



# Health IT/HIE Privacy and Security Terms and Definitions

## Acceptable Use Policy

- Set of rules and guidelines that specify appropriate use of computer systems or networks.

## Access Control

- Preventing the unauthorized 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 which 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.

## 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 my files made to help regain any lost information in my 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.

## 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 the subject of the information or they may be a designated representative such as a parent or guardian. Law, policy and procedures, and business agreements guide the use of consent.



## **Data Use Agreement**

- An agreement between a health provider, agency, or organization and a designated receiver of information to allow for the use of limited health information for the purpose of research, public health, or health care operations. The agreement assures that the information will be used only for specific purposes.

## **Decryption**

- The process used to “unscramble” information so that a “scrambled” or jumbled message becomes understandable.

## **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 e-mail to a patient just as he or she would sign a letter.

## **Disclosure**

- The release, transfer, of information to someone else.

## **Encryption**

- The translation of information to a code to keep it secret.

## **Event**

- Any observable occurrence in a network or system.

## **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 health information from being shared without the owner’s permission.

## **Health Insurance Portability and Accountability Act of 1996 (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 and secure.

## **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.

### **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.

### **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.

### **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 recipient.

### **Notice of Privacy Practices or Privacy Notice**

- HIPAA requires that all covered health plans, health care clearinghouses, or health care providers give patients a document that explains their privacy practices and how information about the patients' medical records may be shared.

### **Opt-in/Opt-out**

- Patients or consumers adding or 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.

### **Protected Health Information**

- Health information transmitted or maintained in any form that can reasonably be used to identify an individual.



## **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.

## **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.

## **Nationwide Health Information Network (NHIN)**

- An interoperable network based on standards that is across the nation and enables the secure exchange of health information.

## **Use**

- Sharing, employing, applying, utilizing, examining, or analyzing health information.

*These materials were compiled by the Consumer Engagement and Education Collaborative of the Health Information Security and Privacy Collaboration.*

*This publication is made possible by the Health Information Security and Privacy Collaboration (HISPC) a contract managed by the Office of the National Coordinator for Health IT (ONC).*