Security and Privacy Swim Lane

Interoperability through trusted exchange using secure, standards-based, and privacy-preserving technologies.

# Baseline capabilities

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Baseline |  |
| Short Narrative Description | Services and capabilities assumed at the beginning | Includes:* Identity: establish means to classify discrete users.
* Authentication: Verifying users are who they say they are.
* Authorization: Confirm users are supposed to have access to the resources requested
* Audit: Record user access to resources and for what purposes.
* Confidentiality: Prevent unauthorized access to information.
* Integrity: guard against unauthorized modification of healthcare information
 |
| Milestone Type | Best Practice |  |
| Rationale | Baseline services necessary prior to the implementation of new and improved capabilities |  It is necessary to baseline where we are in order to measure progress for a goal. |
| Phase I? | Yes |  |
| Phase 2? | No |  |
| Phase 3? | No |  |
| Phase 4? | No |  |
| Dependencies | Establish state of each of listed baseline services. |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Secure Interoperability

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | **Secure Interoperability** |  |
| Short Narrative Description | Automated cross-enterprise trust, consent, authorization, and privacy-preserving access at runtime. | Common interoperable semantic value sets for cross-enterprise security and privacy. Runtime negotiation for context-sensitive exchange. |
| Milestone Type | Software Deliverable Best Practice |  |
| Rationale | Final goal  |  |
| Phase I? | No |  |
| Phase 2? | No |  |
| Phase 3? | No |  |
| Phase 4? | Yes  |  |
| Dependencies | Success dependent upon implementation of other milestones. |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Share with Protection

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Share with Protection  |  |
| Short Narrative Description | Security and Privacy protections are carried with the content.  | All information returned in request. Specific data masked by purpose of use or clearance. All information available to trusted CDS to ensure patient safety. |
| Milestone Type | Best Practice | Avoids practice of redacting data. All information backed by policy-based granular protections based on role and clearance. Ensures that needed information is available to ER without exception. |
| Rationale | Key Milestone |  |
| Phase I? | No |  |
| Phase 2? | No |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies | Assumes ability to classify content (including unstructured data) according to sensitivity.  |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Attribute-based Access Control

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | ABAC.  | Classifying data sensitivity provides basis for access control based upon need. Provides capability to provide security for FHIR resources, medical devices and IoT. Modernizes and transforms the way security and privacy is managed and enforced. |
| Short Narrative Description | Manage access control at a granular level. Facilitates managing emerging technologies such as FHIR. |  |
| Milestone Type | Best Practice |  |
| Rationale | Key trend in access control. Ideal approach to IoT. | According to Gartner, 70% of organizations will employ ABAC by 2020. ABAC has emerged within NIST as providing policy-based enforcement rules. |
| Phase I? |  |  |
| Phase 2? |  |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies | Assumes ability to establish and enforce policy including provisioning of clinical staff by assigned duties or workflow. |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Data Segmentation

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Data Segmentation/Security Labeling Service.  | Technical mechanism for analyzing structured and unstructured data and applying labels according to flexible security and privacy rules. |
| Short Narrative Description | Identify, mark, and segment healthcare information at an appropriate granular level of functionality according to organizational and patient policy/rules. | Core HL7 standards have been in place since 2014. HL7 content has been created “label” ready. See:* HL7 Privacy and Security Healthcare Classification System (HCS),
* HL7 Privacy and Security Services: Security Labeling Service
 |
| Milestone Type | Software DeliverableContent DeliverableBest Practice | Security labeling is well understood, however, implementation in healthcare requires construction of detailed rules requiring high confidence of proper operation. |
| Rationale | Key capability |  |
| Phase I? | Yes |  |
| Phase 2? | Yes |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies | HL7 Label vocabulary, Availability of mature security labeling services.  |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Patient Choice/Consent

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Patient Choice /Consent  | This milestone merges concepts of electronic patient consent, and choice (individual control of their own information as provided by law). This typically involves “authorizations” (approvals and/or directions to share and “restrictions” (patient policy restricting access to certain information to authorized persons organizations.). It also includes “Directions” to healthcare organizations to transmit a copy of their own information to destinations of their choice under patient right of access law. |
| Short Narrative Description | Electronic patient permissions regarding disclosure of their own protected health information. | Eliminates a burden on providers to maintain paper records. Allows automated management of patient privacy preferences. |
| Milestone Type | DocumentSoftware DeliverableBest Practice | Technical implementation using patient managed OAuth Authorization Server demonstrated during HIMSS 2017. See milestone “Secure Delegated Access”. |
| Rationale | Key milestone |  |
| Phase I? | Yes |  |
| Phase 2? | Yes |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies | Electronic Consents, Secure Delegated Access, Security Labeling Service, ABAC |  Paper based consents are not computable and represent a significant management burden. Implementing electronic consents ensures electronic workflows are not broken. Electronic consents provide the “policy” for Secure Delegated Access engines. |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Provenance

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Provenance  | Ensures the integrity of data from origin to destruction. |
| Short Narrative Description | Determine the origin and history of healthcare information | Integrity is one of the most desirable characteristics of a trustworthy health record. |
| Milestone Type | Content Deliverable |  |
| Rationale | Key capability |  |
| Phase I? | No |  |
| Phase 2? | No |  |
| Phase 3? | No will |  |
| Phase 4? | Yes |  |
| Dependencies | Availability of suitable technology  |  Blockchain ledger has been proposed, however, concerns remain regarding overhead impacts. |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Transparent Security

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Transparent security.  | Security remains in background, unobtrusive. Goal is to eliminate security as an impediment to clinical workflow. |
| Short Narrative Description | Provide appropriate safeguards to healthcare information while minimizing impact to clinical workflow or information availability. |  |
| Milestone Type | Best Practice, Implementation Guides |  |
| Rationale | Crosscutting policy |  |
| Phase I? | No  |  |
| Phase 2? | No |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes  |  |
| Dependencies | ABAC, workflow enhancements. |  HL7 Implementation Guides may lag need. |

 **EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

# Secure Delegated Access

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Secure Delegated Access | Mechanism for implementing patient control  |
| Short Narrative Description | Provides patients with ability to express their choices for disclosure of protected health information. | Intent is to implement OAuth and patient owned Authorization Server. See ONC HIMSS 2017 Patient Choice demonstration.Secure Delegation Access is part of HL7’s approved international standard for Privacy and Security services: Access Control |
| Milestone Type | Content DeliverableBest Practice |  |
| Rationale | Key capability |  |
| Phase I? | No |  |
| Phase 2? | No |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies |  |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

Opt-In

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | Opt-In  |  |
| Short Narrative Description | Healthcare information is shared by default. Patients may opt-out or use restrictions to control disclosure of protected health information. | The opt-in model represents an approach most beneficial to the majority of patients. Patients that do not wish to share protected health information have the option of opting-out or requesting restrictions on disclosures. This approach provides the most economical mechanism for healthcare organizations while providing patients choice in how they wish their information to be disclosed. Legislation has been proposed to Congress in support of this initiative. |
| Milestone Type | Best Practice |  |
| Rationale | Provides a significant benefit to providers when dealing with protected health information. |  |
| Phase I? | No |  |
| Phase 2? | Yes |  |
| Phase 3? | Yes |  |
| Phase 4? | Yes |  |
| Dependencies | Congressional action. |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | The label for the milestone as appearing on the T-Map.  | The expectation is that all “significant” milestones on the Transition Map are included in the narrative. It is okay if some milestones are not included, and similarly there may be additional milestones in the narrative section that do not appear on the T-Map. |
| Short Narrative Description | Roughly a sentence describing what the milestone is | Provide just enough definition so that the “lay” reader understands what the milestone is.  |
| Milestone Type | Will ultimately be an enumerated list. Initial values include: DocumentSoftware DeliverableContent DeliverableBest PracticeAchievement Date (for example, an event trigger) | Revise/extend the list as necessary. We will harmonize in subsequent phases |
| Rationale | Short description of why the milestone was included on the community roadmap |   |
| Phase I? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 2? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 3? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 4? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Dependencies | Enumerated list of dependencies (activities or other milestones) |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | The label for the milestone as appearing on the T-Map.  | The expectation is that all “significant” milestones on the Transition Map are included in the narrative. It is okay if some milestones are not included, and similarly there may be additional milestones in the narrative section that do not appear on the T-Map. |
| Short Narrative Description | Roughly a sentence describing what the milestone is | Provide just enough definition so that the “lay” reader understands what the milestone is.  |
| Milestone Type | Will ultimately be an enumerated list. Initial values include: DocumentSoftware DeliverableContent DeliverableBest PracticeAchievement Date (for example, an event trigger) | Revise/extend the list as necessary. We will harmonize in subsequent phases |
| Rationale | Short description of why the milestone was included on the community roadmap |   |
| Phase I? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 2? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 3? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 4? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Dependencies | Enumerated list of dependencies (activities or other milestones) |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |

|  |  |  |
| --- | --- | --- |
| Metadata Item | Guidance | Notes |
| Milestone Name | The label for the milestone as appearing on the T-Map.  | The expectation is that all “significant” milestones on the Transition Map are included in the narrative. It is okay if some milestones are not included, and similarly there may be additional milestones in the narrative section that do not appear on the T-Map. |
| Short Narrative Description | Roughly a sentence describing what the milestone is | Provide just enough definition so that the “lay” reader understands what the milestone is.  |
| Milestone Type | Will ultimately be an enumerated list. Initial values include: DocumentSoftware DeliverableContent DeliverableBest PracticeAchievement Date (for example, an event trigger) | Revise/extend the list as necessary. We will harmonize in subsequent phases |
| Rationale | Short description of why the milestone was included on the community roadmap |   |
| Phase I? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 2? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 3? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Phase 4? | Yes/No indicating applicability of the milestone to this phase | Note that milestones may be unique to one phase, or recurring across multiple phases (such as iterative enhancements of an artifact/product) |
| Dependencies | Enumerated list of dependencies (activities or other milestones) |   |

**EXTENDED SET METADATA**

We would love to have this, but consider it a “nice to have” based upon the needs of your segment/swimlane

|  |  |  |
| --- | --- | --- |
| **Metadata Item** | **Guidance** | **Notes** |
| Risks | Documentation of risks associated with the designated milestone |   |
| Project Category |   |   |
| Project Hooks | Indicate project-level relationships associated with this milestone |   |
| Initiative Hooks | Indicate initiative-level relationships associated with this milestone. |   |