

A FRAMEWORK OF PRINCIPLES AND RESOURCES FOR ADDRESSING THE 4AS

Excerpts from the Minnesota Privacy and Security Project Reports for the:

Privacy and Security Solutions for Interoperable Health Information Exchange Contract

**More detailed information regarding
this framework and the project's activities
is available at:**

<http://www.health.state.mn.us/e-health/mpsp/>

The Minnesota Privacy and Security Project

James I. Golden, Project Director
Minnesota Privacy and Security Project
Minnesota Department of Health
85 East Seventh Place, Suite 220
Saint Paul, MN 55101

E-mail: james.golden@health.state.mn.us
Telephone: 651.201.4819

April 30, 2007



GENERAL PRINCIPLES FOR AUTHORIZING AND AUTHENTICATING INDIVIDUALS, SETTING ACCESS CONTROLS, AND AUDITING IN A HEALTH INFORMATION EXCHANGE

Assumptions

- A.1** A Health Information Exchange will require all participants to sign a standard participation agreement. This agreement will specify the terms of the relationship and the roles, rights and responsibilities of each party. The signing of this agreement means that each participant will adhere to the policies and procedures of the Health Information Exchange.
- A.2** Health Information Exchanges will define the type of patient health information to be exchanged or accessed between organizations participating in a Health Information Exchange.
- A.3** Health Information Exchanges will exchange patients' health information using national standards for data content and data definitions.
- A.4** The exchange of patient health information through a Health Information Exchange will occur using standard-based messaging and/or view-only access to provider's electronic health records.
- A.5** All organizations participating in a Health Information Exchange will have adopted and implemented generally accepted security programs, policies, and procedures to ensure the confidentiality, integrity, and availability of patients' health information.

Authorization Principles

- P1.1** All individuals having access to patients' health information through a Health Information Exchange will be assigned a unique ID for accessing the health information. Consistent with the authentication principles, each ID for accessing patients' health information shall require at least single-factor authentication (e.g., password) to access health information.
- P1.2** When an individual is granted access to patients' health information through a Health Information Exchange from a particular organization participating in a Health Information Exchange, it should be that participating organization's responsibility to authorize, maintain, and terminate the individual's access to patient health information.
- P1.3** The ability of individuals to access patients' health information through a Health Information Exchange should be set using role-based access standards which are developed and accepted by all organizations participating in a Health Information Exchange.
- P1.4** All organizations participating in a Health Information Exchange should develop and accept security credentialing guidelines for authorizing individuals to access patients' health information through a Health Information Exchange. The security credentialing guidelines and process should be as streamlined as possible and minimally include: a) verifying the identity of individuals authorized to access/exchange health information; b) defining the appropriate role-based access for individuals authorized to access/exchange health information; and c) providing individuals the information and mechanisms to be authenticated when accessing/exchanging health information.
- P1.5** Medical credentialing of health care providers (distinct from security credentialing) should not be required by organizations participating in a Health Information Exchange when the health care

provider is only exchanging health information using standard-based messages or accessing health information in view-only access.

Authentication Principles

- P2.1** All organizations participating in a Health Information Exchange should minimally require single-factor authentication for verifying the identity of all individuals authorized to access patients' health information within each organization.
- P2.2** All organizations participating in a Health Information Exchange should minimally require two-factor authentication for verifying the identity of all individuals accessing patients' health information through the Health Information Exchange (i.e., across participating organizations).
- P2.3** Authentication of individuals accessing patients' health information through a Health Information Exchange should be as seamless as possible when accessing information across participating organizations.
- P2.4** From the end-user's perspective (i.e., health care providers), the authentication of individuals accessing patients' health information through a Health Information Exchange should be the same process regardless of which participating organization's health information is being accessed.

Access Control Principles

- P3.1** Health care providers should only access information for patients with whom they have a treatment relationship and then only the health information relevant to the treatment being provided.
- P3.2** All organizations participating in a Health Information Exchange should develop and accept written policies and procedures for accessing and exchanging patients' health information through the Health Information Exchange.
- P3.3** All organizations participating in a Health Information Exchange should develop and accept minimum standard training requirements for educating individuals about the policies and procedures for accessing/exchanging patients' health information through a Health Information Exchange.
- P3.4** All organizations participating in a Health Information Exchange should develop and accept common sanction policies for addressing situations when individuals violate the policies and procedures for accessing/exchanging patients' health information through the Health Information Exchange.
- P3.5** Health Information Exchanges should develop policies and procedures for disabling individuals' access to patients' health information through a Health Information Exchange for inappropriately accessing patients' health information.
- P3.6** Health Information Exchanges should have policies and procedures for terminating a logged-in individual's session accessing patients' health information due to inactivity within the session.

Auditing Principles

- P4.1** All organizations participating in a Health Information Exchange should develop and accept minimum standards for routine auditing of individuals' access to patients' health information through the Health Information Exchange.
- P4.2** All organizations participating in a Health Information Exchange should maintain audit logs that document individuals accessing patients' health information. The audit logs should minimally

identify: a) the individual accessing the health information; b) the health information being accessed; c) the date and time of the access; and d) all failed log-ins.

- P4.3** All organizations participating in a Health Information Exchange should develop and accept: a) the data elements to be maintained and exchanged for auditing individuals' access to patient health information; b) the frequency at which the auditing data will be exchanged between organizations participating in the Health Information Exchange; and c) the minimum retention time of audit logs maintained for auditing individuals' access to patient health information.
- P4.4** All organizations participating in a Health Information Exchange should develop and accept procedures for: a) alerting other participating organizations of situations where patients' health information may have been inappropriately accessed; and b) jointly investigating situations where patients' health information may have been inappropriately accessed.

HEALTH CARE SECURITY STANDARDS AND DEFINITIONS

- **International Standards Organization (www.iso.org)**
 - *ISO 17799 – Code of Practice for information security*
 - *ISO 27799 – Security Management in health using ISO 17799*
 - *ISO/CD TS 21298 – Health informatics functional and structural roles*
 - *ISO/TS 21091:2005 – Directory services for security, communications and identification of professionals and patients*
 - *ISO/TS 17090-1:2002 – Health informatics – Public Key infrastructure*
 - *ISO 26000 – Standard on Social responsibility (In development – 2008)*
 - *ISO/TS 22600-1:2006, “Health informatics – Privilege management and access control – Part 1: Overview and policy management”*

- **ASTM International (www.astm.org)**
 - *E1762-95(2003) – Standard guide for electronic authentication of health care information*
 - *E1985-98(2003) – Standards guide for user authentication and authorization*
 - *E1986-98(2005) – Standard guide for information access privileges to health information*
 - *E1869-04 – Standard guide for confidentiality, privacy, access and data security principles for health care including EHRs*
 - *E1988-98 – Standard guide for training of persons who have access to health information*
 - *E2147-01 – Standard specification for audit and disclosure logs for use in health information systems*

- **US Health and Human Services Resources (www.os.dhhs.gov/healthit)**
 - *Office of the National Coordinator for Health Information Technology (ONCHIT – www.hhs.gov/healthit/onc/mission/)*
 - *The Center for Disease Control and Prevention’s site on the Public Health Information Network (www.cdc.gov/phn)*
 - *Healthcare Information Technology Standards Panel (HITSP) of the American National Standards Institute (ANSI)
(http://www.ansi.org/standards_activities/standards_boards_panels/hisb/hitsp.aspx?menuid=3/)*
 - *American Health Information Community (AHIC) – Confidentiality, Privacy & Security Workgroup (www.hhs.gov/healthit/ahic/cps_main.html)*

- *Certification Commission for Healthcare Information Technology (CCHIT) Product Certification (www.cchit.org)*
- *HHS Privacy & Security Activities (www.hhs.gov/healthit/privacy/)*
- *HHS Agency for Healthcare Research and Quality – HISPC project (www.healthit.ahrq.gov/privacyandsecurity)*
- *2nd Nationwide Health Information Network forum: NHIN Security Services (http://www.hhs.gov/healthit/nhin/forum_oct2006.html)*
- **Other resources**
 - National Institute of Standards and Technology's Computer Security Resource Center (<http://csrc.nist.gov>) (NIST publishes many security guidelines for federal agencies.)
 - Computer Emergency Response Team, a federal funded research and development center at Carnegie Mellon University (www.cert.org)
 - Institute of Internal Auditors, It Security (www.theiia.org) Information security auditing
 - Information Systems Audit and Control Association, "Control Objectives for Informational and related technology (COBIT) (www.isaca.org/cobit)
 - ISSA's General Accepted Information Security Procedures (www.issa.org) The Minnesota Chapter's Healthcare Security Professional Interest Group (www.mn-issa.org)
 - IHE Initiative by HIMSS, ACC & RSNA (www.ihe.net)
 - HL7 (www.hl7.org)
 - The Liberty Alliance (www.projectliberty.org)
 - eHealth Initiative's Technology Working Group (<http://www.ehealthinitiative.org/TechWGMaterials.msp>)
 - International Information Systems Forensics Association (www.iifsa.org) The Minnesota chapter (www.mn-isfa.org)
 - The Markle Foundation's Connecting for Health Common Framework (www.connectingforhealth.org)
 - Healthcare Information and Management Systems Society (www.himss.org)
 - The Minnesota chapter (www.himss-mn.org)
 - American Health Information Management Association (www.ahima.org) The Minnesota chapter (www.mnhima.org)
 - The Public Health Data Standards Consortium (<http://phdatastandards.info/>)