



CALIFORNIA PRIVACY AND SECURITY ADVISORY BOARD COMPARATIVE ANALYSIS OF ACCESS CONTROLS (ALL SCENARIO/USE CASES)



COMMITTEE:	SECURITY – Access Control	Date: April 2009
ISSUE:	Safeguard the personal health information of the patients' directives for consent to have their records exchanged electronically utilizing access controls.	
BACKGROUND	There is a potential that the privacy standards for patients' consent to allow their personal health records to be exchanged electronically in a health information exchange may be a hybrid standard that may incorporate more than one different alternative. For example, the standard may incorporate the use of an opt out alternative for some medical information, an opt in with restrictions for sensitive information, and maybe a no consent for those portions of personal health information that are required to be disclosed by law (e.g., information to the CDC for communicable diseases)	
ASSUMPTIONS	❖ This security implementation specification is intended to meet, and has been tested against, all scenarios reviewed by the privacy committee.	

Alternatives	Primary Access Control Category	Source
1 – HIPAA	General Access Control	[45 CFR section 164.308(a)(4)(ii)(B)]
2 – ISO	General Access Control	[ISO/IEC 27002, part 11.2]
3 – HITSP	General Access Control	TN900: HITSP Security and Privacy Technical Note [v 1.1]: 4.5.4
4 – NIST – Securing IT Systems	Authentication / General Security	800-14 - Principles and Practices for Securing IT Systems [9/1996]
5 – NIST – Authentication	Authentication	Draft 800-63 – Electronic Authentication Guideline [2/2008]
6 – NIST – Authorization & Access Management	Authorization & Identity Management	NIST 800-95 Guide to Secure Web Services [9/2007]
7 – ABAC to ZBAC	Authorization	The Evolution of Access Control Models (a US Military Working Paper)
8 – CA OCIO – Federated Identity Management	Authentication & Identity Management	Proposed California Federated Identity Management Standard

Alternatives	HIPAA (1)	ISO (2)	HITSP (3)	NIST (4) Securing IT Systems	NIST (5) Authentication	NIST (6) Authorization and Access Mgmt	ABAC to ZBAC (7)	Federated Identity Management (8)	Proposal
ISSUES									
Description of Standards	<u>1-Description</u> HIPAA: Access Authorization: Implement policies and procedures for authorizing access to protected health information. [45 CFR section 164.308(a)(4)(ii)(B)] Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights [45 CFR 164.312 (a)] Person or entity authentication	<u>2-Description</u> ISO: User Access Management: Ensure authorized user access and prevent unauthorized access to information systems by utilizing a formal user registration and de-registration procedure for granting and revoking access to all information systems and services. [ISO/IEC 27002, part 11.2]	<u>3-Description</u> HITSP: TN900: HITSP Security and Privacy Technical Note [v 1.1]: 4.5.4 Access Control: Access control ensures that people, computer systems, and software applications can use only those resources (e.g., files, directories, computers, networks) that they are authorized to use and then only for approved purposes. Access controls protect against unauthorized use, disclosure, modification, and destruction of resources and unauthorized issuing of system commands. HITSP provides limitations to	<u>4-Description</u> NIST: SP 800-14 - Principles and Practices for Securing IT Systems [9/1996] 3.11.2 Authentication "Authentication is the means of establishing the validity of this claim. There are three means of authenticating a user's identity which can be used alone or in combination: something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual possesses (a token -- e.g., an ATM card or a smart card); and something the	<u>5-Description</u> NIST: Draft 800-63 – Electronic Authentication Guideline [2/2008] This draft document states specific technical requirements for each of the four levels of assurance defined in the OMB E-Authentication Guidance for Federal Agencies, [OMB 04-04] in the following areas: <ul style="list-style-type: none"> • Tokens (typically a cryptographic key or password) for proving identity, • Identity proofing, registration and the 	<u>6-Description</u> NIST 800-95 Guide to Secure Web Services [8/2007] (3.5) – Distributed Authorization and Access Management: The following authorization models are the most relevant to access management in a service-oriented architecture: <ul style="list-style-type: none"> • Role-based access control (RBAC) • Attribute-Based Access Control (ABAC) • Policy-based access control (PBAC) 	<u>7-Description</u> From ABAC to ZBAC: The Evolution of Access Control Models (a US Military Working Paper) AuthoriZation Based Access Control (ZBAC) is a method which addresses problems with RBAC, ABAC, and PBAC. With ZBAC, we choose to authorize based on authentication in the user's domain before the request is made. The request is cryptographically bound to this original domain authorization and this binding is used throughout a transaction's	<u>8-Description</u> California Proposed Federated Identity Management Standard Provides the framework for statewide federated identity management, and is the proposed basis of the CalPSAB authentication implementation strategy. The organization must adopt the Federal Electronic Authentication Guide (NIST 800-63) four levels of authentication assurance and map its security policy to the appropriate level. The provider and consumers of	<u>Proposal-Description</u> Part I: Authentication through a combination of direct, trusted 3rd party, and federated chain of trust relationships. PSAB Security proposes to use the State of California OCIO California Federated Identity Management standard for its authentication model. Trust levels are left to decisions between trading partners and/or further specification in standardized federal or state DURSAs (Data Use and Reciprocal Support Agreements). Part II: Authorization and Access

Alternatives	HIPAA (1)	ISO (2)	HITSP (3)	NIST (4) Securing IT Systems	NIST (5) Authentication	NIST (6) Authorization and Access Mgmt	ABAC to ZBAC (7)	Federated Identity Management (8)	Proposal
ISSUES									
	standard requires entities to implement procedures to verify that a person or entity seeking access to electronic protected health Information is the one claimed. [45 CFR 164.312 (d)]		access including information about the requesting user, type of data, consumer's recorded choice to determine when access is granted. <i>Clarifications</i> <ul style="list-style-type: none"> HITSP extends the nature of access controls into consumer choice and data sensitivity. Chosen Implementation Specification is in line with the HITSP TN900 which sets out the standards to be used for Privacy and Security in the NHIN and demonstration national efforts. 	individual is (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). <i>Clarifications</i> <ul style="list-style-type: none"> NIST Standards are tiered to provide levels of security from minimal to national top secret 	delivery of credentials which bind an identity to a token, <ul style="list-style-type: none"> Remote authentication mechanisms, that is the combination of credentials, tokens and authentication protocols used to establish that a claimant is in fact the subscriber he or she claims to be, Assertion mechanisms used to communicate the results of a remote authentication to other parties. <i>Clarifications</i> <ul style="list-style-type: none"> NIST Standards are tiered to provide levels of security from minimal to national top secret 	<ul style="list-style-type: none"> Risk adaptive access control (RADAC) (using a subject's risk profile) <i>Clarifications</i> <ul style="list-style-type: none"> NIST Standards are tiered to provide levels of security from minimal to national top secret. Consistent with ONC/NHIN demonstration project. 	lifecycle to validate authorization of the transaction. This is also used to establish access privileges at whatever level of granularity is needed with the system.	the identity service must implement a trust agreement defining the trust relationship based on NIST 800-47. <i>Clarifications</i> <ul style="list-style-type: none"> Allows any combination of RBAC, ABAC, PBAC, and ZBAC authorization models 	Control through proposed Authorization Arbitration Implementation Specification conforming to the HIPAA, NIST, ISO, and HITSP standards as discussed above. Authorization Arbitration is an attribute-based process of considering all relevant information that may affect the decision on what "protected" information is provided in response to a data request from an authorized requestor (ABAC). To the extent that these authorization attributes and valuations can be standardized throughout the state, arbitration can be accomplished at the time of user authentication (ZBAC). The process will consider 7 dimensions (attributes) of relevant factors: (1) Data Source; (2) Entity of Requestor; (3) Role of Requestor; (4) Use of Data; (5) Sensitivity of Data; (6) Form of Data (or, how the data is provided); (7) Consent Directives of the Data Subject .
Level of Security Protection	1-Level of Security HIPAA is non-specific – HIPAA only specifies that technical policies and procedures be implemented to protect health information	2-Level of Security ISO is non-specific – ISO says to ensure authorized user access and prevent unauthorized access to information systems	3-Level of Security – HITSP is more framework than standards	4-Level of Security – NIST: SP 800-14 <i>Securing IT Systems</i> is more framework than standards	5-Level of Security <ul style="list-style-type: none"> NIST provides up to four levels of assurance Specific standards, but not specific as to how implemented + Specific on how to set up process to implement standards and set policies	6-Level of Security <ul style="list-style-type: none"> Specific standards, but not specific as to how implemented + Specific on how to set up process to implement standards and set policies	7-Level of Security + Implementation specific authorization and delegation process upfront when authenticating + Supports record level protection + Supports cryptographically bound transfer of trust between participating systems + More resistant to "Man-in-the-Middle" attack and confused deputy attack	8-Level of Security + Supports any level of authentication assurance. + Requires security details to be documented in DURSA (or equivalent) document. + If solution requires encryption beyond SSL/TLS, then it must meet W3C XML Encryption + If proof of sender is required (message integrity), then the solution must meet W3C XML Signature + Supports CalPSAB's authorization arbitration model. + Must meet OASIS WS-Security standard including Secure Token Service	Proposal-Level of Security + Flexible framework to meet any security level requirements. + Supports flexible authorization model to meet any combination of access requirements. + Federates to local domain to set appropriate access levels.

Alternatives	HIPAA (1)	ISO (2)	HITSP (3)	NIST (4) Securing IT Systems	NIST (5) Authentication	NIST (6) Authorization and Access Mgmt	ABAC to ZBAC (7)	Federated Identity Management (8)	Proposal
ISSUES									
Cost	<p>1-Cost</p> <ul style="list-style-type: none"> - HIPAA non-covered entities may incur added cost to implement HIPAA rules + Provider entities are assumed to have HIPAA access controls already in place which would significantly lower implementation and maintenance costs 	<p>2-Cost</p> <ul style="list-style-type: none"> - ISO and HIPAA are nearly identical in their requirement for access controls, and such are assumed to be already in place in provider entities, so only non-covered HIPAA entities may incur added cost to implement ISO rules + Many public entities follow ISO standards, so implementation costs should be minimal 	<p>3-Cost</p> <ul style="list-style-type: none"> - It is expected that all entities exchanging data in CA will require some additional investment in infrastructure services to implement the HITSP specification with initial costs incurred. + Ease of integration and communication should result in long-term savings if adopted nationally. 	<p>4-Cost</p> <ul style="list-style-type: none"> • It could be no additional costs. - It could result in additional costs for implementing access standard beyond the entities current protections. 	<p>5-Cost</p> <ul style="list-style-type: none"> • It could be no additional costs. - It could result in additional costs for implementing access standard beyond the entities current protections. 	<p>6-Cost</p> <ul style="list-style-type: none"> • It could be no additional costs. - It could result in additional costs for implementing access standard beyond the entities current protections. 	<p>7-Cost</p> <ul style="list-style-type: none"> + Assuming federated authorization is adopted, this option will reduce costs due to federated authorization management (because user administration is principally done in local domains) - More attributes = more cost and more values 	<p>8-Cost</p> <ul style="list-style-type: none"> - Associated costs to implement trust agreements. + Consistent with National direction toward DURSA and use ONC DURSA template 	<p>Proposal-Cost</p> <ul style="list-style-type: none"> + Minimizes access controls administration. • Dependent upon standard attributes and vendor implementation
Business Practices (Policy & Procedure)	<p>1-Business Practices</p> <ul style="list-style-type: none"> - Implementing New Policies and Procedures – Poor for HIPAA non-covered entities 	<p>2-Business Practices</p> <ul style="list-style-type: none"> - Implementing New Policies and Procedures – Poor for those entities who have not implemented any ISO standards 	<p>3-Business Practices</p> <ul style="list-style-type: none"> - Implementing New Policies and Procedures – Poor if not adopted nationally + Ease of integration and communication should result if adopted nationally. + HITSP extends the nature of access controls into consumer choice and data sensitivity, and therefore requires an implementation similar to that proposed by CalPSAB 	<p>4-Business Practices</p> <ul style="list-style-type: none"> + Implementing New Policies and Procedures – Fairly Good to the extent that providers and other entities already implement access standards guided by the NIST framework, integration would likely not be too much of an issue 	<p>5-Business Practices</p> <ul style="list-style-type: none"> + Implementing New Policies and Procedures – Fairly Good to the extent that providers and other entities already implement access standards guided by the NIST framework, integration would likely not be too much of an issue 	<p>6-Business Practices</p> <ul style="list-style-type: none"> + Implementing New Policies and Procedures – Fairly Good to the extent that providers and other entities already implement access standards guided by the NIST framework, integration would likely not be too much of an issue 	<p>7-Business Practices</p> <ul style="list-style-type: none"> + Implementing New Policies and Procedures – Provider business processes would likely improve using ZBAC as it provides the ability to authorize based on authentication within the user's own domain + Authorization and delegation vectors allow precise control of privileges. + Repudiation and revocation checking on the user can be performed locally + Policy can be cryptographically bound to the transaction 	<p>8-Business Practices</p> <ul style="list-style-type: none"> + Improved communication using detailed trust agreements + If the Federal DURSA can be adapted for use in CA and is comprehensive enough to include authorization models, it could simplify a statewide rollout and be adapted to both small and large HIEs. + Third-party identity service provider credentials must be created in strict accordance with the trust agreement 	<p>Proposal-Business Practices</p> <ul style="list-style-type: none"> + Standardizes credential format and exchange policies. + Allows organizations of all sizes to securely exchange health information + Authorization and delegation vectors allow precise control of privileges. + Repudiation and revocation checking on the user can be performed locally
Technology	<p>1-Technology</p> <ul style="list-style-type: none"> + Good if HIPAA access controls are assumed to already be in place in provider and public entities - Poor for non-covered private entities in that they would incur added technical complexity to implement HIPAA rules. 	<p>2-Technology</p> <ul style="list-style-type: none"> + ISO and HIPAA are nearly identical in their requirement for access controls, and such are assumed to be already in place in provider and public entities - Poor for non-covered HIPAA private entities in that they would incur added technical complexity to implement ISO standards. 	<p>3-Technology</p> <ul style="list-style-type: none"> + If adopted nationally, this alternative would enhance technical compatibility and integration. - Technical complexity would be a problem if this option is not adopted nationally 	<p>4-Technology</p> <ul style="list-style-type: none"> + To the extent that providers and other entities already implement access standards guided by the NIST framework, technology would be fairly compatible and integration would likely not be too much of an issue 	<p>5-Technology</p> <ul style="list-style-type: none"> + To the extent that providers and other entities already implement access standards guided by the NIST framework, technology would be fairly compatible and integration would likely not be too much of an issue 	<p>6-Technology</p> <ul style="list-style-type: none"> + To the extent that providers and other entities already implement access standards guided by the NIST framework, technology would be fairly compatible and integration would likely not be too much of an issue 	<p>7-Technology</p> <p>ZBAC uses a complimentary approach:</p> <ul style="list-style-type: none"> + Can adapt sites using Name-Based Access Control (NBAC) + All user administration is in the local domain + Allows local identity verification/authentication systems to be used intact if allowed by remote domain restrictions + Enhances capability of implementation of SSO across orgs + Creates a rights inheritance model that can be used by some systems to automate rights management within the local domain for controlling access to remote systems 	<p>8-Technology</p> <ul style="list-style-type: none"> + Meets OASIS and W3C security standards. + Platform and vendor neutral + Facilitates standardization of authorization attributes across organizations 	<p>Proposal-Technology</p> <ul style="list-style-type: none"> + Meets OASIS and W3C standards. + Platform and vendor neutral + Facilitates standardization of authorization attributes across organizations + All user administration is in the local domain + Creates a rights inheritance model

Alternatives	HIPAA (1)	ISO (2)	HITSP (3)	NIST (4) Securing IT Systems	NIST (5) Authentication	NIST (6) Authorization and Access Mgmt	ABAC to ZBAC (7)	Federated Identity Management (8)	Proposal
ISSUES									
National Efforts (Compatibility)	1-Compatibility + Since HIPAA is already implemented nationally, it would increase compatibility	2-Compatibility – Decreased compatibility for entities who have not implemented ISO formal user registration and deregistration procedure	3-Compatibility – If adopted nationally, this alternative would enhance compatibility	4-Compatibility + NIST is widely implemented by many entities and would generally increase compatibility	5-Compatibility + NIST is widely implemented by many entities and would generally increase compatibility	6-Compatibility + NIST is widely implemented by many entities and would generally increase compatibility	7-Compatibility + Compatibility would be good since ZBAC sits on top of administrative systems and is built to interface with local environments + Consistent with HITSP TN900 authorization recommendations.	8-Compatibility + Compatible with NIST, NHIN, HISPC and HITSP + Consistent with CalPSAB Privacy Committee use cases.	Proposal-Compatibility + Compatible with NIST, NHIN, HISPC and HITSP + Consistent with HITSP TN900 authorization + Consistent with CalPSAB Privacy Committee use cases.
CalPSAB Principles	1-Principles + Consistent with health information quality – Inconsistent with openness, individual participation, security safeguards, accountability, and collection, use and purpose limitation	2-Principles + Consistent with, health information quality, security safeguards and accountability – Inconsistent with openness, individual participation, collection limitation, use limitation, purpose limitation,	3-Principles + Consistent with health information quality, accountability and individual participation – Inconsistent with security safeguards, openness, and collection, use and purpose limitation	4-Principles + Consistent with health information quality, accountability, security safeguards, and collection, use and purpose limitation – Inconsistent with openness and individual participation	5-Principles + Consistent with health information quality, accountability, security safeguards, and collection, use and purpose limitation – Inconsistent with openness and individual participation	6-Principles + Consistent with health information quality, accountability, security safeguards, and collection, use and purpose limitation – Inconsistent with openness and individual participation	7-Principles + Consistent with all CalPSAB principles	8-Principles – Consistent with health information quality, security safeguards and accountability – Inconsistent with openness, individual participation, Collection, use and purpose limitation	Principles + Consistent with all CalPSAB principles