March 31, 2009

Health Information Security and Privacy Collaboration

Health Information Technology / Health Information Exchange Privacy and Security Glossary

Prepared for

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by
Multi-State Consumer Education and Engagement Collaborative
Common Project

Kansas, Georgia

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

Contract Number HHSP 233-200804100EC
RTI Project Number 0211557.000.007.100

March 31, 2009

Health Information Security and Privacy Collaboration

Health Information Technology / Health Information Exchange Privacy and Security Glossary

RTI International
230 W Monroe, Suite 2100
Chicago, IL 60606

Jodi Daniel, JD, MPH, Director
Steven Posnack, MHS, MS, Policy Analyst
Office of Policy and Research
Office of the National Coordinator for Health IT
200 Independence Avenue, SW, Suite 729D
Washington, DC 20201

Prepared by

Helen Connors, Kansas
Doris Konneh, Georgia
Alicia McCord-Estes, Georgia
Christina Stephan, Kansas
Victoria Wangia, Kansas

Identifiable information in this report or presentation is protected by federal law, section 924(c) of the Public Health Service Act, 42 USC. § 299c-3(c). Any confidential identifiable information in this report or presentation that is knowingly disclosed is disclosed solely for the purpose for which it was provided.

Table of Contents

These materials were compiled by the Consumer Engagement and Education Collaborative of the Health Information Security and Privacy Collaboration (HISPC/CEEC).

Introduction

This glossary project was completed by the Health Information Security and Privacy Collaboration (HISPC) consumer education and engagement collaborative (CEEC) and led by individuals from the states of Kansas and Georgia. All the states in the HISPC CEEC have the common goals of educating consumers about health information technology (health IT)/ health information exchange (HIE) privacy and security and engaging consumers. The core HISPC CEEC project team consists of representatives from 8 states:

Colorado: Phyllis Albritton
Georgia: Alicia McCord-Estes, PMP
Kansas: Victoria Wangia PhD, MS
Massachusetts: Jerilyn Heinold MPH
New York: Ellen Flink MBA
Oregon: Dawn Bonder JD
Washington: Peggy Evans PhD
West Virginia: Patty Ruddick RN, MSN

The glossary project is one among several common projects being completed by the HISPC CEEC. The target audience of the HISPC CEEC is the *consumer*. Therefore, the document includes the *top 45* health IT/HIE privacy and security terms for those who communicate with consumers, as a starting point on presenting definitions with improved readability. A select number of Health IT/ HIE privacy and security terms are included as an example and starting point for future work. With further conversion of definitions to lower literacy levels, the definitions will also be useful to the individual consumer. The *top 45 terms* included in this document were selected from a document with over 500 health IT/HIE privacy and security terms and definitions, developed by the HISPC CEEC glossary project team. The 45 terms were selected for this document through a consensus process that involved ranking and selecting terms by all the members of the HISPC CEEC.

To accomplish this:

- The glossary team developed a ranking tool that included over 500 health IT/HIE privacy and security terms.
- The glossary team then requested the other members of the HISPC CEEC to rank their top 60 terms.
- The glossary team proceeded to select 45 of the most commonly ranked terms.
- The terms were then presented to a volunteer literacy expert who provided recommendations on how to modify the definitions to improve readability.
- The glossary team made modifications to the definitions based on the literacy expert's feedback. However, the team recommends that the next step would need to involve a literacy expert to determine the specific literacy level and the validity of the definitions presented in this glossary.

Any feedback and recommendations can be e-mailed to Victoria Wangia: vwangia@kumc.edu.

Top 45 Consumer 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 heath information.

Use

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