption, i.e., protected from being damaged, altered, added or removed.

INTELLECTUAL PROPERTY is defined as ownership, copyrights, licenses, trademarks, data, programs, inventions, ideas, information, documentation, programs, inventions, formulas, procedures, and any other material, real or imagined, generated by an individual while working at or for Tenet Healthcare Corporation.

INTERNET A worldwide "network of networks" that uses Transmission Control Protocol/Internet Protocol (TCP/IP) for communications.

INTRANET A web based, browser accessed, internal service which allows Internet like searches and access for a company's internal use.

“ **INTERNET PROTOCOL**” (IP) A standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

J.

JOINT NOTICE A Notice of Privacy Practices (NPP) that applies to the joint activities of Covered Entities who participate in an Organized Health Care Arrangement (OHCA).

L.

LAN or Local Area Network An interconnected system of computers and peripherals. LAN users can share data stored on hard disks in the network and can share printers connected to the network. Access to a LAN is normally restricted to internal users; access from outside the LAN is normally controlled by a firewall

A **LIMITED DATA SET** is protected health information that can only be used or disclosed for research, public health, or Health Care Operations and excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: names; postal address information, other than town or city, state, and zip code; telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

LOGGING The act of writing information to a log file.

LOGS A file on a system that records events. This can include:

- a. System logs with startup, shutdown, errors and other information.
- b. Database logs showing access, changes.
- c. Application logs
- d. Network logs

M.

MALICIOUS SOFTWARE or MALWARE Unauthorized programs or code that have been introduced into organizational software with the intent to, and purpose of, causing damage to data, applications, or networks. Malicious code includes viruses, time bombs, logic bombs, Trojan horses, and worms.

MARKETING An arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses protected health information to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service., unless the communication is made:

- a. To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about: the entities participating in a Health Care Provider network or Health Plan network; replacement of, or enhancements to, a Health Plan; and health-related products or services available only to a Health Plan enrollee that add value to, but are not part of, a plan of benefits.
- b. For the treatment of the individual; or
- c. For case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, Health Care Providers, or settings of care to the individual.

MEMORANDUM OF UNDERSTANDING or MOU An agreement between governmental agencies or groups for the purpose of exchanging PHI as outlined in the limited data set.

MINIMUM NECESSARY When using or disclosing protected health information or when requesting protected health information from another Covered Entity, a Covered Entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

MODEM Short for modulator-demodulator. A device that allows digital signals to be transmitted and received over analog telephone lines. This type of device makes it possible to link a digital computer to the analog telephone system.

A **MOBILE DEVICE** is a small portable computing device such as a smartphone or tablet computer.

N.

The **NEED TO KNOW** concept indicates that permission to access or view something is not authorized in a general manner. Each individual being authorized access to data shall have a proven "need to know" which can be determined by their job description, authorized duties, real duties or by management decision. With limited exceptions, individuals must limit uses and disclosures of, and requests for, Protected Health Information (as defined below) to the minimum necessary to accomplish the intended and permitted purpose of the use, disclosure or request of this information. Tenet's Privacy Policies and Procedures define the minimum necessary information required by workforce members with specific job responsibilities and procedures for handling exception situations. Individuals must adhere to these policies and procedures.

NETWORK LEVEL FIREWALL Also called a "screened host firewall". Controls the access to a single host. Uses a router operating at the network level. The host is a bastion host. Decisions are based on the source, IP addresses and ports in individual IP packets. These firewalls can range from "simple" (a router), to much more sophisticated firewalls that maintain internal information about, but not limited to, the connections passing through them and the contents of data streams. This level of firewall can route traffic directly through the firewall. An incoming transmission must (usually) have a valid IP address.

NON-MARKETING means a communication about a product or service that encourages recipients of the communication to purchase or use the product or service and the communication is:

- a. To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, provided that any financial remuneration received by the Tenet Facility in exchange for making the communication is reasonably related to the Tenet Facility's cost of making the communication;

- b. For the following Treatment and Health Care Operation purposes, provided the Tenet Facility receives no financial remuneration for making the communication:
1. For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatment, therapies, health care providers, or settings of care to the individual;
 2. To describe a health-related product or service (or Payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, including communications about: the entities participating in a Health Plan network; replacement of, or enhancements to, a Health Plan; and health-related products or services available only to a Health Plan enrollee and add value to, but are not part of, a plan of benefits; or
 3. For case management or care coordination for the patient, or to direct or recommend alternative Treatments, therapies, Health Care Providers, or settings of care to the patient.

The **NOTICE OF PRIVACY PRACTICES** or **NPP** is a document that tells patients how a Covered Entity may use and disclose their PHI and also informs patients of their legal rights regarding their PHI.

O.

OPEN RECORDS Medical records of patients who are undergoing active inpatient or outpatient care and who have not been discharged or released from the facility.

OPT-IN Agreement by a user to participate in an activity or function of the Web site, provided after the Web site has fully disclosed the terms and conditions of participation to the user.

OPT-OUT A process by which a user declines to participate in an activity or function of the Web site.

An **ORGANIZED HEALTH CARE ARRANGEMENT** or **OHCA** is

- a. A clinically integrated care setting, such as a hospital, in which patients typically receive health care services from more than one Health Care Provider; or
- b. an organized system of health care in which more than one Covered Entity participates, and in which the participating Covered Entities:

- i. Hold themselves out to the public as participating in a joint arrangement; and
- ii. Participate in joint activities that include at least one of the following: (i) utilization review , in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf; (ii) quality assessment and improvement activities; or (iii) payment activities, if the financial risk for delivering health care is shared by participating Covered Entities and if PHI created or received by a Covered Entity is reviewed by participating Covered Entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

OWNER OF INFORMATION ASSET or INFORMATION ASSET OWNER The individual or group of individuals who own an information asset, and have authority to decide whether or not that system is necessary. This role typically resides with the Director of the department that has primary responsibility for the system's use.

P.

PASSWORD A secret code that is selected by each registered computer user and which, when recognized by a system's security program, in conjunction with the User ID, allows the user to access the computer system.

PASSWORD BASED AUTHENTICATION Authentication based on a unique User ID and password combination to determine access.

PATENT, *"in law, the abbreviated term for letters patent, in its most general sense a document issued by a government conferring some special right or privilege. In the U.S. the term is now restricted principally to patents for inventions granted under federal statute. The specific attributes of novelty of the item for which a patent is sought are called claims. A patent gives the inventor the exclusive privilege of using a certain process or of making, using, and selling a specific product or device for a specified period of time."*

From Microsoft's Encarta 96 Encyclopedia

PATIENT The person who is the subject of PHI and/or (as used in the Privacy Policies and Procedures), a person with authority, under the law, to act on behalf of the patient.

PAYMENT The activities undertaken by a Health Plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the Health Plan; or The activities undertaken by a Health Care Provider or Health Plan to obtain or provide reimbursement for the provision of health care; and The activities described above relate to the individual to whom health care is provided and include, but are not limited to:

- a. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
- b. Risk adjusting amounts due based on enrollee health status and demographic characteristics;
- c. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;
- d. Review of health care services with respect to medical necessity, coverage under a Health Plan, appropriateness of care, or justification of charges;
- e. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and
- f. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: name and address; date of birth; social security number; payment history; account number; and name and address of the Health Care Provider and/or Health Plan.

PRIVATE BRANCH EXCHANGE, or PBX a telephone switching system used internally to route calls from external lines to internal extensions. Controls, in part, voice mail and call forwarding.

PERSONAL COMPUTER or PC A computing device which contains its own memory, processing, storage and I/O devices, and which is intended for use by a single individual or a very small number of individuals.

PERSONAL PORTABLE ELECTRONIC COMMUNICATION DEVICES or PECD includes standard cellular phones, PDA/Smartphones (iPhones, Blackberry, Androids, etc.). Broadband access cards (laptop wireless connectors/air-cards) and numeric and alpha-numeric pager devices.

A **PERSONAL REPRESENTATIVE** is the person(s) under applicable state and federal law who has the authority to act on behalf of a Patient in making decisions related to health care as more fully set forth in Tenet Policies and Procedures.

PERSONALLY IDENTIFIABLE INFORMATION or PII means any information about an individual maintained by Tenet, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

PHI See Protected Health Information.

PHYSICAL SECURITY The protection of personnel, information assets, facilities, and utilities against intrusion, disclosure, theft, damage, destruction or misuse.

PIRT refers to the Privacy Incident Response Team.

PRIVACY MATTERS means the internal database that tracks audits, risk assessments and compliance-related issues.

PRIVACY SECURITY COMPLIANCE OFFICER The person designated by Tenet to be responsible for the development and implementation of the privacy policies and procedures of Tenet.

PRIVACY REGULATIONS Regulations governing the Use and Disclosure of PHI promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

PRODUCT SECURITY LIFE-CYCLE PROGRAM refers to the Corporate Information Security Department's program to manage the entire life cycle of a product introduced into the Tenet network.

PROPRIETARY INFORMATION OR SENSITIVE/PROPRIETARY INFORMATION means any trade secret, know-how, invention, software program, application, documentation, schematic, procedure, contract, information, knowledge, data, process, technique, design, drawing, program, formula or test data, work in progress, engineering, manufacturing, marketing, financial, sales, supplier, customer, patient, employee, investor, or business information, whether in oral, written, graphic or electronic form. This information is intended for use within Tenet unless authorized for additional distribution.

PROTECTED HEALTH INFORMATION or **PHI** means individually identifiable health information that is transmitted by electronic media; maintained in any medium as described in the definition of electronic media; or transmitted or maintained in any other form. PHI excludes individually identifiable health information in education records and student health records covered by the Family Educational Rights and Privacy Act (FERPA), and employment records held by a Covered Entity in its role as employer.

PROXY SERVER See APPLICATION FIREWALL. Proxies can be modified to allow or disallow specific services, (i.e. An FTP proxy can be configured to permit incoming FTP while block outgoing FTP).

PUBLIC INFORMATION means information that has been released to the public by Tenet.

PUBLIC KEY INFRASTRUCTURE or **PKI** A public-key cryptography method that is implemented through the use of security architectures, techniques, practices, and procedures.

PSYCHOTHERAPY NOTES Notes recorded (in any medium) by a Health Care Provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint or family counseling session, and are maintained separately from the rest of the patient's medical record. If a mental health professional's

counseling session notes are commingled with a patient's general medical record, then the notes no longer retain their status as Psychotherapy Notes for purposes of this policy. In any case, Psychotherapy Notes are not medication prescriptions, information about the monitoring of medications, counseling session start and stop times, the modalities and frequencies of Treatment furnished to the patient, the results of clinical tests, or any summary of the following items: diagnosis, functional status, treatment plan, symptoms, prognosis and progress to date. (These items of information are excluded from the definition because it is expected that they are maintained in the patient's medical records.)

R.

RECORD CUSTODIAN An individual designated by the facility to be responsible for the safekeeping, maintenance, and release of PHI.

RE-IDENTIFIED INFORMATION De-identified Information which is subsequently re-identified using a code, key, or other record identifier.

REMOTE ACCESS Access to Tenet information resources from outside the established LAN/WAN environment.

RESEARCH is any systematic investigation, including research development, testing, and evaluation designed to develop or contribute to generalizable knowledge.

S.

SECURE TEXTING Any messaging occurring inside a Tenet approved encryption application.

SECURITY VIOLATION means a failure in the physical security and/or Information Security measures resulting in a loss of data, the inability to provide computing services, unauthorized use or modification of information assets, or the unauthorized access to files, data, and services.

SENSITIVE INFORMATION includes but is not limited to any of the following information: social security numbers, any government-issued identification number (e.g. driver's license, passport), individually identifiable patient data, ePHI, Cardholder Data, account number, credit or debit card number, security code, access code, password, PIN, human resources employee files, or any information that is deemed protected or confidential by contractual obligations or any federal, state or local law or regulation.

SOCIAL ENGINEERING The process used by persons intent on gaining illegal access to Tenet's computing assets (disgruntled associates, intruders, industrial spies, etc.) to gather information by impersonation, fraud, lying, intimidation and social interaction.

SOFTWARE The computer program that instructs computer hardware to perform an action. System software is the operating system that controls the basic functioning capabilities of the

computer, network software enables multiple computers to communicate with one another, and language software is used to develop programs.

The **SYSTEMS DEVELOPMENT LIFE CYCLE** or **SDLC**, also referred to as the **APPLICATION DEVELOPMENT LIFE-CYCLE**, is a term used in systems engineering, information systems and software engineering to describe a process for planning, creating, testing, and deploying an information system.

T.

TCP Transmission Control Protocol

TABLE-TOP EXERCISES means discussion-based sessions where the CIRT members meet to discuss their roles and responses during various simulated incidents as specified by the CISO. The CISO or a facilitator designated by the CISO guides CIRT members through these exercises.

TENET ENTERPRISE OPERATIONS means Tenet Healthcare Corporation, and all hospitals and other healthcare operations owned or operated by Tenet or its consolidated subsidiaries.

TERMINAL A terminal is the end point in a computing environment where an individual interfaces with a computer, network or other information asset. The following are examples of a terminal:

- a. A personal computer in stand-alone mode.
- b. A personal computer when connected to a network.
- c. A “dumb” terminal (normally just a CRT and a keyboard).
- d. A bio-medical device, which takes input from an individual.
- e. A handheld computing device (Palm Pilot, barcode scanner).

TEXT MESSAGING or **TEXTING** is the act of composing and sending brief, electronic messages between two or more mobile phones, or fixed or portable devices over a cellular or Wi-Fi network. It also includes sending messages from mobile carrier websites and web-based paging applications. MMS Messages are messages that contain images, video and sound content. These forms of messaging are not allowed under Tenet policy.

THREAT Any circumstance or event with the potential to cause harm to an information asset.

TRADEMARK OR SERVICE MARK *“A Trademark is any symbol, such as a word, number, picture, or design, used by manufacturers or merchants to identify their own goods and distinguish them from goods made or sold by others. Thus, a trademark identifies the source of a product and fixes responsibility for its quality. If customers like the goods, the trademark enables them to know what to purchase in the future; if they dislike the product, they will avoid goods with that trademark.”*

“The name of a type of product cannot be a trademark, because every maker of that product is free to use its name. Sony, for example, is a well-known trademark for televisions, radios, and

audio equipment, but no one can have trademark rights to the word television or radio. On several occasions, however, words intended by manufacturers to be used as trademarks for new products were instead used by customers to name the products; such words then lost their legal status as trademarks. Examples include aspirin, cellophane, and escalator.”

From Microsoft's Encarta 96 Encyclopedia

For most intents and purposes, a **SERVICE MARK** is the same as a **TRADEMARK**.

TRANSMISSION OF INFORMATION is the transfer of data between applications, systems, companies, or personnel.

TREATMENT The provision, coordination, or management of health care and related services by a Health Care Provider(s), including the coordination or management of health care by a Health Care Provider with a third party; consultation between Health Care Providers related to a patient; or the referral of a patient for health care from one Health Care Provider to another.

TRUSTED NETWORK means the networks within Tenet's LAN/WAN environment perimeter defense which comply with Tenet's Information Security policies and standards.

U.

UNIX, LINUX or X-NIX refers to a family of multitasking, multiuser computer operating systems that derive their base from the original 1970's AT&T UNIX operating system.

UNSECURED PROTECTED HEALTH INFORMATION or UNSECURED PHI means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111-5. Redaction is not an approved method of destruction.

UNSECURED TEXTING Any messaging occurring outside of a Tenet approved encryption application.

UNTRUSTED NETWORK means networks, outside of Tenet's LAN/WAN environment and perimeter defenses to include internal wireless networks that process payment card data, which are not subject to Tenet's Information Security policies and standards.

UPS Un-interruptible power supply. A device that isolates the power provided to an asset from the commercial supply. This is done by taking in the commercial supply, converting it to DC, charging a set of batteries, converting the battery output to AC, and providing that to the asset.

USE means the sharing, utilization, examination, or analysis of PHI within an entity that maintains PHI.

USERS mean individuals that input/output data to/from Tenet information assets. These individuals are collectively referred to as Users, and may include, but are not limited to, employees, students, physicians, contractors, agents, consultants, clients, vendors, business partners and electronic (web site) visitors.

USER ID A unique identification code used by an information asset to identify an individual gaining access to that asset. When the User ID is matched with the appropriate password, access is granted and the process uses the User ID to set access privileges for resource allocation, batch or interactive processes, file or record ownership.

V.

VIRUS A computer virus is an unauthorized program that replicates and spreads through computing assets onto various data storage media (floppy disks, magnetic tapes, hard drives, etc.) and/or across a network, or resides in memory.

A **VISITOR** means an individual that is not an employee, and may include, but are not limited to contractors, agents, consultants, clients, vendors, patients, their guests and visitors.

A **VIRTUAL PRIVATE NETWORK**, or **VPN** is a secured external network that uses encryption to secure a link between two sites across a public network. All traffic across the network is encrypted by the VPN, not by the individual users. This allows the sites to verify the data is from the specified source, that the data has not been modified, and ensures that a person who intercepts a data block between the two sites cannot read the data. A VPN is not restricted to a public network, but can be used with leased lines as well.

VULNERABILITY A bug or feature in an information asset that enables an attacker to circumvent security measures.

W.

WEB SITE or WEBSITE A source of health content, commerce, connectivity, and/or care delivery that users access via the Internet or other electronic means.

WHISTLEBLOWER An individual who believes in good faith that the facility has acted unlawfully or violated professional or clinical standards, or that its care or services potentially endanger a patient, employee, or the public, and in that connection discloses PHI to a health oversight agency, accrediting agency, appropriate public health authority, or to an attorney retained by the individual.

WINDOWS SERVER refers to a group of operating systems designed by Microsoft that supports enterprise-level management, data storage, applications, and communications.

WORKFORCE includes employees, volunteers, trainees and other persons, whose conduct, in the performance of work for the facility, is under the direct control of such facility, whether or not they are paid by the facility. Workforce excludes independent contractors of the facility because the facility may not exercise direct control over an independent contractor. Workforce also excludes Business Associates or an employee, agent or contractor of a Business Associate.

WORKSTATION See Terminal.

Z.

ZEROIZATION The act of electronically writing a series of zeroes (0s) over a magnetic media to ensure that the data formerly stored on that media is no longer readable or recoverable.