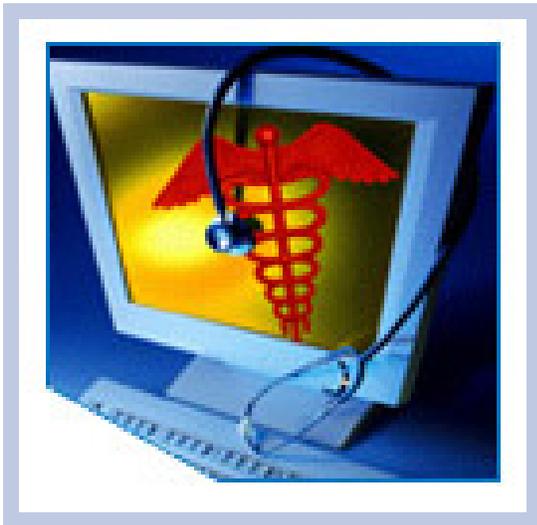


HITSP Glossary



Submitted to:

Healthcare Information Technology Standards Panel



DOCUMENT CHANGE HISTORY

Version Number	Description of Change	Name of Author	Date Published
1.0	Reference	HITSP Project Team	December 5, 2007
1.1	Reference	HITSP Project Team	March 19, 2008
1.2	Reference	HITSP Project Team	September 26, 2008

REFERENCE



HITSP GLOSSARY

Term	Definition
Acceptable Risk	Level of risk that management finds acceptable to a particular information asset. It is based on empirical data, and supportive of technical opinion and understanding of the overall risk. The controls placed on the asset or environment will lower the potential for its loss. Any remaining risk is recognized and accepted as an accountability issue.
Acceptable Use Policy (AUP)	Set of rules and guidelines that specify the expectations for the appropriate use of systems or networks.
Access	Ability and the means necessary to read from, write to, modify, or communicate data/information, or to make use of any system resource.
Access Control	Prevention of unauthorized use of information assets (ISO 7498-2). It is the policy rules and deployment mechanisms, which control access to information systems, and physical access to premises (OASIS XACML).
Access Control Decision Function (ADF)	Specialized function that makes access control decisions by applying access control policy rules to an access request, ADI (of initiators, targets, access requests, or that retained from prior decisions), and the context in which the access request is made (ISO 10181-3). See PDP.
Access Control Enforcement Function (AEF)	Specialized function that is part of the access path between an initiator and a target on each access control request, and enforces the decision made by the ADF (ISO 10181-3).
Access Control Information (ACI)	Information used for access control purposes, including contextual information (ISO 10181-3).
Access Control Service (ACS)	Access control service that includes embedded security management capabilities, and all other user-side access control and decision making capabilities (PEP, PDP, PIP, PAP, Obligation service, etc.) needed to enforce use-side, and system-object security and privacy policy. The ACS is responsible for creating trustworthy credentials forwarded in cross-domain assertions regarding security information and attributes. Access control services may be hierarchical and nested, distributed, or local.
Accounting of Disclosures	Refers to the right of individuals, with limitations, to a listing of the uses and disclosures of their individually identifiable health information for a period of time; not to exceed six years prior to the date of the request.
Action	Any interaction by an actor with the public health system, including Electronic Health Record system.
Action Level	That level of worker exposure determined by workplace sampling, at or above which medical monitoring will be performed. The concentration designated in 29 CFR, Part 1910 for a specific substance, calculated as an 8-hour time-weighted average, which initiates certain activities, such as exposure monitoring and medical surveillance; usually one-half the Permissible Exposure Limit (PEL). For substances with an OSHA PEL, the action level is defined and may be one-half of the PEL. For exposures not regulated by OSHA, other consensus standards may be used for an action level. One such consensus standard is the use of one-half of the Threshold Limit Value (TLV) as an action level.
Actor	Entities that interact with the system, e.g., users (provider, public health officer, patient, etc.)
Administrative Safeguards	Actions, including policies and procedures, that manage the selection, development, implementation, and maintenance of security and privacy measures to protect individually identifiable health information, and to manage the conduct of the workforce in relation to the protection of that information.



Term	Definition
American Health Information Community (AHIC)	The United States Department of Health and Human Services (HHS) Secretary, Mike Leavitt, announced the membership for the American Health Information Community (the Community) on September 13, 2005. The Community is a federally-chartered commission, and will provide input and recommendations to HHS on how to make health records digital and interoperable, and assure that the privacy and security of those records are protected, in a smooth, market-led way.
Anonymized	Personal data which has been processed to make it impossible to know whose data it is. Used particularly for secondary use of health data. In some cases, it may be possible for authorized individuals to restore the identity of the individual, e.g. for public health case management.
Association	In data modeling, an association is a structural relationship that specifies that instance of one thing connected to another instance.
Attribute	In data modeling, an attribute refers to specific items of data that can be collected for a class.
Audit	Review and examination of records (including logs), and/or activities to ensure compliance with established policies and operational procedures. This review can be manual or automated.
Auditing	Specific activities that make up an audit (see Audit). This can be manual, automated, or a combination.
Audit Record	Generates alerts for action, as evidence of output of an audit.
Authentication	Act of verifying the identity of an individual, originator, terminal, or workstation, to determine that entity's right to access specific categories of information, and a measure designed to protect against fraudulent transmission by verifying the validity of a transmission, message, station, or originator.
Authenticity	Ability to verify the confidence in the validity of a transmission, a message, or message originator.
Authorization	Method and form to secure permission from an individual for the use, or disclosure of individually identifiable health information, for any activity not specifically allowed without one. Uses and disclosures related to treatment, payment, and healthcare operations generally do not require a HIPAA authorization; but some non-healthcare related activities such as marketing do. Authorization is a new term used in the HIPAA Privacy Rule to denote an activity that has often been called a consent or a release.
Authorization Decision	Function that is returned by the PDP to the PEP. The function evaluates to "Permit", "Deny", "Indeterminate" or "Not Applicable", and optionally also returns a set of obligations (OASIS XACML).
Authorized Access	Mechanism by which access to data is granted by challenges to the requesting entity. It assures proper authority based on the identity of the individual, level of access to the data, and rights to manipulation of that data.
Availability	Systems responsible for delivering, storing and processing information are accessible when needed, and that the information provided will be of acceptable integrity.
BioSense	National program designed to improve the nation's capabilities for conducting near real-time biosurveillance, enabling health situational awareness through access to existing data from healthcare organizations across the country. http://www.cdc.gov/biosense
Biosurveillance	Surveillance programs in areas such as human health, hospital preparedness, state and local preparedness, vaccine research and procurement, animal health, food and agriculture safety and environmental monitoring that integrate those efforts into one comprehensive system. See also Surveillance.



Term	Definition
Biosurveillance System	<p>Biosurveillance systems must leverage two major surveillance methods:</p> <p>1) Well established public health surveillance methods and sources used for the tracking, monitoring, and reporting of health-related information, such as epidemiologic investigations of infectious disease outbreaks or environmental conditions, are needed to ensure a broad coverage of data sources, to use as baselines comparisons, and to support the accuracy and reliability of the biosurveillance findings.</p> <p>2) Early event detection and situational awareness, through the use of an automated system to evaluate case and suspect case reporting, along with statistical surveillance and data visualization of pre-diagnostic and diagnostic data, to support the earliest possible detection of events that may signal a public health emergency. It is an essential component for near real-time detection of natural or man-made health events.</p>
Business Associate	<p>A person who, on behalf of a covered entity, or an organized healthcare arrangement in which the covered entity participates, performs, or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information. Functions and activities include claims processing or administration, data analysis, processing and administration, utilization review, quality assurance, billing, benefit management, practice management, and reprising. Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a covered entity, where the provision of the service involves the disclosure of individually identifiable health information.</p>
Business Associate Agreement	<p>Agreement between a covered entity and its business associate in which the business associate agrees to restrict its use and disclosure of the covered entities protected health information.</p>
Care setting	<p>The physical location or entity providing healthcare.</p>
Certification	<p>The process used to establish whether systems can meet the high-level functionalities and detailed messages/metrics required to support public health activities.</p>
CHI Standards	<p>CHI (Consolidated Health Informatics) standards were selected for use in U.S. federal government systems for the electronic exchange of clinical health information. The initiative was absorbed into Federal Data Architecture initiative, but the list of selected standards remains a benchmark.</p>
Class	<p>In data modeling, a class is a description of a set of objects that share the same attributes, relationships and semantics.</p>
Classifications and Terminologies	<p>Classifications and terminologies are used with code sets to define and classify individual health terms. They serve as a way to relate terms to one another so that they are easily and consistently understood by users. Classifications arrange related terms for easy retrieval, while vocabularies are sets of specialized terms that facilitate precise communication by eliminating ambiguity. Important classifications include: ICD-9-CM, ICD-10, ICD-10-CM/PCS, and ICF. Important terminologies include LOINC and SNOMED. There are subtle differences between vocabularies, nomenclatures, terminologies and classifications. These have been addressed by the American Health Information Management Association (AHIMA).</p>
Clinical Encounter	<p>An encounter between a patient and a healthcare practitioner or healthcare provider (e.g. hospital or clinic) for clinical care. May also be used to refer to an encounter between a patient and a physician or other practitioner, as distinguished from ancillary services, such as lab tests or vaccinations.</p>



Term	Definition
Clinical Episode	A clinical episode is an extended period of care, often involving one or more encounters with a practitioner, and one or more ancillary tests or treatments. Sometimes, but not always, clinical episodes are defined as a period of care for a specific disease. Clinical episodes may include outpatient encounters as well as inpatient hospitalizations.
Collect /Collection	Assembly of personal information through interviews, forms, reports, or other information sources.
Compliance	Adherence to those policies, procedures, guidelines, laws, regulations and contractual arrangements, to which the business process is subject.
Concept	A concept is an atomic unit of a vocabulary. Each concept within a vocabulary has at least one unique identifier (known as the concept code, or simply code) that identifies the concept within the context of a specific vocabulary.
Confidentiality	Obligation of an entity that receives identifiable information about an individual as part of providing a service to that individual, to protect that data or information, including not disclosing the identifiable information to unauthorized persons or through unauthorized processes; including an obligation of those who receive information to respect the privacy interests of those to whom the data relate.
Connecting Laboratory Systems	Have the following three main definitions: 1. Standard HL7 message formats and terminology standards for specimen receipt and laboratory result reporting 2. Receipt and management of specimen and sample data 3. Monitoring of testing activity to project load distribution during a large-scale event
Consent	Under the HIPAA Privacy Rule, consent is made by an individual for the covered entity to use or disclose individually identifiable health information for treatment, payment, and healthcare operations purposes only. This is different from consent for treatment, which many providers use, and which should not be confused with the consent for use or disclosure of individually identifiable health information. Consent for use and/or disclosure of individually identifiable health information is optional under the Privacy Rule, although it may be required by state law, and may be combined with consent for treatment, unless prohibited by other law.
Consent Directive	The record of a healthcare consumer's privacy policy that grants or withholds consent for: <ul style="list-style-type: none"> • one or more principals (identified entity or role) • performing one or more operations (e.g., collect, access, use, disclose, amend, or delete) • purposes such as Treatment, Payment, Operations, Research, Public Health, Quality Measures, Health Status Evaluation by third parties, or Marketing • certain conditions, e.g., when unconscious • a specified time period, e.g., effective and expiry dates • a certain context, e.g., in an emergency



Term	Definition
Consent, Informed	Requirement that all researchers explain the purposes, risks, benefits, confidentiality protections, and other relevant aspects of a research study, to potential human subjects so that they may make an informed decision regarding their participation in the research. Institutional Review Boards (IRB) review informed consent processes and forms documenting the consent to ensure compliance with research regulations and policies.
Consenter	An author of a Consent Directive who may be the healthcare consumer or patient, a delegate of the healthcare consumer, e.g., a representative with healthcare power of attorney, or a provider with legal authority to either override a healthcare consumer's Consent Directive or create a Directive that prevents a patient's access to individually identifiable health information (IIHI) until the provider has had an opportunity to review the IIHI with the patient.
Consistent Time	Ensures that all the entity systems that are communicating within the network have synchronized system clocks.
Covered Entity	A health plan, a healthcare clearinghouse, or a healthcare provider that transmits electronic transactions.
Data Aggregation	Combining individually identifiable health information (IIHI) by a business associate, on behalf of more than one covered entity, to permit data analysis related to the healthcare operations of the participating covered entities.
Data Classification	Conscious decision to assign a level of sensitivity to data as they are being created, amended, enhanced, stored, or transmitted. The classification of the data, whether established by federal or state law or by the entity holding the data, will determine the extent the data needs to be protected, controlled and/or secured, and is indicative of its value in terms of information assets.
Data Flow	The sequence in which data is collected, transferred, managed, stored and used by actors.
Data Model	A framework for the development of a new or enhanced application. The purpose of data modeling is to develop an accurate model or graphical representation, of the client's information needs and business process.
Data Use Agreement	Confidentiality agreement between a covered entity and the recipient of health information in a limited data set.
Datatype	A specification of the allowed format for the values of an attribute. Examples include string, number, code, and text.
De-identified Health Information	Removal of individual identifiers, so that it cannot be used to identify an individual. De-identified health information is not protected by HIPAA.
Decrypting	Process of reversing the encryption of a file or message to recover the original data in order to use or read it.
Designated Record Set	Healthcare provider's medical records and billing records about individuals, a health plan's enrollment, payment, claims adjudication, case or medical management records, and any other records used by a covered entity to make decisions about individuals.
Diagnosis	The condition for which the patient is seeking care. Types of diagnoses range from early and indefinite to final and definitive. Some examples (in general order of definiteness) include presenting (or chief complaint), presumptive, working, admitting, discharge, dismissal, or final. Applying classification codes to the diagnosis becomes more straightforward as the diagnosis is more established. Early diagnoses may be vague or even expressed in natural language rather than coded.



Term	Definition
Digital Signature	Mathematical computer program creates a digital signature. It is neither a hand-written signature nor a computer-produced picture of one. The signature is like a wax seal that requires a special stamp to produce it, and is attached to an email message or file. The digital signature may then verify the origin of the message or file.
Disaster	A large emergency event that is beyond the community's ability to address within its own and mutual aid resources.
Disclosure	Release, transfer, provision of access to, or divulging in any other manner of information outside the covered entity holding the information.
Document Integrity	To ensure the integrity of a document that is exchanged or shared.
Early event detection	Defined as: <ol style="list-style-type: none"> 1. Secondary use of clinical care and other health-related data for early identification of public health events 2. Reportable disease case reporting from clinical care via the Web and 24/7 call reporting systems with triage of disease urgency 3. Situational awareness of the size, location, and spread of a health event using secondary use data and case reporting 4. Disease data exchange using HL7-specific implementation guides 5. Detection algorithms to determine and visualize deviation from normal disease patterns
Electronic Data Interchange (EDI)	A standard format for exchanging business data. An EDI message contains a string of data elements, each of which represents a singular fact, such as a price, product model number, and so forth, separated by delimiters (a character that identifies the beginning and end of a character string). The entire string is called a data segment. EDI is one form of e-commerce, which also includes e-mail and fax.
Electronic Health Record (EHR)	The EHR is information, assembled and maintained in an electronic format, which pertains to the health status of an individual, and the health services delivered to an individual.
Electronic Health Record Infrastructure	Databases, programs, software, hardware, servers, firewalls, access rules, Virtual Private Network (VPN) linkages, and web browser capabilities of the Electronic Health Record system.
Electronic Health Record Standards	Standardization in the field of information for health, and Health Information and Communications Technology, to achieve compatibility and interoperability between independent systems. Also, to ensure compatibility of data for comparative statistical purposes (e.g., classifications), and to reduce duplication of effort and redundancies.
Electronic Health Record System (EHRS)	System that includes: <ol style="list-style-type: none"> 1. Longitudinal collection of electronic health information for and about persons, where health information is defined as information pertaining to the health of an individual, or health care provided to an individual 2. Authorized users 3. Provision of knowledge and decision-support that enhance the quality, safety, and efficiency of patient care 4. Support of efficient processes for health care delivery <p>Critical building blocks of an EHR system are the Electronic Health Records (EHR) maintained by providers (e.g., hospitals, nursing homes, ambulatory settings), and by individuals (also called Personal Health Records).</p>
Electronic Protected Health Information (EPHI)	Within the context of HIPAA, any protected health information (PHI) which is created, stored, transmitted, or received electronically.



Term	Definition
Emergency	Sudden demand for action; a condition that poses an immediate threat to the health of the patient. This definition is further clarified to mean any potential denial of critical health services or information, that could reasonably result in personal injury or death to an individual or the public. http://www.astm.org
Emergency Access	Granting of user rights and authorizations to permit access to individually identifiable health information (IIHI) and applications in emergency conditions outside of normal workflows (Emergency Room access is considered to be a normal workflow).
Emergency Permission	Permission granted to certain caregivers in advance that allows self-declaration of an emergency and assumption of an emergency role. Emergency permissions defined in standard ways compliant with ANSI INCITS RBAC standards and HL7 Healthcare Permission definitions are suitable for Federated circumstances, where the person declaring the emergency is not a member of the organization possessing the requested information.
Employee Retirement Income and Security Act (ERISA) of 1975	Most group health plans covered by ERISA are also health plans under HIPAA.
Employee Welfare Benefit Plan	A plan, fund or a program maintained by an employer or an employee organization that provides medical, surgical or hospital care.
Encoded	Information, such as diseases, procedures, and/or demographic data may be coded into discrete categories, identified by codes which may be numeric, alphabetic or a combination of these. In computer-based systems, this eases retrieval and simplifies analysis. In healthcare, 'encoded' may refer to clinical conditions or interventions coded into specific coding systems for administrative, financial, and other analyses. Among the most common coding systems are the International Classifications of Diseases (see ICD) and Current Procedural Terminology (see CPT). Another approach to coding is atomic coding, which involves assigning a value to each position in the code. (A simple example would be "35yoF " meaning "35 year old female.") Such coding systems, of which SNOMED is the most well known, are more flexible than hierarchical classifications, but may be more difficult to use.
Encryption	Process by which data are temporarily re-arranged into an unreadable or unintelligible form for confidentiality, transmission, or other security purposes.
Entity	A person or computer-based equivalent.
Entity Identity Assertion	Ensure that an entity is the person or application that claims the identity provided.
Enzyme	A substance that speeds up a chemical reaction. Every chemical reaction in living organisms is facilitated by an enzyme.
Event	Action or activity that occurs within a system and/or network scope, inclusive of its boundaries.
Event Aggregation	Consolidation of similar log entries into a single entry containing a count of the number of occurrences of the event.
Event Correlation	Relationships between two or more log entries.
Event Filtering	Suppression of log entries from analysis, reporting, or long-term storage, because their characteristics indicate that they are unlikely to contain information of interest.
Event Reduction	Removal of unneeded data fields from all log entries to create a new log that is smaller.



Term	Definition
eXtensible Markup Language (XML)	A specification developed by the World Wide Web Consortium. XML is designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. XML provides a file format for representing data, a schema for describing data structure, and a mechanism for extending and annotating HTML with semantic information.
Facility Directory	Listing or reference document containing information about each individual patient or resident receiving care or treatment. It is maintained by a healthcare provider, such as (but not limited to) a hospital, nursing home, or treatment center, of persons receiving care or treatment from that provider.
Filtering	In data processing, it is the selection of a subset of records based on specified criteria present in the data.
PHIN Functional Requirements	PHIN functional requirements describe functionality that is necessary to support activities in a particular area (e.g. laboratory systems must transmit result messages to public health systems). See PHIN.
Gap Analysis	Evaluation of results of a security inventory against requirements.
Harmonization	Harmonization is the name given to the effort by industry to replace the variety of product standards and other regulatory policies adopted by nations, in favor of uniform global standards. Usually used to in the context of trade agreements, harmonization has recently been adopted by the United States government to refer to information technology standards.
Health alerts	Urgent messages from the Centers of Disease Control (CDC) to health officials requiring immediate action or attention.
Healthcare	Broad term that directly refers to different activities and means used to prevent or cure different processes of morbidity.
Healthcare Provider	Refers to a person licensed, certified, or otherwise authorized or permitted by law to administer healthcare in the ordinary course of business or practice of a profession, including a healthcare facility. This includes primary care providers, other physicians, nurse-practitioners, physician assistants, etc. Note: HL7 uses "practitioner". The term "provider" may also refer to healthcare facilities, clinics, hospitals, etc.
Health Information	Information, whether oral or recorded in any form or medium, that: <ol style="list-style-type: none"> 1. is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse 2. relates to the past, present, or future physical or mental health, or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual.
Health Information Exchange (HIE)	The mobilization of healthcare information electronically across organizations within a region or community. HIE provides the capability to electronically move clinical information between disparate healthcare information systems, while maintaining the meaning of the information being exchanged. The goal of HIE is to facilitate access to, and retrieval of, clinical data to provide safer, more timely, efficient, effective, equitable, and patient-centered care.
Health Information Exchange Architecture	Overall structural approach, from an information technology perspective, utilized in the establishment and deployment of HIEs.
Health Information Privacy	An individual's right to control the acquisition, uses, or disclosures of his or her identifiable health information.
Health Information Security	Physical, technological, or administrative safeguards or tools used to protect identifiable health information from unwarranted access or disclosure.



Term	Definition
Health Insurance Portability and Accountability Act (HIPAA)	Seeks to establish standardized mechanisms for electronic data interchange, security, and confidentiality of all healthcare-related data. The Act mandates standardized formats for all patient health, administrative, and financial data; unique identifiers (ID numbers) for each healthcare entity, including individuals, employers, health plans and healthcare providers; and security mechanisms to ensure confidentiality and data integrity for any information that identifies an individual.
Health Plan	This term encompasses a review entity, utilization management organization, payer, third party administrator, processor, health plan, or any entity the authorization approval process on behalf of the health plan. While each of these entities may perform other functions in the healthcare arena, the function is grouped together in this guide, under one term "Health Plan"
Health updates	CDC health updates; these do not require immediate action.
Healthcare	Services or supplies related to the health of an individual.
Healthcare Clearinghouse	Organization that processes health information received from another entity in a nonstandard format, or containing nonstandard data content into standard data elements, or a standard transaction, or vice versa.
Healthcare Operations	Operations, including quality assessment and improvement, peer review, underwriting, medical review audits, and business planning, management and development.
Healthcare Provider	Person or organization that furnishes, bills, or is paid for healthcare in the normal course of business.
Identity Access Management (IAM)	Set of services to include authentication, user provisioning (UP), password management, role matrix management, enterprise single sign-on, enterprise access management, federation, virtual and meta-directory services, and auditing (Gartner 2006).
Identity Digital Management (IdM)	Comprised of the set of business processes, and a supporting infrastructure, for the creation, maintenance, and use of digital identities, within a legal and policy context (BurtonGroup™ 2003).
In-band	Communications which occur together in a common communications method or channel. For example, a privacy label that applies to a clinical document will be sent <i>in-band</i> with the document.
Individual	Person who is the subject of information collected, used, or disclosed by the entity holding the information.
Individually Identifiable Health Information (IIHI)	Information that relates to an individual's physical or mental health; the provision of healthcare to an individual; or the payment for healthcare provided to an individual, in which the information identifies the individual or could be used to identify the individual. This is a more encompassing term that includes Protected Health Information and Personal Health Information.
Individually Identifying Information	Single item or compilation of information or data that indicates or reveals the identity of an individual, either specifically (such as the individual's name or social security number), or that does not specifically identify the individual but from which the individual's identity can reasonably be ascertained.
Influenza	A serious disease caused by viruses that infect the respiratory tract.
Information Asset	Refers to any information in any form (e.g. written, verbal, oral or electronic) upon which the organization places a measurable value. This includes information created by the entity holding the information, gathered for the entity, or stored by the entity for external parties.
Information Owner/User	Individual or individuals that make use of computer systems and networks.
Information Security	Programs that technically manage and protect the organization from unacceptable risks of an organization's information assets. Also, a mechanism and practice to protect confidential and sensitive information.



Term	Definition
Information System	Interconnected set of electronic information resources and/or applications under the same direct management control. A system normally includes hardware, software, information, data, applications, communications, and people. It is made up of databases, application programs, and manual and machine procedures. It also encompasses the computer systems that do the processing, as well as intermediary systems that route or perform some action as part of the processing.
Initiator	An (authenticated) entity (e.g. human user or computer-based entity) that attempts to access other entities (ISO 10181-3). Also known as Claimant or Principal.
Institutional Review Board (IRB)	Specially constituted review body established or designated by an entity, in accordance with 45 CFR Part 46, to protect the welfare of human subjects recruited to participate in biomedical or behavioral research.
Integrity	Data or information that has not been altered or destroyed in an unauthorized manner or data that has not been modified or deleted in an unauthorized and undetected manner.
Interoperability	Interoperability is the ability of health information systems to work together within and across organizational boundaries, in order to advance the effective delivery of health care for individuals and communities.
International Standards Organization (ISO)	A worldwide federation of national standards bodies from some 100 countries; one from each country. Among the standards it fosters is Open Systems Interconnections (OSI), a universal reference model for communication protocols. Many countries have national standards organizations, such as the U.S. American National Standards Institute (ANSI), that participate in and contribute to ISO standards development.
Law Enforcement Official	Officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to: <ul style="list-style-type: none"> • Investigate or conduct an official inquiry into a potential violation of law; or • Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law
Limited Data Set	Specifies health information from which identifiers have been removed. Information in a limited data set is protected, but may be used for research, healthcare operations, and public health activities, without the individual's authorization.
Log	Record that is created by an event(s).
Log Analysis	Studying log entries to identify events of interest or suppress log entries for insignificant events.
Log Archival	Retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
Log Clearing	Removal of all entries from a log that precedes a certain date and time.
Log Compression	Storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.
Log Conversion	Parsing a log in one format and storing its entries in a second format.
Log Entry	Individual record within a log.
Log In, Logging Into	Action performed by an end-user, when authenticating into a computer system.
Log Management	Process for generating, transmitting, storing, analyzing, and disposing of log data.
Logging	Activities involved in creating logs.



Term	Definition
Logical Observations, Identifiers, Names and Codes (LOINC)	LOINC laboratory terms set provides a standard set of universal names and codes for identifying individual laboratory and clinical results, and allows users to merge clinical results from many sources into one database for patient care, clinical research, or management.
Malicious Software	Viruses designed to damage or disrupt a system's software.
Manage Consent Directives	Ensure that individually identifiable health information (IIHI) is only accessed with a consumer's consent.
Marketing	Communications that encourage the purchase or use of a product or service. This does not include a covered entity's communications about its own products, services or benefits, communications for treatment, case management, care coordination or referral for care.
Minimum dataset (AHIC)	A subset of data elements (derived from a larger planned set) that may be used to simplify the design and implementation of an early version of a breakthrough project.
Minimum Data Set (MDS)	Part of the U.S. federally mandated process for clinical assessment of all residents in Medicare or Medicaid certified nursing homes.
Minimum Necessary	Minimum amount of individually identifiable health information (IIHI) necessary to accomplish permitted use or disclosure for payment or healthcare operations.
Mission Critical	Activities, processing, etc., which are deemed vital to the organization's business success and possibly its very existence.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other.
National Health Information Network Consortia (NHIN)	As described by Secretary Mike Leavitt, November 10, 2005, the Nationwide Health Information Network (NHIN) contracts will bring together technology developers with doctors and hospitals to create innovative state-of-the-art ideas for how health information can be securely shared. "This effort will help design an information network that will transform our health care system resulting in higher quality, lower costs, less hassle and better care for American consumers."
Node	Originating or terminating point of information or signal flow in a telecommunications network.
Nonrepudiation	Verification that the sender and the recipient were, in fact, the parties who claimed to send or receive the message, respectively. In other words, nonrepudiation of origin proves that data has been sent, and nonrepudiation of receipt proves it has been received.
Notifiable condition	Any disease or condition determined by law to be notifiable in the United States. Conditions may be notifiable at various levels of jurisdiction, including nationally, at the state level, in sub-state jurisdictions, in US territories, or in a combination of jurisdictions. Variation in reporting requirements exists within the various jurisdictions. Incidences of communicable disease, traumatic injury, cancer, or other health condition.
Notification, public health	Interaction with a caseworker, person, or party, to report or document a disease or situation related to the health of the public.
Obligation	Operations specified in a policy or policy set that should be performed by the PEP in conjunction with the enforcement of an authorization decision (OASIS XACML).
Obligation Handler	An obligation handler evaluates obligation attributes in the Obligation section of a XACML.
Opt-in	Mechanism that states data collection and/or use methods, and provides user choice to accept such collection and/or use.



Term	Definition
Opt-out	Mechanism that states data collection and/or use methods and provides user choice to decline such collection and/or use.
Organized Healthcare Arrangement	Organized system of healthcare in which more than one covered entity participates, and in which the participating covered entities hold themselves out to the public as participating in a joint arrangement; and participate in joint utilization review, quality assurance or financial risk for healthcare services.
Ontology	Data model that represents a set of concepts within a domain and the relationships between those concepts.
Out-of-band	Communications which occur outside of a communications method or channel. For example, the communication of security policies that will be applied to data in the future are communicated out-of-band; they are communicated prior to, not at the same time as, the data.
Pandemic	The worldwide outbreak of a disease in numbers clearly in excess of normal.
Pandemic influenza or "flu"	The worldwide outbreak of a particular strain of influenza.
Payment	Activities of a healthcare provider to obtain payment for healthcare services; or activities of a health plan to obtain premiums or to adjudicate and pay claims.
Personal Health Information	Individually identifiable health information (IIHI) that is transmitted or maintained by electronic media, or is transmitted or maintained in any other form or medium. See IIHI.
Personal Representative	Person who has the authority, under applicable state law, to act on behalf of an individual who is an adult or an emancipated minor, in making decisions related to the program, service, or activity that an entity provides to the individual. Under applicable state law, a parent, guardian, or other person acting in 'loco parentis', with authority to act on behalf of an individual who is an un-emancipated minor in making decisions related to the program, service or activity, should be treated as the personal representative of the individual.
Physical Safeguards	Measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards and unauthorized intrusion.
Plan Sponsor	An employee welfare benefit plan (typically an employer or union).
Policy Access Point (PAP)	Another term used for a policy repository.
Policy Determination Point (PDP)	Logical entity or place on a server that makes admission control and policy decisions in response to a request from a user wanting to access a resource on a computer or network server.
Policy Enforcement Point (PEP)	An application functions in the role of the Policy Enforcement Point (PEP) if it guards access to a set of resources, and asks the Policy Determination Point (PDP) for an authorization decision.
Policy Information Point (PIP)	Directories or any other identity providers. PIPs can provide attributes on the resource that is being accesses as well as the entity (identity) that tries to access that resource.
Policy Repository	A policy repository stores policies specific to the environment in which it resides. The policy repository may also be called a Policy Access Point (PAP), as an entity that wishes to access policy information would go through the policy repository to evaluate policies.
Point-to-Point	Communication line that provides a path from one location to another.



Term	Definition
Privacy	Individual's or organization's right to determine whether, when, and to whom, personal or organizational information is released. Also, the right of individuals to control or influence information that is related to them, in terms of who may collect or store it, and to whom that information may be disclosed.
Privacy Officer	Appointed by a covered entity to be responsible for developing and implementing policies and procedures for complying with the health information privacy requirements of HIPAA.
Privacy Rights	Specific actions that an individual can take, or request to be taken, with regard to the uses and disclosures of their information.
Process Model	A framework describing the activities, functions, and processes of an organization. Processes in a process model are often defined in terms of their inputs and outputs. Process models often accompany data models; a data model does not reflect any action or flow of information, and presents only a static view of data.
Protected Health Information (PHI)	Within the context of HIPAA, PHI is individually identifiable health information (IIHI), whether oral or recorded, in any form or medium, that is created or received by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse. It relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual. PHI includes any data transmitted or maintained in any other form or medium by covered entities, including paper records, fax documents, and all oral communications, or any other form (i.e., screen prints of eligibility information, printed emails that have identified individual's health information, claim or billing information, hard copy birth or death certificate). Protected health information (PHI) excludes school records that are subject to the Family Educational Rights and Privacy Act (FERPA), and employment records held by the entity in its role as an employer.
Psychotherapy Notes	Notes that are recorded in any medium by a healthcare 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, when such notes are separated from the rest of the individual's record.
Public Health Activities	<p>Privacy Rule permits covered entities to disclose protected health information, without authorization, to public health authorities who are legally authorized to collect information for the purpose of preventing or controlling disease, illness or injury. Public health activities may include any of the following essential services of public health:</p> <ul style="list-style-type: none"> • Surveillance • Investigations • Education • Community Mobilization • Workforce Training • Research • Personal care services delivered or funded by governmental agencies
Public Health Authority	Agency or authority of the United States, a state, a territory, a political subdivision of a state, territory, or an Indian tribe, or a person or entity acting under a grant of authority from, or contract with such public agency, including the employees or agents of such public agency, or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.



Term	Definition
Public Health Information Network (PHIN)	CDC's vision for advancing fully capable and interoperable information systems in the many organizations that participate in public health. PHIN is a national initiative to implement a multi-organizational business and technical architecture for public health information systems.
Registry	A centralized public health data file pertaining to a defined set of health records for a particular population, e.g., cancer registry, immunization registry, blood lead registry. It is a common management tool used in public health to assist a health care practice in providing appropriate care to a population of patients, and/or to evaluate the effectiveness of public health intervention.
Requirements Specification	A complete and precise description of the system from the user's point of view.
Research	Systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalized knowledge.
Response	Taking action when a disaster occurs to save lives, prevent injuries, and prevent or limit property damage.
Risk	Specific threat or event that will exploit or impact certain vulnerabilities.
Risk Assessment/Risk Analysis	Systematic evaluation of risk in an organization.
Risk Management	Overall program implemented in an organization to control risk.
Role-Based Access Control (RBAC)	Nondiscretionary method of regulating or controlling access to resources based on the roles of individual users within an enterprise.
Scenario	Instance of a use case.
Secondary Use of Health Data	Non-direct care use of personal health information (PHI), including, but not limited to analysis, research, quality and safety measurement, public health, payment, provider certification or accreditation, and marketing and other business (including strictly commercial) activities. Secondary use of health data can enhance health care experiences for individuals, expand knowledge about disease and appropriate treatments, strengthen understanding about the effectiveness and efficiency of our health care systems, support public health and security goals, and aid businesses in meeting the needs of their customers.
Secured Communication Channel	Ensures the authenticity, the integrity, and the confidentiality of transactions, and the mutual trust between communicating parties.
Security	Refers to the physical, technological, or administrative safeguards or tools used to protect identifiable health data from unwarranted access or disclosure.
Security Incident	Attempted or successful unauthorized access, use, disclosure, modification, or destruction of information, or the interference with system operations in an information system.
Security/Security Measures/Safeguards	Encompass all of the administrative, physical, and technical actions used or taken to protect health information from unwarranted access or disclosure, regardless of the medium or format.
Semantic interoperability	The ability to preserve the meaning of exchanged information.
Shared Account	Refers to an account in an information system shared by a group of users. If the account is misused, it is very difficult or impossible to know which of the users was responsible.



Term	Definition
Situational awareness	Awareness of everything that is happening around oneself, and the relative importance of everything observed; with a constantly evolving picture of the state of the environment. Situational awareness can be described broadly as a person's state of knowledge or mental model of the situation around him or her. Situational awareness is important for effective decision making and performance in any complex and dynamic environment. It was originally an aviation term used to describe awareness of tactical situations during aerial warfare. It has now been adopted throughout aviation, and increasingly in other dynamic, complex situations requiring human control. A general, widely applicable definition describes situational awareness as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" (Endsley, 1988).
Standard	The term Standard is used [by HITSP] to refer to Specifications, Implementation Guides, Code Sets, Terminologies, Integration Profiles; it is a well-defined approach that supports a business process and: <ol style="list-style-type: none"> 1. has been agreed upon by a group of experts 2. has been publicly vetted 3. provides rules, guidelines, or characteristics 4. helps to ensure that materials, products, processes, and services are fit for their intended purpose 5. is available in an accessible format 6. is subject to an ongoing review and revision process
Strain	A group of organisms within a species or variety.
Structured Data	Coded, semantically interoperable data that is based on a reference information model.
Subtype	A specialization of another class, which inherits the attributes of its parent class.
Surveillance	The systematic ongoing collection, collation, and analysis of data and the timely dissemination of information to those who need to know so that action can be taken. Surveillance is the essential feature of epidemiological practice.
Synchronous	Events that are synchronized, or coordinated, in time.
System	An organized set of communicating parts organized for a specific purpose.
Systematized Nomenclature of Medicine (SNOMED)	A structured nomenclature and classification of the terminology used in human and veterinary medicine developed by the College of Pathologists and American Veterinary Medical Association. Terms are applied to one of eleven independent systematized modules.
Technical Safeguards	Policies and procedures to protect electronic health information and control access.
Threats	Exploitation or compromise of the security of systems or networks.
Trading Partner Agreement	Related to the exchange of information in electronic transactions, specifically the communications protocols and transaction standards to be used.
Transaction, Electronic Transaction	Transmission of information in electronic form between two parties to carry out financial, administrative or clinical exchanges of health information.
Transmission	Transfer of data over a communications channel.
Transmission Confidentiality	Process to ensure that information in transit is not disclosed to unauthorized individuals, entities, or processes.
Transmission Integrity	Process to guard against improper information modification or destruction while in transit.



Term	Definition
Transparency	Transparency implies openness, communication, and accountability. It is a metaphorical extension of the meaning used in the physical sciences: a "transparent" object is one that can be seen through. Transparent procedures include open meetings, financial disclosure statements, the freedom of information legislation, budgetary review, audits, etc.; HITSP's contract promises transparency and openness.
Transport Layer Security (TLS)	Authentication and security protocol widely implemented in web browsers and web servers.
Trauma	Any injury, whether physically or emotionally inflicted. Physical trauma refers to a physical injury. In medicine, however, the words trauma patient usually refer to someone who has suffered serious and life-threatening physical injury, potentially resulting in secondary complications such as shock, respiratory failure, and death. Trauma patients require specialized care, including surgery and sometimes blood transfusion, within the so-called golden hour of emergency medicine; the first sixty minutes after trauma occurs. This is not a strict deadline, but recognizes that many deaths which could have been prevented by appropriate care, occur a relatively short time after injury. In many places, organized trauma referral systems have been set up to provide rapid care for injured people. Research has shown that deaths from physical trauma decline where there are organized trauma systems.
Trauma Center	Trauma centers are usually classified as Level I and Level II; based on the severity of cases they treat, although the criteria for classification have changed over time, and are subject to scrutiny by medical professional organizations and health jurisdictions.
Treatment	Provision, coordination, or management of healthcare and related services by one or more healthcare providers, including the coordination or management of healthcare by a healthcare provider with the third party; consulting between healthcare providers relating to a patient, or the referral of a patient for healthcare from one healthcare provider to another.
Unified Modeling Language (UML)	A graphical language for visualizing, specifying, constructing, and documenting the artifacts of a software-intensive system. A standard set of notations for representing the system in a graphical way.
Unified Modeling Language System (UMLS)	Developed by the National Library of Medicine as a standard health vocabulary that enables cross-referencing to other terminology and classification systems. Includes a meta-thesaurus, a semantic network, and an information sources map. Purpose is to help health professionals and researchers retrieve and integrate electronic biomedical information from a variety of sources, irrespective of the variations in the way similar concepts are expressed in different sources and classifications systems. Has incorporated most source vocabularies.
Use	Sharing, employment, application, utilization, examination, or analysis of information within the entity that maintains such information.
Use Case	In software engineering, a Use Case is a technique for capturing the potential requirements of a new system or software change. Each Use Case provides one or more scenarios that convey how the system should interact with the end user, or another system, to achieve a specific business goal. Use Cases typically avoid technical jargon, preferring instead the language of the end user or domain expert. Use Cases are often co-authored by business analysts and end-users.
Use Case Diagram	A product of the requirement elicitation process (UML notation) that depicts graphical (symbolic) description of the functionality of the system for the selected use case.



Term	Definition
User	Person or entity with authorized access.
Vocabulary	Also known as a terminology is a collection of concepts along with their relationships to each other.
Work Flow	A sequence of activities by actors within a selected use case that generate, manage, and use data within the system.

References

Definitions to the terms included in this glossary have been generally extracted from Standard Development Organizations and several of the following sources:

1. Centers for Disease Control and Prevention. <http://www.cdc.gov/ncipc/>
2. Health Level 7 (HL7). www.hl7.org
3. Integrating the Healthcare Enterprise. www.ihe.net
4. International Organization for Standardization (ISO). www.iso.org
5. National Committee on Vital and Health Statistics. <http://ncvhs.hhs.gov/hipaa000706.pdf>
6. National Security and Privacy policy organizations
7. Mayo Clinic College of Medicine. www.mayo.edu
8. SNOMED International. www.SNOMED.org
9. US Code of Federal Regulations
10. U.S. Department of Health and Human Services. <http://www.hhs.gov/healthit/ahic.html>
11. <http://www.astho.org/pubs/BiosurveillancePositionStatementFINAL030706.pdf>
12. <http://www.citizen.org/trade/harmonization/>
13. <http://www.eff.org/Privacy/Anonymity/>
14. http://en.wikipedia.org/wiki/Minimum_Data_Set
15. http://en.wikipedia.org/wiki/Physical_trauma
16. http://en.wikipedia.org/wiki/Situational_awareness
17. http://en.wikipedia.org/wiki/Transparency_%28humanities%29

