

The following is a list of technical terms and acronyms used in discussions about Health Information Technology (HIT) and Health Information Exchange (HIE).

Acceptable Use Policy: set of rules and guidelines that specify appropriate use of computer systems or networks

Access Control: preventing the unauthorized access or use of health information resources

Accountability: makes sure that the actions of a person or agency may be traced to that individual or agency

Anonymized: personal information that has been processed to make it impossible to know whose information it is

Antivirus Software: a software program that checks a computer or network to find all major types of harmful software that can damage a computer system or networks

Audit Trail: a record showing specific individuals who have accessed a computer and what they have done while they were in that computer

Authentication: verifying the identity of a user, process, or device before allowing access to resources in an information system

Backup: a copy of an individual's files made to help regain any lost information in his or record, if necessary

Certification: a complete examination of an information system to be sure that the system can perform at the level required to support the intended results and meet the national standards for health information technology

Computerized Provider Order Entry (CPOE): a computer application that allows a physician's orders for diagnostic and treatment services (such as medications, laboratory, and other tests) to be entered electronically instead of being recorded on order sheets or prescription pads; the computer compares the order against standards for dosing, checks for allergies or interactions with other medications, and warns the physician about potential problems

Confidentiality: obligation of a person or agency that receives information about an individual, as part of providing a service to that individual, to protect that information from unauthorized persons or unauthorized uses; confidentiality also includes respecting the privacy interest of the individuals who are associated with that information

Consent: consent is the permission granted by an authorized person that allows the provider, agency, or organization to release information about a person; the authorized person may be either the subject of the information or a designated representative, such as

a parent or guardian; law, policy and procedures, and business agreements guide the use of consent

Consolidated Health Informatics (CHI) Initiative: one of the 24 Presidential eGovernment initiatives with the goal of adopting vocabulary and messaging standards to facilitate communication of clinical information across the federal health enterprise; CHI now falls under FHA (Federal Health Architecture)

Consumer-Patient: members of the public who receive healthcare services

Consumer-Provider: any recipient or legal proxy of a recipient of healthcare who wishes to create preferences regarding aspects of their care and how their medical information is accessed or shared

Consumer Preference Profile: a collection of the consumer's individual declarations which represent the consumer's decisions to provide access or deny access to all or portions of their health information

Decryption: The process used to "unscramble" information so that a "scrambled" or jumbled message becomes understandable

Decision-Support System (DSS): computer tools or applications to assist physicians in clinical decisions by providing evidence-based knowledge in the context of patient specific data; examples include drug interaction alerts at the time medication is prescribed and reminders for specific guideline-based interventions during the care of patients with chronic disease; information should be presented in a patient-centric view of individual care and also in a population or aggregate view to support population management and quality improvement

De-identified Health Information: name, address, and other personal information are removed when sharing health information so that it cannot be used to determine who a person is

Digital Certificate: like a driver's license, it proves electronically that the person is who he or she says they are

Digital Signature: uniquely identifies one person electronically and is used like a written signature; for example a doctor or nurse may use a digital signature at the end of an email to a patient just as she would sign a letter

Disclosure: the release, transfer, of information to someone else

Electronic Health Record (EHR): a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making; the EHR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated; it can also prevent delays in response that result in gaps in care; the EHR can also support the collection of data for uses other than clinical care, such

as billing, quality management, outcome reporting, and public health disease surveillance and reporting; also known as Electronic Medical Record (EMR)

Electronic Medical Record (EMR): a real-time patient health record with access to evidence-based decision support tools that can be used to aid clinicians in decision-making; the EMR can automate and streamline a clinician's workflow, ensuring that all clinical information is communicated; it can also prevent delays in response that result in gaps in care; the EMR can also support the collection of data for uses other than clinical care, such as billing, quality management, outcome reporting, and public health disease surveillance and reporting; also known as Electronic Health Record (EHR)

Electronic Prescribing: a type of computer technology whereby physicians use handheld or personal computer devices to review drug and formulary coverage and to transmit prescriptions to a printer or to a local pharmacy; e-prescribing software can be integrated into existing clinical information systems to allow physician access to patient specific information to screen for drug interactions and allergies; also known as e-Prescribing or eRx

E-Prescribing: a type of computer technology whereby physicians use handheld or personal computer devices to review drug and formulary coverage and to transmit prescriptions to a printer or to a local pharmacy; e-prescribing software can be integrated into existing clinical information systems to allow physician access to patient specific information to screen for drug interactions and allergies; also known as Electronic Prescribing or eRx

Encryption: the translation of information to a code to keep it secret

Enterprise Architecture: a strategic resource that aligns business and technology, leverages shared assets, builds internal and external partnerships, and optimizes the value of information technology services

Event: any observable occurrence in a network or system

Health Information: according to HIPAA, any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse; and relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual

Health Information Exchange (HIE): the electronic movement of health-related information among organizations according to nationally recognized standards

Health Information Privacy: an individual's right to control the acquiring, use or release of his or her personal health information

Health Information Security: the protection of a person's personal information from being shared without the owner's permission

Health Information Technology (HIT): the application of information processing involving both computer hardware and software that deals with the storage, retrieval, sharing, and use of health care information, data, and knowledge for communication and decision-making

Health Insurance Portability and Accountability Act (HIPAA): the law Congress passed in 1996 to make sure that health insurance would not stop when he or she changed employer; it also requires that health information be kept private (

Health Record Banks: entities/mechanisms for holding an individual's lifetime health records; this information may be personally controlled and may reside in various settings such as hospitals, doctor's offices, clinics, etc.

Identity: a unique characteristic of an individual person; for example, a driver's license proves that this person is who he or she says they are

Inappropriate Usage: using personal information without that person's permission

Incident Response Plan: the instructions or procedures that an organization can use to detect, respond to, and limit the effect of computer system attacks

Individually Identifiable Health Information (IIHI): according to the Health Insurance Portability and Accountability Act (HIPAA), IIHI is information that is a subset of health information, including demographic information collected from an individual, and: (1) is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (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; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual

Informed Consent: information exchange between a clinical investigator and research subjects; this exchange may include question/answer sessions, verbal instructions, measures of understanding, and reading and signing informed consent documents and recruitment materials

Integrity: data or information that has not been changed or destroyed in an unauthorized way

Interoperability: the ability of systems or components to exchange health information and to use the information that has been exchanged accurately, securely, and verifiably, when and where needed

Limited Data Set: health information that does not contain identifiers; it is protected but may be used for certain purposes without the owner's consent

Log In/Logging Into: the action a person must take to confirm his or her identity before being allowed to use a computer system

Master Patient Index (MPI): a list of all known patients in an area, activity or organization

Meaningful Use: the American Recovery and Reinvestment Act authorizes the Centers for Medicare & Medicaid Services (CMS) to provide a reimbursement incentive for physician and hospital providers who are successful in becoming “meaningful users” of an electronic health record (EHR); these incentive payments begin in 2011 and gradually phase down; starting in 2015, providers are expected to have adopted and be actively utilizing an EHR in compliance with the “meaningful use” definition or they will be subject to financial penalties under Medicare

National Health Information Network (NHIN): an interoperable, network based on standards that is across the nation and enables the secure exchange of health information

National Provider Identifier (NPI): a system for classifying all providers of health care services, supplies, and equipment covered under HIPAA

Non-Repudiation: the process of confirming proof of information delivery to the sender and proof of sender identity to the recipient¹

Notice of Privacy Practice: HIPAA requires that all covered health plans, healthcare clearinghouses, or healthcare providers give patients a document that explains their privacy practices and how information about the patients’ medical records may be shared; also known as Privacy Notice

Office of the National Coordinator for Health Information Technology (ONC): ONC is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information

Opt-in: patients or consumers adding themselves

Opt-out: patients or consumers removing themselves

Patient Permission: the consent or authorization that patients provide regarding their health care or the use of their health information

Permitted Purposes: authorized reasons

Personal Health Record (PHR): an electronic application through which individuals can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment

Protected Health Information: health information transmitted or maintained in any form that can reasonably be used to identify an individual

Providers: the health care clinicians within healthcare delivery organizations with direct patient interaction in the delivery of care, including physicians, nurses and other clinicians; this can also refer to health care delivery organizations

Privacy Notice: HIPAA requires that all covered health plans, healthcare clearinghouses, or healthcare providers give patients a document that explains their privacy practices and how information about the patients' medical records may be shared; also known as Notice of Privacy Practice

Safeguards: measures that protect the security of health information

Security: processes, practices and software that secure health information from unauthorized access, ensuring that the information is not altered and that it is accessible when needed by those authorized

Sensitive Information: health information such as details on substance abuse, family planning, mental health and others

Unauthorized Access: this is the act of gaining access to a network, system, application, health information or other resource without permission

Unauthorized Disclosure: an act that involves exposing, releasing or displaying health information to those not authorized to have access to the information

Use: sharing, employing, applying, utilizing, examining or analyzing health information

References:

Daniel, Posnak, Health Information Security and Privacy Collaboration - [Health Information Technology/Health Information Exchange Privacy and Security Glossary](#) (Office of the National Coordinator for Health Information Technology)

North Carolina Healthcare Information and Communications Alliance, Inc., [Glossary of Top 45 Security & Privacy Terms](#)

Office of the National Coordinator for Health Information Technology, [Health IT Meaningful Use](#)

Office of the National Coordinator for Health Information Technology, [Health IT Terms - Glossary of Selected Terms Related to e-Health](#)

US Department of Health and Human Services, Office of the National Coordinator, [Consumer Preferences Draft Requirements Document](#)