



*Glossary of
terms related to
health information
exchange*

Glossary of terms related to health information exchange

Note: The definitions of many of the terms in this new field are rapidly evolving.

ACCESS CONTROL. A security technology that selectively permits or prohibits certain types of data access based on the identity of the accessing entity and the data object being accessed.

ACCOUNTABILITY. The ability to trace the actions of an entity such as people, organizations, programs, computers, etc.

ADT. Admission, Discharge and Transfer system located in a Hospital. The Admitting Discharge and Transfer module is used to track a patient/person's bed use from admission to discharge. In identifying and registering clients, the system makes it possible for the institution to track client location and encounters, and to produce statistical reports. Pre-admission and admitting information can be collected prior to actual admittance. Service, transfer and discharge information is also collected and input as close to the source as possible.

ALERTS. Electronic notification of an event or immediate action required. In general terms, system alerts are parameters that a user (or another system) can specify to control a system or agent's behavior.

ANSI (AMERICAN NATIONAL STANDARDS INSTITUTE). A voluntary standards organization that serves as the coordinator for national standards in the United States and the U.S. member body to the International Organization for Standards. ANSI accredits standards committees and provides an open forum for interested parties to identify, plan and agree on standards; it does not itself develop standards. Standards are developed by Standards Development Organizations (SDOs).

APPLICATION ARCHITECTURE. Defines how applications are designed and how they cooperate, promotes common presentation standards to facilitate rapid training and implementation of new applications and functions. Good application architecture enables a high level of system integration, reuse of components and rapid deployment of applications in response to changing business requirements.

APPLICATION PROGRAMMING INTERFACE (API). 1: A set of standard software interrupts calls, functions, and data formats that can be used by an application program to access network services, devices, applications or operating systems. 2: A set of pre-made functions used to build programs. APIs ask the operating system or another application to perform specific tasks.

ARCHITECTURE. Architecture is a term applied to both the process and the outcome of specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception. (*Also see Business Architecture, Enterprise Architecture, Federated Architecture, IT/IS Architecture*).

ARCHIVE. To store records and associated journals for a given period of time for security, backup, or auditing purposes.

AUDIT TRAIL. A security component of a computer system that maintains a log of which users accessed what files at what times to help detect unauthorized uses.

AUTHENTICATION. A process used to confirm the identity of a person or to prove the integrity of specific information. *Message authentication* involves determining its source and verifying that it has not been modified or replaced in transit.

AUTHORIZATION. Permission associated with accessing functions or subsets of data. Generally, an administrator will define the users who are authorized to access application functions or data.

B2B. Business-to-business electronic commerce typically takes the form of automated processes between trading partners. This may be an exchange of goods or services, or information, as is the case with health information exchanges.

BIOINFORMATICS. Research, development, or application of computational tools and approaches for expanding the use of biological, medical, behavioral or health data, including those to acquire, store, organize, archive, analyze, or visualize such data.

BIOMETRICS. Electronic capture and analysis of biological characteristics, such as fingerprints, facial structure, or patterns in the eye. Through advancements in smart cards and cheaper reader prices, biometrics is catching on as a security alternative to passwords.

BROKER. Application system that acts as an intermediary between two collaborating systems or services.

BROKER SERVICES. This service reads the business message that has been transformed to the canonical form and instantiates the appropriate workflow that will be used to process the business request.

BUSINESS ANALYST. The business analyst (BA) is skilled at working with end-users to determine their needs. Often, the business analyst has some technical experience that is useful in determining if a user's requests are feasible. The BA is responsible for drilling down in to each business requirement to ensure that what is being asked is actually what is needed. It is also the business analyst's role to translate what the user is asking for into a technical form that the programmer or system developer can understand.

BUSINESS ARCHITECTURE. 1: Defines the organization and functions of the business and the business processes that support those functions. 2: Pre-design plans for a technical architecture (see Architecture). It is the business "blueprint" of how a technical project will roll out and what it is trying to accomplish.

BUSINESS PARTNER. According to the definition in the Health Insurance Portability and Accountability Act (HIPAA), with respect to an entity covered under HIPAA regulations, business partner means a person to whom the covered entity discloses protected health information so that the person can carry out, assist with the performance of, or perform on behalf of, a function or activity for the covered entity. Business partner includes contractors or other persons who receive protected health information from the covered entity (or from another business partner of the covered entity) for the purposes described in the previous sentence, including lawyers, auditors, consultants, third-party administrators, health care clearinghouses, data processing firms, billing firms, and other covered entities. Business partner excludes persons who are within the covered entity's workforce.

BUSINESS PROCESS. A set of related work tasks designed to produce a specific desired business result (such as one or more products or services for customers of the business enterprise). The process result may be customer or market oriented or internal to the organization.

BUSINESS PROCESS ANALYSIS. The act of documenting and rethinking an entire business process for the purpose of restructuring the sequence and tasks required. The goal is to dramatically improve the means by which the organization achieves the desired results associated with the process.

(BUSINESS) 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.

BUSINESS RULE. A business rule is a statement that defines or constrains some aspect of the business. It is intended to assert business structure or to control or influence the behavior of the business. The statement is usually in “if _then” format that describes the appropriate next step to take given a variety of variables.

CCHIT (CERTIFICATION COMMISSION FOR HEALTH INFORMATION TECHNOLOGY). CCHIT was formed by three leading health care organizations to create an efficient, impartial and trusted mechanism for to certify ambulatory electronic health records and other health care information technology (IT) products.

CHANGE MANAGEMENT. A set of principles, techniques, and prescriptions applied to the human aspects of executing major change initiatives in organizational settings.

CHI (CONSOLIDATED HEALTH INFORMATICS). A collaborative effort to adopt health information interoperability standards, particularly health vocabulary and messaging standards, for implementation in federal government systems. About 20 department/agencies including the Department of Health and Human Services, the Department of Defense and the Department of Veterans Affairs are active in the CHI governance process. CHI originally identified a portfolio of 24 health domains that later expanded to 27. CHI adopted 20 uniform standards for electronic exchange of clinical information to be used across the federal health enterprise.

CLIENT/SERVER. The term client/server describes one possible relationship between two software applications in which the “client” application makes a service request from the “server” application. The client/server relationship can apply to two programs running on a single computer or two programs running over a network. In the case of a network, the client/server model provides a convenient way to interconnect programs that are distributed efficiently across different locations. For example, to check your e-mail from your computer, a client program on your computer forwards your request to a server program at your Internet Service Provider (ISP). Once the server program has retrieved your e-mail, it forwards them to the client on your computer, which then allows you to read the e-mail. The client/server model has become one of the central ideas of network computing. Most business applications being written today use the client/server model. A distinction used to be made between client/server applications and Internet-based applications. However, that distinction is being blurred such that even Internet-based applications are beginning to make use of the client/server model.

CLINICAL DATA. Any information element obtained during an encounter relating to the assessment of a patient/person's health state, diagnostic of ailments/diseases and/or treatments.

CLINICAL DATA REPOSITORY. An operational data store that holds and manages clinical data collected from service encounters at the point of service locations (e.g. hospitals, clinics, etc.). Data from a CDR can be fed to the EHR for that patient/person, in that sense the CDR is recognized as a source system for the EHR.

CLINICAL INFORMATION SYSTEM (CIS). A clinical information system is a system dedicated to collecting, storing, manipulating and making available clinical information important to the delivery of health care. Clinical information systems may be limited in scope to a single area (e.g. lab system, ECG management system) or they may be comprehensive and cover virtually all facets of clinical information (e.g. electronic patient the original discharge summary residing in the chart, with a copy of the report sent to the admitting physician, another copy existing on the transcriptionist's machine, etc.).

CONFIDENTIALITY. The condition in which sensitive data is kept secret and disclosed only to authorized parties.

CONTINUITY OF CARE RECORD (CCR). The Continuity of Care Record (CCR) is an emerging standard for communicating patient information electronically among providers. The CCR is intended to provide a snapshot of essential patient information, rather than a complete patient record, that will enable a physician to understand a patient context and provide appropriate care. The format of the CCR allows it to be used universally to help to bridge the gaps between EHR systems and improve portability of patient information.

CONTINUUM OF CARE. A holistic approach to health care delivery across multiple providers, aiming to improve the quality of care and promote wellness.

CPT (Current Procedural Terminology). CPT codes are the numbers a doctor puts on an insurance form to describe the services he or she performed. They are published annually by the American Medical Association in a *Current Procedural Terminology: CPT*, formerly *Physician's Current Procedural Terminology*. The book is commonly available in medical libraries. In addition, CPT Codes and other CPT information is available through the AMA's CPT Online page (see <https://webstore.ama-assn.org/index.jhtml>).

DATA INTEGRITY. A condition in which data has not been altered or destroyed in an unauthorized manner.

DATA MODEL. Describes the organization of data in an automated system. The data model includes the subjects of interest in the system (or entities) and the attributes (data elements) of those entities. It defines how the entities are related to each other (cardinality) and establishes the identifiers needed to relate entities to each other (primary and foreign keys). A data model can be expressed as a conceptual, logical, or physical model.

DATA WAREHOUSE. A database of information intended for use as part of a decision support system. The data is typically extracted from an organization's operational databases.

DATABASE. A set of related information created, stored, or manipulated by a computerized management information system.

DATABASE MANAGEMENT SYSTEM. Systems that manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications: commercial examples include DB2, Oracle, SQL-Server, Sybase etc.

DECISION SUPPORT SYSTEM (DSS). Software that taps into database resources and massages and presents data to assist users in making business decisions. A clinical decision support system gives physicians structured (rules-based) information to help make decisions on diagnoses, treatment plans, orders and results.

DESIGN. 1: Phase of software development following analysis, and concerned with how the problem is to be solved. 2: The process and result of describing how a system or process is to be automated. Design must thoroughly describe the function of a component and its interaction with other components. Design usually also identifies areas of commonality in systems and optimizes reusability.

DIGITAL CERTIFICATE. An electronic file used for security purposes. Certificates are used to verify that a user or computer is who they claim to be (authentication) and to encode data exchange (encryption).

DIGITAL IMAGING COMMUNICATIONS IN MEDICINE (DICOM) STANDARDS. A series of standards that enable images and associated diagnostic information to be retrieved and transferred from various manufacturers' devices as well as medical staff workstations.

DIGITAL SIGNATURE. An electronic signature generated by software that can be used to validate the sender of a message or validate that the content of a message has not been modified. Involves the transformation of an electronic message using an asymmetric cryptosystem such that a person receiving the initial message can accurately determine whether the transformation was created by the sender and whether the message has been altered since the transformation was made.

ebXML. A technical framework of standards, ebXML is intended to enable the adoption of automated Business-to-Business transaction processing for any organization of any size.

e-HEALTH. The use of emerging information and communication technology, especially the Internet, to improve or enable health and health care. In a broader sense, the term characterizes not only a technical development, but also a way of thinking about improving health care locally, regionally, and worldwide by using information and communication technology.

ELECTRONIC HEALTH RECORD (EHR). An Electronic Health Record (EHR) provides each individual with a secure and private lifetime record of their key health history and care within the health system. The record is available electronically to authorized health care providers and the individual anywhere, anytime in support of high quality care.

ELR (ELECTRONIC LAB-BASED REPORTING). ELR is the transmission of data of public health importance from clinical laboratories to public health agencies in electronic format. Ideally, data transmitted by ELR would be automated and would use standardized codes for tests and results allowing for timely and complete reporting.

ENCOUNTER. An encounter is a service event that occurs within an episode of care.

ENCRYPTION. The process of transforming plaintext data into an unintelligible form (ciphertext) such that the original data either cannot be recovered (one-way encryption) or cannot be recovered without using an inverse decryption process (two-way encryption).

ENTERPRISE. A relative business unit. A public health enterprise may be the local public health department, a particular division within a large metropolitan health department, a state health department, or the entire local-state-and-federal public health system.

ENTERPRISE ARCHITECTURE (EA). An explicit, common and meaningful structural frame of reference to enable efficient, consistent articulation of business objectives and information systems planning at all levels of an organization. EA development and evolution serves as a focal point for internal planning over time as well as the means to consistently articulate and extend organizational objectives and implications to business partners. (*See also Architecture, Federated Architecture, and IT/IS Architecture.*)

EPISODE OF CARE. An encounter or series of encounters related to the detection and subsequent care for a particular health care requirement.

EXTENSIBILITY. The ability to economically modify or add functionality.

EXTENSIBLE MARK-UP LANGUAGE. XML is a mark-up language for structuring arbitrary data based on element tags and attributes.

FEDERATED ARCHITECTURE. A collection of database systems (components) to unite into a loosely coupled federation in order to share and exchange information. The term federation refers to the collection of constituent databases participating in a federated database. (*See also Architecture, Enterprise Architecture, and IT/IS Architecture.*)

FILE TRANSFER PROTOCOL. 1: A standard high-level protocol for transferring files of different types between computers over a TCP/IP network. FTP can be used with a command line interface or graphical user interface. 2: The name of a utility program available on several operating systems which makes use of this protocol to access and transfer files on remote computers.

FIREWALL. A computer networking security device that controls access to network resources (e.g. computers and systems) using pre-defined security policies and rules.

FLEXIBILITY. The ability to support architectural and hardware configuration changes.

FORMAT. The structured arrangement of data fields and elements that make up a particular electronic transaction. The organization of data in such a way as to have a specific, agreed meaning to users.

GRAPHICAL USER INTERFACE. An interface to an application that allows users to do things by clicking on a visual screen, as opposed to typing commands on a line. GUIs (pronounced "gooey") feature the following components: a pointing device (such as a mouse), icons, windows and menus.

HEALTH LEVEL 7 (HL7) SDO. A standards development organization formed in 1987 to produce a standard for hospital information systems. HL7 received ANSI accreditation as an Accredited Standards Development Organization in 1994. The HL7 standard is an American National Standard for electronic data exchange in health care that enables disparate computer applications to exchange key sets of clinical and administrative information. HL7 is primarily concerned with movement within institutions of orders; clinical observations and data, including test results, admission, transfer and discharge records, and charge and billing information (coordinating here with X12). HL7 is the selected standard for the interfacing of clinical data for most health care institutions and has recently been approved by the U.S. Department of Health and

Human Services to be among the first set of uniform standards for the electronic exchange of clinical health information to be adopted across the federal government.

HEALTH INFORMATION EXCHANGE. Refers to local or regional networks of providers, and public health organizations, that facilitate the sharing of client/patient (individual person) information.

HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT). The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 are intended to reduce the costs and administrative burdens of health care by making possible the standardized, electronic transmission of many administrative and financial transactions that are currently carried out manually on paper. It requires that the Department of Health and Human Services adopt standards for electronic health transactions, including health claims and attachments, enrollment / dis-enrollment, eligibility, payments and premiums, claims status, referral authorizations and digital signatures. It also requires the creation of unique identifiers and standards for data confidentiality.

HL7 REFERENCE INFORMATION MODEL. A conceptual model that defines all the information from which the data content of HL7 messages is drawn.

HOSPITAL INFORMATION SYSTEM (HIS). Generic term to describe application systems that manage all facets of a hospital operation, including administrative and clinical records.

HTML (HYPERTEXT MARKUP LANGUAGE). An authoring language for the creation of World Wide Web documents.

HTTP (HYPERTEXT TRANSFER PROTOCOL). The data transfer standard that underlies the World Wide Web. It is used for all Web browser communication and for a large and growing number of automated business-to-business transaction sets.

ICD 9-CM. International Classification of Diseases - The International Classification of Diseases, Ninth Revision, Clinical Modification (ICD-9-CM) was developed in the United States to provide a way to classify morbidity data for indexing of medical records, medical case reviews, and ambulatory and other medical care programs, as well as for basic health statistics. It is based on the World Health Organization (WHO) international ICD-9. A new version modified for U.S. clinical care (ICD-10-CM), based on a tenth revision by the WHO, has not yet been adopted by the U.S. health care industry.

IMPLEMENTATION. Implementation is the carrying out, execution, or practice of a plan, a method, or any design for doing something. Implementation is the action that must follow any preliminary thinking in order for something to actually happen.

INFORMATICS. The science of information. It is often, though not exclusively, studied as a branch of computer science and information technology and is related to database, ontology and software engineering. Informatics focuses on understanding problems and then applying information (and other) technology as needed. (*Also see Bioinformatics, Medical Informatics, and Public Health Informatics.*)

INFORMATION INFRASTRUCTURE. The comprehensive information support structure, or core IT capacity, that enables achievement of broad objectives.

INFORMATION MANAGEMENT (IM). The policies, procedures and people used to direct and maintain IS deployment and operation.

INFORMATION SYSTEMS (IS). The applications that enable the use of IT to address specific business processes, in this case, the work of public health.

INFORMATION TECHNOLOGY (IT). The specific technical elements that enable electronic data management solutions.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS 1073 (IEEE1073) STANDARDS. A series of standards that allow health care providers to plug medical devices into information and computer systems. For example, systems that allow health care providers to monitor information from an ICU or through telehealth services on Indian reservations, and in other circumstances.

INTEGRATION. 1: The process of bringing together related parts into a single system. To make various components function as a connected system. 2: Combining separately developed parts into a whole so that they work together. The means of integration may vary, from simply mating the parts together at an interface to radically altering the parts or providing something to mediate between them.

INTERFACE. As a noun, an interface is either: 1) A user interface, consisting of the set of dials, knobs, operating system commands, graphical display formats, and other devices provided by a computer or a program to allow the user to communicate and use the computer or program. A graphical user interface (GUI) provides its user a more or less "picture-oriented" way to interact with technology; 2) A programming interface, consisting of the set of statements, functions, options, and other ways of expressing program instructions and data provided by a program or language for a programmer to use; or 3) The physical and logical arrangement supporting the attachment of any device to a connector or to another device. As a verb, to interface means to communicate with another person or object. With hardware equipment, to interface means making an appropriate physical connection so that two pieces of equipment can communicate or work together effectively.

INTEROPERABILITY. The ability of two or more systems or their components to exchange information and to use the information that has been exchanged. Interoperability enables 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.

ISO. International Organization for Standardization. Note that ISO is not an acronym; instead, the name derives from the Greek word "isos" which means equal. Founded in 1946, ISO is an international organization composed of national standards bodies from over 75 countries. For example, ANSI (American National Standards Institute) is a member of ISO. ISO has defined a number of important computer standards, the most significant of which is perhaps OSI (Open Systems Interconnection), a standardized architecture for designing networks.

IT PORTFOLIO. A compilation of information about an agency's investments in its IT infrastructure. The information is organized to show how these investments support the agency's mission and programs and to demonstrate the relationships among current and planned investments. The portfolio enhances the ability of key decision-makers to assess the probable impact of investments on an agency's programs and infrastructure, as well as on the overall state IT infrastructure.

IT/IS ARCHITECTURE. A framework and set of guidelines to build new information systems. IT architecture is a series of principles, guidelines, and design patterns used by an organization to direct the process of acquiring, building, modifying, and interfacing IT resources throughout the organization. These resources can include equipment, software, interface protocols, communications, development methodologies, modeling

tools, organizational structures, and more. (See also *Architecture, Enterprise Architecture, and Federated Architecture.*)

LABORATORY INFORMATION SYSTEM (LIMS). Generic term to describe application systems that manage all facets of a clinical laboratory operation, including acquiring and distributing results of laboratory exams as part of clinical records.

LDAP (LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL). An Internet protocol that email programs use to look up contact information from a server. Recommended in the PHIN technical specifications.

LEGACY SYSTEM. Generic term that is often used to reference application/processing systems that were designed and deployed in the past.

LHII (LOCAL HEALTH INFORMATION INFRASTRUCTURE). The term National Health Information Infrastructure (NHII) stems from the NCVHS report *Information for Health: A Strategy for Building the National Health Information Infrastructure* (see <http://www.ncvhs.hhs.gov/nhiilayo.pdf>). The concept of an NHII promoted in that report envisioned a network of local health information infrastructures (LHIIs), each facilitating exchange of health information in a community. (See also *Regional Health Information Infrastructure (RHIO) and Health Information Exchange.*)

LOGICAL DESIGN. The process in which the database requirements for the system are described. This is the final step in the requirements development process, prior to physical design. The products of logical design provide guidelines from which the programmer can work.

LOINC (LOGICAL OBSERVATIONS, IDENTIFIERS, NAMES AND CODES). The LOINC database provides a set of universal names and ID codes for identifying laboratory and clinical observations. The purpose is to facilitate the exchange and pooling of clinical laboratory results for clinical care, public health, outcomes management, and research.

MASTER PATIENT INDEX (MPI). A MPI (Master Person Index) is a system which coordinates client identification across multiple systems namely by collecting and storing IDs and person-identifying demographic information from source system (track new persons, track changes to existing persons). These systems also take on several other tasks and responsibilities associated with client ID management.

MEDICAL INFORMATICS. The application of information technology to health care.

MESSAGE. A digital representation of information; a computer-based record.

MIDDLEWARE. Software systems that facilitate the interaction of disparate components through a set of commonly defined protocols. The purpose is to limit the number of interfaces required for interoperability by allowing all components to interact with the Middleware using a common interface.

NCD CP (NATIONAL COUNCIL ON PRESCRIPTION DRUG PROGRAMS) STANDARDS. A series of standards for ordering drugs from retail pharmacies to standardize information between health care providers and the pharmacies. These standards already have been adopted under the Health Insurance Portability and Accountability Act (HIPAA) of 1996.

NCVHS (NATIONAL COMMITTEE ON VITAL AND HEALTH STATISTICS). External Advisory Committee to the Secretary of the Department of Health and Human Services (DHHS), and to the DHHS Data Council. Consists of 16 members with overlapping four-year terms. The National Center for Health Statistics (NCHS) serves as Executive Secretary. The NCVHS was established in 1949 in response to a recommendation by the World Health Organization (WHO). The committee was re-chartered in January 1996 to include more direct focus on data standardization and privacy activities.

NEDSS. An initiative that promotes the use of data and information system standards to advance the development of efficient, integrated, and interoperable surveillance systems at federal, state and local levels. It is a major component of the Public Health Information Network (PHIN).

NEDSS LOGICAL DATA MODEL. The CDC-defined data model based on HL7, LOINC and SNOMED.

NHII (NATIONAL HEALTH INFORMATION INFRASTRUCTURE). In its 2001 report, *Information for Health: A Strategy for Building the National Health Information Infrastructure* (see <http://ncvhs.hhs.gov/nhiilayo.pdf>), the National Committee on Vital and Health Statistics (NCVHS) advances a series of recommendations to the U.S. Department of Health and Human Services (DHHS) to develop NHII, defined as an "effective, comprehensive health information infrastructure that links all health decision makers, including the public."

NHIN (NATIONAL HEALTH INFORMATION NETWORK). A National Health Information Network would link disparate health care information systems together to allow patients, physicians, hospitals, public health agencies, and other authorized users across the nation to share clinical information in real-time under stringent security, privacy, and other protections. (See <http://www.hhs.gov/news/press/2005pres/20050603.html>).

NON-REPUDIATION. Assurance that a principal (user) cannot deny being the originator of a message (or transaction) after sending it.

NORMALIZATION. The process of creating a uniform and agreed upon set of standards, policies, definitions and technical procedures to allow for interoperability.

OPEN SYSTEMS INTERCONNECTION (OSI). A seven-layer reference model developed by ISO as a framework for the development of standards for interconnecting heterogeneous computers. The layers from the top are Application, Presentation, Session, Transport, Network, Data Link and Physical.

ORDER ENTRY SYSTEM. An application system that provides the ability to create and manage orders for exams, drugs, procedures and/or other materials.

PARSER. A function that recognizes valid sentences of a language by analyzing the syntax structure of a set of tokens passed to it from a lexical analyzer.

PATIENT RECORD. Patient record is information about a single patient/person. The patient record system is the set of components that comprise the mechanism by which patient/person records are created, used, stored and retrieved. The system includes the patient records and associated metadata. Patient record system metadata is data about the patient record system. This includes administrative metadata (lists of doctors, assembly order, copies of allowable forms, etc. and clinical metadata (current nursing procedures, historical practice standards, charting by exception standards). Metadata is required to describe the patient

record system more fully and to define the standard of practice at the time of the recorded events, thus providing context for historical decisions.

PERFORMANCE. The ability to execute functions fast enough to meet requirements.

PERFORMANCE INDICATORS. Summarize the focus (e.g., workforce capacity, customer service) of performance goals and measures, often used for communication purposes and preceding the development of specific measures.

PERFORMANCE MEASURES. Quantitative measures of capacities, processes, or outcomes relevant to the assessment of a performance indicator (e.g., the number of trained epidemiologists available to investigate, percentage of clients who rate health department services as “good ”or “excellent”).

PERFORMANCE STANDARDS. Objective standards or guidelines that are used to assess an organization’s performance (e.g., one epidemiologist on staff per 100,000 population served, 80 percent of all clients who rate health department services as “good ” or “excellent”.) Standards may be set based on national, state, or scientific guidelines; by benchmarking against similar organizations; based on the public’s or leaders’ expectations (e.g., 100% access, zero disparities); or other methods.

PERFORMANCE TARGETS. Set specific and measurable goals related to agency or system performance. Where a relevant performance standard is available, the target may be the same as, exceed, or be an intermediate step toward that standard.

PERSONAL HEALTH RECORD (PHR). A personal health record (PHR) is an individual’s personal collection of information, in an electronic form. It is controlled by the individual, and may contain a patient’s own notes in addition to electronic information from providers.

PHIN (PUBLIC HEALTH INFORMATION NETWORK). A national initiative of the Centers for Disease Control and Prevention (CDC) to enable real-time data exchange between organizations for the promotion of interoperability, collaboration, rapid dissemination of critical information, and computer-assisted statistical analysis.

PICTURE ARCHIVING AND COMMUNICATIONS SYSTEM (PACS). 1: Application system that uses an image server to exchange X-rays, CT scans and other medical images over a network. Mini-PACS specialize in one type of image such as an ultra- sound. 2: Application system that is used to store, retrieve and manage digital images.

PRIMARY CARE PHYSICIAN (PCP). A physician involved in a practice that acts as the first line of access to the health care system. Usually a general practitioner (GP).

PRIVACY. The right of an individual to live free of intrusive monitoring of their personal affairs by third parties not of their choosing.

PROJECT MANAGER. A project manager is a facilitator and a problem solver. The ideal project manager does whatever it takes to ensure that the members of the project team can do their work. This means working with management to ensure they provide the resources and support required as well as dealing with team issues that may be negatively impacting a team’s productivity. The actions of a project manager should be almost unnoticeable. When a project is moving along smoothly, the project team may be tempted to

question the need for a project manager. However, when the skilled project manager is taken out of the mix, the project is much more likely to miss deadlines and exceed budgets.

PUBLIC HEALTH INFORMATICS. Public health informatics is the systematic application of information and computer science and technology to public health practice, research and learning. In this context, public health informatics refers to the strategic use of all information resources to satisfy the business requirements of public health.

REFERENCE INFORMATION MODEL (RIM). HL7 information model from which all other information models (e.g., R-MIMs) and messages are derived.

REGISTRY. Directory-like system that focuses solely on managing data pertaining to one conceptual entity.

REPUDIATION (See also NON-REPUDIATION). The denial or attempted denial by an entity involved in a communication of having participated in all or part of the communication.

REQUIREMENTS DEFINITION. Requirements definition refines understanding of the workflow and defines database outputs needed to support that work. Requirements definition serves to specifically define the functionality to be supported. In addition, the physical constraints are examined and the specific project scope determined. Requirements definition answers the question, "How would you see information systems supporting (task X)?"

RHIN (REGIONAL HEALTH INFORMATION NETWORK). The technology infrastructure and associated applications and services enabling RHIO participants to securely access clinical data across enterprise borders.

RHIO (REGIONAL HEALTH INFORMATION ORGANIZATION). A collaboration of local health care stakeholders providing leadership, oversight, fiduciary responsibility, and governance for the development, implementation, and application of secure health information exchange across care settings. Intended to reflect the health care priorities of a local area as well establish the legitimacy and trustworthiness of this activity to clinicians and consumers. (See also *Health Information Exchange, and LHII - Local Health Information Infrastructure.*)

ROI (RETURN ON INVESTMENT). For a given use of money in an enterprise, ROI is how much profit or cost saving is realized. An ROI calculation is sometimes used along with other approaches to develop a business case for a given proposal.

ROLE-BASED ACCESS CONTROL. Security environment in which users' rights to access or change information are controlled by the role or roles they fulfill within the organization; that is 'what' they are, rather than 'who' they are.

RxNorm. Clinical drug nomenclature produced by NLM, in consultation with FDA, VA, and the HL7 standards development organization. RxNorm provides standard names for clinical drugs and for dose forms as administered.

SAML. Secure Assertion Markup Language - SAML provides an XML-based framework for exchanging authentication and authorization information, enabling single sign-on—the ability to use a variety of Internet resources without having to log in repeatedly. Provides a technology neutral way to exchange security information using XML to communicate authentication, authorization, and other user attribute information.

SCALABILITY. The ability to support the required quality of service as load increases.

SECURITY. The ability to ensure that information is neither modified nor disclosed except in accordance to the security policy.

SECURITY ARCHITECTURE. A plan and set of principles for an administrative domain and its security domains that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment. A complete security architecture for a system addresses administrative security, communication security, computer security, emanations security, personnel security, and physical security, and prescribes security policies for each. A complete security architecture needs to deal with both intentional, intelligent threats and accidental threats. A security architecture should explicitly evolve over time as an integral part of its administrative domain's evolution.

SECURITY POLICY. A set of rules and practices that specify or regulate how a system or organization provides security services to protect resources. Security policies are components of security architectures. Significant portions of security policies are implemented via security services, using security policy expressions.

SECURITY STANDARD. A set of requirements adopted or established to preserve and maintain the confidentiality and privacy of electronically stored, maintained, or transmitted health information.

SERVICE ENDPOINT. A name used to specify the target of an electronic message. For example the World Wide Web uses URLs (Uniform Resource Locators) as service endpoints that we are familiar with as the ubiquitous www.somewebpagename.com.

SERVICE LEVEL AGREEMENT (SLA). A service-level agreement is a contract that defines the technical support or business parameters that an application service provider or other IT outsourcing firm will provide its clients. The agreement typically spells out measures for performance and consequences for failure.

SIMPLE OBJECT ACCESS PROTOCOL (SOAP). Lightweight protocol intended for exchanging structured information in a decentralized, distributed environment. It uses XML technologies to define an extensible messaging framework providing a message construct that can be exchanged over a variety of underlying protocols. The framework has been designed to be independent of any particular programming model and other implementation specific semantics.

SNO (SUB-NETWORK ORGANIZATION). Refers to a health information exchange network comprising providers that are linked by a common purpose or function rather than geography.

SNOMED (SYSTEMIZED NOMENCLATURE OF MEDICINE). 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.

SQL (STRUCTURED QUERY LANGUAGE). A standard language for requesting information from a database.

SSL (SECURE SOCKETS LAYER). The de-facto standard for executing secured transactions over the World Wide Web (for example, SSL is in use when the padlock icon is displayed during secure online

transactions). SSL protects confidentiality and data integrity through encryption and can also provide authentication of the parties involved in a transaction.

STANDARDS. Clearly defined and agreed upon conventions for the operation of specific computing operations, formats, and data elements.

SYSTEM ARCHITECT. The system architect has the task of putting together the skeleton of an information system project. Depending on the specifications gathered by the business (or requirements) analyst, the system architect will choose to focus on ease of maintenance, application performance, compatibility with existing systems, or a combination of all three. Each decision that the system architect makes has to be carefully considered because a wrong move the beginning of a project can have damaging effects later in the information systems development life cycle.

SYSTEM SECURITY. That component of a security program that integrates physical and personnel security with procedures designed to protect the entity/system needing protection.

TCP/IP (TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL). Standards that are the basis for data transmission on the Internet and over LANs (local area networks) and WANS (wide area networks).

TECHNICAL ARCHITECTURE. 1: A technical architecture identifies and describes the types of applications, platforms, and external entities; their interfaces; and their services, as well as the context within which the entities interoperate. The technical architecture is the basis for selecting and implementing the infrastructure to establish the target architecture. 2: The specific code plans to build an IT solution is called the Technical Architecture. It is the IT "blue print" of the planned technical roll out.

TRANSACTION. A unit of interaction with a DBMS or similar system. It must be treated in a coherent and reliable way independent of other transactions.

TRUSTED THIRD PARTY. In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers. Relative to information systems, a trusted third party does not connote the existence of a trustor-trustee or other fiduciary relationship.

UML. Unified Modeling Language: general purpose language for specifying and visualizing software systems. Favored for object-oriented software development.

VIRTUAL PRIVATE NETWORK (VPN). Secure and encrypted connection between two points across the Internet. VPNs transfer information by encrypting and encapsulating traffic in IP packets and sending the packets over the Internet. That practice is called tunneling. Most VPNs are built and run by Internet service providers and secure protocols like Point to Point Tunneling Protocol (PPTP) to ensure that data transmissions are not intercepted by unauthorized parties.

WEB SERVICES. A Web service is a software system identified by a URI [RFC 2396], whose public interfaces and bindings are defined and described using XML. Its definition can be discovered by other software systems. These systems may then interact with the Web service in a manner prescribed by its definition, using XML based messages conveyed by Internet protocols.

X.500. A standard for computer based directories.

X.509. A standard for defining digital certificates.

X12. A set of standards for electronic data exchange for business transactions.

X12. A standards development organization that develops uniform standards for inter-industry electronic interchange of business transactions - electronic data interchange (EDI). X12N, a subcommittee of X12, develops standards for health care insurance and claims processing.

XML (EXTENSIBLE MARKUP LANGUAGE). A language for formatting and describing data that enables exchange between systems.

XML (EXTENSIBLE MARKUP LANGUAGE). 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.

062405