OpenHIE Privacy and Security

To help navigate the current and future thinking of OpenHIE Privacy and Security

Preamble

Privacy and security are two related, but quite distinct, topics. In its 2016 document, **Connecting Health and Care for the Nation – A Shared Nationwide Interoperability Roadmap**, the US department of Health and Human Services (HHS) states that:

> *Participation in and use of a learning health system will be highly dependent upon reliable mechanisms to ensure that (1) a secure network infrastructure is widely available; (2) privacy is protected; (3) health information and services are accessed only by participants whose identity has been verified and who have been authenticated to access the system they are seeking to access; (4) users have access only to data they are authorized to access, where authorization is determined by individuals' choices, or, if no choices are recorded, what the statutes, regulations and consensus rules say a user may access, use, disclose and receive. All of these components are necessary for enabling broad scale interoperability and a learning health system.*

In many low-resource settings the legislative and policy protections for personal health information (PHI) privacy and security are still in the process of being developed and enacted. Even so, it is an underlying principle of the OpenHIE initiative that privacy, security and confidentiality of PHI are important requirements and that, at a minimum, internationally accepted de facto baseline protections should be supported. It is expected that, as implementing jurisdictions' PHI policies mature, expanded protections may be operationalized in the OpenHIE infrastructure to augment the initial, basic capabilities.

OHIE Privacy and Security Framework

To help implementers think about the multiple dimensions of security, OpenHIE has the following framework. Each quadrant represents a different aspect that needs to be considered when implementing OpenHIE.

Unknown macro: 'gliffy'

OpenHIE Security and Privacy Policy Considerations

Unknown macro: 'gliffy'

The following types items should be considered when determining the security and privacy policies for HIE exchanges and the HIE:

- Use cases being supported or planned to be supported by the HIE.
- The types of data exchanged with and stored in the HIE. Is personal health data or other sensitive data such as financial data being managed or exchanged?
- Country, regional and local laws and cultural practices and expectations need to be considered.

Policies can range from data exchange and use agreements to policies for management of physical and logical access to HIE servers and data.

Security and Privacy Policy Resources

The following is a list that can be added or update to include resources and examples from various implementations.

Resource	Description
Data Use and Reciprocal Support Agreement (DURSA)	A draft Data Use and Reciprocal Support Agreement (DURSA) example developed by: NHIN Cooperative DURSA Workgroup January 23, 2009. These types of agreements are used to support exchange between one or more HIEs or an HIE and a point-of-care or point-of-service application.
Sequoia Project Data Use and Reciprocal Support Agreement (DURSA)	Definitions of DURSA, Links to current and previous versions from the Sequoia project, a webinar and additional materials.
DURSA Policy Assumptions	An example of a framework for broad-based information exchange among a set of trusted entities who either wish to query and retrieve data or push data to others in the network.
Data Use Agreement Practices Guide	Background on a data use agreement

OpenHIE Data Sharing Agreement Roadmap for Health Worker Data	As of 9-Nov-2016, this document is being developed to help implementers think through the data sharing aspects of the Health Worker Registry.

OpenHIE Security Technology Assessment

OpenHIE has done an assessment of the security technology that is provided in the current OpenHIE reference solutions. Assessment as of June 2016.

Unknown macro: 'gliffy'

Basic Security - Technical capabilities	OHIE Security - Level 1	OHIE Security - Level 2	OHIE Security - Level 3
Encryption in transit between entities	System Level - OpenHIE can be configured to support encrypted transactions between HIE and external system(s).	HIE System Component level - OpenHIE can be configured to support encrypted transactions inside the HIE.	
Security in processing / storage	HIE System Component Level - Option OHIE Architecture components have the option to require authentication to access data	HIE Component Level OHIE Architecture components require authentication to access data	
Authentication / Identity assertion level	System Level - HIE and the external system are authenticated at the “device” level.	HIE System Component level - HIE components are mutually authenticated at the device level	User Level - External systems are able to assert user identity, location and purpose of use to the HIM
Audit Record Points	HIE Component Level Audits for PHI transactions Mirrored audits are collected between the HIM and infrastructure services whenever PHI is conveyed.	HIE Component Level Audits for all transactions Mirrored audits are collected between the HIM and infrastructure services whenever PHI is conveyed.	Mirrored audits between all parties POS systems are able to send relevant audits to central audit-repository
Audit Records Content	Basic content Transactions between the HIE and an external system are tracked.	Audit contents contain subject field Audits contain the X.509 Subject field of the requesting party	Detailed Audit Contents Audit contents All audits contain the asserted user identity, location and purpose of use.

Key - OHIE Reference Architecture Status
Supported - All OpenHIE Reference Technologies can be configured to support this capability
Some support - One or more OpenHIE components can be configured to support this capability
Not supported / Not yet supported in reference implementations

OpenHIE Security Workflows

OpenHIE does support specific IHE security profiles. Common message security workflow

OpenHIE's Security Behaviour

As of OpenHIE v2 release, the basic privacy & security behaviour of the reference architecture may be described as follows:

- **OpenHIE never talks to strangers**. All participating nodes in the health information exchange are mutually authenticated using PKI. (Ref. IHE's ATNA profile)
- **OpenHIE operationalizes a *trusted* network.** It is expected that point of service (POS) applications authenticate and authorize *individual* system users. If a user is authorized by the POS, it is trusted by OpenHIE.
- **Traffic on the exchange is secured**. The 2-sided PKI is leveraged to establish secure, encrypted (HTTPS) packet exchange between nodes (Ref. IHE's ATNA profile)
- **Personal health information access is traceable.** OpenHIE keeps an audit log, at the *authenti cated node* level, of PHI exchanged over the network. (Ref. IHE's ATNA profile)
- **By default, PHI will be shared for *health care delivery* purposes.** OpenHIE's out-of-the-box configuration supports the exchange of **all** PHI with **all** members of a care delivery network to support a client's **continuity of care**. This is commonly known as an "opt-out" consent model. By default, PHI will be shared; it is up to an individual to explicitly *withdraw* their consent and indicate that they do NOT want their health information shared.
- **An individual may withdraw their consent to disclose their PHI.** As of OpenHIE v2, a client registry flag is supported that indicates whether the client's PHI will be shared. If this flag indicates consent has been withdrawn, then OpenHIE's interoperability layer will not return shared health record content to POS applications that request this client's PHI. NOTE: there is no way for a POS to override the client's consent directive (e.g. there is no "break the glass"

capability). Importantly, although a client may withdraw their consent to **disclose**, they may not opt out of having their health information **collected** and saved to the HIE. Such data is crucial to population/public health, system management, and disease surveillance workflows.

Although it is possible for OpenHIE to be set up to operate under an "opt-in" consent model, such an HIE configuration has proven in practice to be very expensive and difficult to administer; implementations have been generally been unsuccessful. As such, the opt-in configuration is not recommended.

Underlying Privacy & Security Standards

OpenHIE is committed to the operationalization of pervasive, interoperable health information exchange networks based on international standards. The following lists the digital health standards that underlie OpenHIE's *basic* privacy and security behaviour (indicated with *) and those which may be employed to extend/expand the HIE's privacy and security architecture (PSA) over time.

- *IHE ATNA – the Audit Trail and Node Authentication profile defines how message audit logs will be maintained and how network nodes will establish 2-sided mutual authentication.
- *ISO 14265 – ISO's "Classification of purposes for processing personal health information" specification identifies a code system for purposes of data use; this code system may be employed to establish different authorities for different network sharing purposes. OpenHIE operates on the premise that its core purpose of use is care delivery.
- *IHE PDQ – the Patient Demographic Query profile describes the client registry content that is to be returned in response to a query. The PDQ ITI-21 transaction is employed by OpenHIE's Interoperability Layer to return the client's consent flag. OpenHIE uses this flag to determine if the requested content will be returned, or not returned (throwing an exception).
- IHE XUA – the Cross-enterprise User Assertion profile would enable a point of service application to explicitly share with the HIE the identity of the application's logged-in user. With such information, the audit trail (see ATNA, above) could include a more precise record indicating which user has retrieved PHI; today, the audit trail indicates which authenticated node has accessed PHI and it would be up to the POS applications audit trail to indicate which user made the query. For successful implementation, POS applications must support XUA-based user assertion at the time content is posted to or queried from the HIE.
- IHE IUA – the Internet User Authorization profile defines how SAML or OAuth tokens may be employed to authorize individual user access to RESTful web resources. With the implementation of appropriate shared authentication services, IUA could be leveraged to explicitly establish trusted access to the HIE at the *individual* level.
- IHE BPPC – the Basic Patient Privacy Consents profile describes how a client's consent directive documents may be managed by the HIE and how these consents may be applied to govern queries for specific clinical documents in the shared health record. BPPC supports consent management by facility, by health worker, and for purposes of use beyond care delivery. It relies on XUA or IUA and on the "confidentiality code" being specified by the POS at the time the clinical content is first posted to the HIE.
- IHE APPC – the Advanced Patient Privacy Consents profile extends BPPC to support more precise, policy-based (rule-based) access controls to be applied to the sharing of clinical content, including to subsections within a clinical document. In addition to the implementation requirements for BPPC, APPC leverages the XML Access Control Markup Language (XACML) to define a rich, precisely articulated, policy-based access control regime. NOTE: the APPC profile is a new profile presently in its public comment phase.