

Share with Protections Project Scope Statement

[PSS Help and FAQs](#)
[Comments](#)

1a. Project Name	Share with Protections White Paper
1b. Project ID	1566
1c. Is Your Project an Investigative Project (aka PSS-Lite)?	No
1d. Is your Project Artifact being Reaffirmed or proceeding to Normative directly after being either Informative or STU?	No
1e. Today's Date	
1f. Name of standard being reaffirmed	
1g. Project Artifact Information	
1h. ISO/IEC Standard to Adopt	
1i. Does the standard include excerpted text from one or more ISO, IEC or ISO/IEC standards, but is not an identical or modified adoption?	
1j. Unit of Measure	
2a. Primary/Sponsor WG	Security
2d. Project Facilitator	Mike Davis
2e. Other Interested Parties (and roles)	
2f. Modeling Facilitator	Mohammad Jafari
2g. Publishing Facilitator	Mike Davis
2h. Vocabulary Facilitator	Kathleen Connor
2i. Domain Expert Representative	Mike Davis, Mohammad Jafari (CA), Alex Mense (AU)
2j. Business Requirements Analyst	Kathleen Connor
2k. Conformance Facilitator	
2l. Other Facilitators	

2m. Implementers	VA Others TBD
3a. Project Scope	<p>Share with Protection PPS</p> <p>The “Share with Protections” paper will describe business requirements and technical solutions for a new approach to enabling accessibility and liquidity of health information governed by privacy, security, provenance and trust policies. Healthcare business may require the ability of health information exchange partners to convey computable policies to which they must comply by means of interoperable Security Label metadata on shared information, and for real-time negotiations of the means by which Receivers will consume and persist Security Labels so as to enforce the access control requirements of the conveyed policies.</p> <p>Share with Protections (SwP) extends the concepts of Data Segmentation for Privacy (DS4P) by providing standards-based technology supporting enhanced data sharing, and enabling Receivers to manage local policy-aware workforce access, use, and further by their staff. SwP may enable policy domains to move from explicit patient consent to implicit patient consent, which could ease the burden on patients and their information custodian to enable information exchange.</p> <p>Given the increasingly ubiquitous network of health information exchange and the likewise increasing need to share more easily without information blocking , SwP offers a framework for trusted negotiation between Senders, who are accountable for downstream adherence to the policies that govern their sharing, with Receivers which may not be members of the same policy domain, at run time without resorting to out-of-band static contract methods such as MOUs and DURSA.</p> <p>This paper will describe SwP business requirements, use cases, supporting work flows. It will provide technical solutions, at a conceptual level, that leverage current HL7 Security Labeling standards in HL7 Version 2.9 ARV segment, CDA DS4P Implementation Guide (IG), and FHIR R5 Security Label Module, all of which are based on the HL7 Healthcare Privacy and Security Classification System (HCS).</p> <p>In addition, it will reference capabilities described in the HL7 Security Labeling, Privacy Preserving, Access Control, and Audit Service specifications; the Trust Framework for Federated Authorization Conceptual and Behavioral Models; and the Provenance Domain Analysis Model. Finally, it will reference Sender and Receiver capabilities outlined in the FHIR DS4P IG, which is in ballot, and the Cross-Paradigm US Security Labeling IG, which is in development.</p> <p>Technical Requirements and Solutions to be described include:</p> <ul style="list-style-type: none"> Generating Security Labels per policy Assigning Security Labels using a Security Labeling Service Consuming Security Labels sent on information being integrated into a system Persisting and managing Security Labels Enforcing Security Labels using End User Provisioning, and Access Control and Privacy Protective Services Advertising and discovering Security Label CapabilityStatements Negotiating Sender and Receiver CapabilityStatement using Trust Contracts Reassigning Security Labels when disclosing information previously labeled by another entity. Reclassifying Security Labels per policy, Displaying to end users Security Labels per policy, Retrieving related artifacts associated with a Security Label tag, e.g., the consent directive instance associated with a Security Label policy tag, or a provenance record instance associated with a Security Label provenance tag.
Attachments	<p>Share with Protections with Citations 2020 0210.pptx</p> <p>DS4P_Share with Protections 2020 0220 V2.2.pdf</p>
3b. Project Need	<p>To support (1) the goals of international jurisdictions participants in those jurisdictions' healthcare exchange to share health information in accordance with governing privacy policies; and (2) the goals of the 21st Century Cures Act, participants in US healthcare exchange will be required to share health information in accordance with governing privacy policies. Requirements to meet these laws are addressed in the latest version of the Trusted Exchange Framework and Common Agreement proposal.</p>
3c. Security Risk	No
3d. External Drivers	<p>International health information exchange privacy and security policy requirements. Federal law: 21st Century Cures Act, 32 CFR Part 2002, 42 CFR Part 2, and Title 38 Section 7332 as well as draft Trusted Exchange Framework and Common Agreement (TEFCA).</p>

3e. Objectives/Deliverables and Target Dates	<p>May through July 2020 - Refine current SwP material. Add technical requirements and solutions listed in 3a Project Scope above.</p> <p>September 2020 - Ballot SwP white paper as informative.</p> <p>October 2020 - Complete ballot reconciliation.</p> <p>November 2020 - Complete revisions per reconciliation and add/enhance material within project scope.</p> <p>December 2020 - Submit for Jan Ballot cycle.</p> <p>February 2021 - Complete ballot reconciliation.</p> <p>March 2021 - Decide whether ready to request publication or rebalot.</p>
3f. Common Names / Keywords / Aliases:	SwP
3g. Lineage	
3h. Project Dependencies	None
3i. HL7-Managed Project Document Repository URL:	Share with Protections White Paper Project https://confluence.hl7.org/display/SEC/Share+with+Protections+White+Paper+Project
3j. Backwards Compatibility	Yes
3k. Additional Backwards Compatibility Information (if applicable)	Compatible with HL7 V2.9 ARV segment, CDA DS4P IG, FHIR DS4P IG, and Cross-Paradigm US Regulatory Security Labeling IG
3l. Using Current V3 Data Types?	N/A
3l. Reason for not using current V3 data types?	
3m. External Vocabularies	No
3n. List of Vocabularies	
3o. Earliest prior release and/or version to which the compatibility applies	No previous SwP white paper version.
4a. Products	White Paper
4b. For FHIR IGs and FHIR Profiles, what product version(s) will the profiles apply to?	
4c. FHIR Profiles Version	
4d. Please define your New Product Definition	
4d. Please define your New Product Family	
5a. Project Intent	White Paper
5a. White Paper Type	Balloted Informative
5a. Is the project adopting/endorsing an externally developed IG?	
5a. Externally developed IG is to be (select one)	
5a. Specify external organization	

5a. Revising Current Standard Info	
5b. Project Ballot Type	Informative
5c. Additional Ballot Info	
5d. Joint Copyright	No
5e. I understand I must submit a Joint Copyright Letter of Agreement to the TSC in order for the PSS to receive TSC approval.	no
6a. External Project Collaboration	
6b. Content Already Developed	50%
6c. Content externally developed?	No
6d. List Developers of Externally Developed Content	
6e. Is this a hosted (externally funded) project?	No
6f. Stakeholders	Clinical and Public Health Laboratories, Immunization Registries, Quality Reporting Agencies , Regulatory Agency, Standards Development Organizations (SDOs), Payors, Other
6f. Other Stakeholders	Providers, healthcare consumers, Payors, HIEs.
6g. Vendors	Pharmaceutical, EHR, PHR, Health Care IT, Clinical Decision Support Systems, Lab, HIS
6g. Other Vendors	
6h. Providers	Clinical and Public Health Laboratories, Emergency Services, Local and State Departments of Health, Medical Imaging Service, Healthcare Institutions (hospitals, long term care, home care, mental health), Other
6h. Other Providers	Care in the Community Providers providing long term services and support.
6i. Realm	Universal
7d. US Realm Approval Date	
7a. Management Group(s) to Review PSS	
7b. Sponsoring WG Approval Date	Apr 07, 2020
7c. Co-Sponsor Approval Date	
7c. Co-Sponsor 2 Approval Date	
7c. Co-Sponsor 3 Approval Date	
7c. Co-Sponsor 4 Approval Date	
7c. Co-Sponsor 5 Approval Date	
7c. Co-Sponsor 6 Approval Date	

7c. Co-Sponsor 7 Approval Date	
7c. Co-Sponsor 8 Approval Date	
7c. Co-Sponsor 9 Approval Date	
7c. Co-Sponsor 10 Approval Date	
7e. CDA MG Approval Date	
7f. FMG Approval Date	
7g. V2 MG Approval Date	
7h. Architecture Review Board Approval Date	
7i. Steering Division Approval Date	Apr 20, 2020
7j. TSC Approval Date	May 18, 2020

Version	4
Modifier	Anne Wizauer
Modify Date	May 19, 2020 19:43
1a. Project Name	Share with Protections White Paper
1b. Project ID	1566
1c. Is Your Project an Investigative Project (aka PSS-Lite)?	No
1d. Is your Project Artifact now proceeding to Normative directly or after being either Informative or STU?	No
2a. Primary/Sponsor WG	Service Oriented Architecture
2d. Project Facilitator	Mike Davis
2f. Modeling Facilitator	Mohammad Jafari
2g. Publishing Facilitator	Mike Davis
2h. Vocabulary Facilitator	Kathleen Connor
2i. Domain Expert Representative	Mike Davis, Mohammad Jafari (CA), Alex Mense (AU)
2j. Business Requirements Analyst	Kathleen Connor
2m. Implementers	VA Others TBD

<p>3a. Project Scope</p>	<p>Share with Protection PPS The “Share with Protections” paper will describe business requirements and technical solutions for a new approach to enabling accessibility and liquidity of health information governed by privacy, security, provenance and trust policies. Healthcare business may require the ability of health information exchange partners to convey computable policies to which they must comply by means of interoperable Security Label metadata on shared information, and for real-time negotiations of the means by which Receivers will consume and persist Security Labels so as to enforce the access control requirements of the conveyed policies.</p> <p>Share with Protections (SwP) extends the concepts of Data Segmentation for Privacy (DS4P) by providing standards-based technology supporting enhanced data sharing, and enabling Receivers to manage local policy-aware workforce access, use, and further by their staff. SwP may enable policy domains to move from explicit patient consent to implicit patient consent, which could ease the burden on patients and their information custodian to enable information exchange.</p> <p>Given the increasingly ubiquitous network of health information exchange and the likewise increasing need to share more easily without information blocking , SwP offers a framework for trusted negotiation between Senders, who are accountable for downstream adherence to the policies that govern their sharing, with Receivers which may not be members of the same policy domain, at run time without resorting to out-of-band static contract methods such as MOUs and DURSA.</p> <p>This paper will describe SwP business requirements, use cases, supporting work flows. It will provide technical solutions, at a conceptual level, that leverage current HL7 Security Labeling standards in HL7 Version 2.9 ARV segment, CDA DS4P Implementation Guide (IG), and FHIR R5 Security Label Module, all of which are based on the HL7 Healthcare Privacy and Security Classification System (HCS).</p> <p>In addition, it will reference capabilities described in the HL7 Security Labeling, Privacy Preserving, Access Control, and Audit Service specifications; the Trust Framework for Federated Authorization Conceptual and Behavioral Models; and the Provenance Domain Analysis Model. Finally, it will reference Sender and Receiver capabilities outlined in the FHIR DS4P IG, which is in ballot, and the Cross-Paradigm US Security Labeling IG, which is in development.</p> <p>Technical Requirements and Solutions to be described include: Generating Security Labels per policy Assigning Security Labels using a Security Labeling Service Consuming Security Labels sent on information being integrated into a system Persisting and managing Security Labels Enforcing Security Labels using End User Provisioning, and Access Control and Privacy Protective Services Advertising and discovering Security Label CapabilityStatements Negotiating Sender and Receiver CapabilityStatement using Trust Contracts Reassigning Security Labels when disclosing information previously labeled by another entity. Reclassifying Security Labels per policy, Displaying to end users Security Labels per policy, Retrieving related artifacts associated with a Security Label tag, e.g., the consent directive instance associated with a Security Label policy tag, or a provenance record instance associated with a Security Label provenance tag.</p>
<p>Attachments</p>	<p>Share with Protections with Citations 2020 0210.pptx DS4P_Share with Protections 2020 0220 V2.2.pdf</p>
<p>3b. Project Need</p>	<p>To support (1) the goals of international jurisdictions participants in those jurisdictions' healthcare exchange to share health information in accordance with governing privacy policies; and (2) the goals of the 21st Century Cures Act, participants in US healthcare exchange will be required to share health information in accordance with governing privacy policies. Requirements to meet these laws are addressed in the latest version of the Trusted Exchange Framework and Common Agreement proposal.</p>
<p>3c. Security Risk</p>	<p>No</p>
<p>3d. External Drivers</p>	<p>International health information exchange privacy and security policy requirements. Federal law: 21st Century Cures Act, 32 CFR Part 2002, 42 CFR Part 2, and Title 38 Section 7332 as well as draft Trusted Exchange Framework and Common Agreement (TEFCA).</p>

3e. Objectives/Deliverables and Target Dates	<p>May through July 2020 - Refine current SwP material. Add technical requirements and solutions listed in 3a Project Scope above.</p> <p>September 2020 - Ballot SwP white paper as informative.</p> <p>October 2020 - Complete ballot reconciliation.</p> <p>November 2020 - Complete revisions per reconciliation and add/enhance material within project scope.</p> <p>December 2020 - Submit for Jan Ballot cycle.</p> <p>February 2021 - Complete ballot reconciliation.</p> <p>March 2021 - Decide whether ready to request publication or rebalot.</p>
3f. Common Names / Keywords / Aliases:	SwP
3h. Project Dependencies	None
3i. HL7-Managed Project Document Repository URL:	Share with Protections White Paper Project https://confluence.hl7.org/display/SEC/Share+with+Protections+White+Paper+Project
3j. Backwards Compatibility	Yes
3k. Additional Backwards Compatibility Information (if applicable)	Compatible with HL7 V2.9 ARV segment, CDA DS4P IG, FHIR DS4P IG, and Cross-Paradigm US Regulatory Security Labeling IG
3l. Using Current V3 Data Types?	N/A
3m. External Vocabularies	No
3o. Earliest prior release and/or version to which the compatibility applies	No previous SwP white paper version.
4a. Products	White Paper
5a. Project Intent	White Paper
5a. White Paper Type	Balloted Informative
5b. Project Ballot Type	Informative
5d. Joint Copyright	No
6b. Content Already Developed	50%
6c. Content externally developed?	No
6e. Is this a hosted (externally funded) project?	No
6f. Stakeholders	Clinical and Public Health Laboratories, Immunization Registries, Quality Reporting Agencies, Regulatory Agency, Standards Development Organizations (SDOs), Payors, Other
6f. Other Stakeholders	Providers, healthcare consumers, Payers, HIEs.
6g. Vendors	Pharmaceutical, EHR, PHR, Health Care IT, Clinical Decision Support Systems, Lab, HIS
6h. Providers	Clinical and Public Health Laboratories, Emergency Services, Local and State Departments of Health, Medical Imaging Service, Healthcare Institutions (hospitals, long term care, home care, mental health), Other
6h. Other Providers	Care in the Community Providers providing long term services and support.
6i. Realm	Universal

7b. Sponsoring WG Approval Date	Apr 07, 2020
7i. Steering Division Approval Date	Apr 20, 2020
7j. TSC Approval Date	May 18, 2020
Version	3
Modifier	Kathleen Connor
Modify Date	May 06, 2020 17:04
1a. Project Name	Share with Protections White Paper
1b. Project ID	1566
1c. Is Your Project an Investigative Project (aka PSS-Lite)?	No
1d. Is your Project Artifact now proceeding to Normative directly or after being either Informative or STU?	No
2a. Primary/Sponsor WG	Service Oriented Architecture
2d. Project Facilitator	Mike Davis
2f. Modeling Facilitator	Mohammad Jafari
2g. Publishing Facilitator	Mike Davis
2h. Vocabulary Facilitator	Kathleen Connor
2i. Domain Expert Representative	Mike Davis, Mohammad Jafari (CA), Alex Mense (AU)
2j. Business Requirements Analyst	Kathleen Connor
2m. Implementers	VA Others TBD

<p>3a. Project Scope</p>	<p>Share with Protection PPS</p> <p>The “Share with Protections” paper will describe business requirements and technical solutions for a new approach to enabling accessibility and liquidity of health information governed by privacy, security, provenance and trust policies. Healthcare business may require the ability of health information exchange partners to convey computable policies to which they must comply by means of interoperable Security Label metadata on shared information, and for real-time negotiations of the means by which Receivers will consume and persist Security Labels so as to enforce the access control requirements of the conveyed policies.</p> <p>Share with Protections (SwP) extends the concepts of Data Segmentation for Privacy (DS4P) by providing standards-based technology supporting enhanced data sharing, and enabling Receivers to manage local policy-aware workforce access, use, and further by their staff. SwP may enable policy domains to move from explicit patient consent to implicit patient consent, which could ease the burden on patients and their information custodian to enable information exchange.</p> <p>Given the increasingly ubiquitous network of health information exchange and the likewise increasing need to share more easily without information blocking , SwP offers a framework for trusted negotiation between Senders, who are accountable for downstream adherence to the policies that govern their sharing, with Receivers which may not be members of the same policy domain, at run time without resorting to out-of-band static contract methods such as MOUs and DURSA.</p> <p>This paper will describe SwP business requirements, use cases, supporting work flows. It will provide technical solutions, at a conceptual level, that leverage current HL7 Security Labeling standards in HL7 Version 2.9 ARV segment, CDA DS4P Implementation Guide (IG), and FHIR R5 Security Label Module, all of which are based on the HL7 Healthcare Privacy and Security Classification System (HCS).</p> <p>In addition, it will reference capabilities described in the HL7 Security Labeling, Privacy Preserving, Access Control, and Audit Service specifications; the Trust Framework for Federated Authorization Conceptual and Behavioral Models; and the Provenance Domain Analysis Model. Finally, it will reference Sender and Receiver capabilities outlined in the FHIR DS4P IG, which is in ballot, and the Cross-Paradigm US Security Labeling IG, which is in development.</p> <p>Technical Requirements and Solutions to be described include:</p> <ul style="list-style-type: none"> Generating Security Labels per policy Assigning Security Labels using a Security Labeling Service Consuming Security Labels sent on information being integrated into a system Persisting and managing Security Labels Enforcing Security Labels using End User Provisioning, and Access Control and Privacy Protective Services Advertising and discovering Security Label CapabilityStatements Negotiating Sender and Receiver CapabilityStatement using Trust Contracts Reassigning Security Labels when disclosing information previously labeled by another entity. Reclassifying Security Labels per policy, Displaying to end users Security Labels per policy, Retrieving related artifacts associated with a Security Label tag, e.g., the consent directive instance associated with a Security Label policy tag, or a provenance record instance associated with a Security Label provenance tag.
<p>Attachments</p>	<p>Share with Protections with Citations 2020 0210.pptx</p> <p>DS4P_Share with Protections 2020 0220 V2.2.pdf</p>
<p>3b. Project Need</p>	<p>To support (1) the goals of international jurisdictions participants in those jurisdictions' healthcare exchange to share health information in accordance with governing privacy policies; and (2) the goals of the 21st Century Cures Act, participants in US healthcare exchange will be required to share health information in accordance with governing privacy policies. Requirements to meet these laws are addressed in the latest version of the Trusted Exchange Framework and Common Agreement proposal.</p>
<p>3c. Security Risk</p>	<p>No</p>
<p>3d. External Drivers</p>	<p>International health information exchange privacy and security policy requirements. Federal law: 21st Century Cures Act, 32 CFR Part 2002, 42 CFR Part 2, and Title 38 Section 7332 as well as draft Trusted Exchange Framework and Common Agreement (TEFCA).</p>

3e. Objectives/Deliverables and Target Dates	<p>May through July 2020 - Refine current SwP material. Add technical requirements and solutions listed in 3a Project Scope above.</p> <p>September 2020 - Ballot SwP white paper as informative.</p> <p>October 2020 - Complete ballot reconciliation.</p> <p>November 2020 - Complete revisions per reconciliation and add/enhance material within project scope.</p> <p>December 2020 - Submit for Jan Ballot cycle.</p> <p>February 2021 - Complete ballot reconciliation.</p> <p>March 2021 - Decide whether ready to request publication or rebalot.</p>
3f. Common Names / Keywords / Aliases:	SwP
3h. Project Dependencies	None
3i. HL7-Managed Project Document Repository URL:	Share with Protections White Paper Project https://confluence.hl7.org/display/SEC/Share+with+Protections+White+Paper+Project
3j. Backwards Compatibility	Yes
3k. Additional Backwards Compatibility Information (if applicable)	Compatible with HL7 V2.9 ARV segment, CDA DS4P IG, FHIR DS4P IG, and Cross-Paradigm US Regulatory Security Labeling IG
3l. Using Current V3 Data Types?	N/A
3m. External Vocabularies	No
3o. Earliest prior release and/or version to which the compatibility applies	No previous SwP white paper version.
4a. Products	White Paper
5a. Project Intent	White Paper
5a. White Paper Type	Balloted Informative
5b. Project Ballot Type	Informative
5d. Joint Copyright	No
6b. Content Already Developed	50%
6c. Content externally developed?	No
6e. Is this a hosted (externally funded) project?	No
6f. Stakeholders	Clinical and Public Health Laboratories, Immunization Registries, Quality Reporting Agencies, Regulatory Agency, Standards Development Organizations (SDOs), Payors, Other
6f. Other Stakeholders	Providers, healthcare consumers, Payers, HIEs.
6g. Vendors	Pharmaceutical, EHR, PHR, Health Care IT, Clinical Decision Support Systems, Lab, HIS
6h. Providers	Clinical and Public Health Laboratories, Emergency Services, Local and State Departments of Health, Medical Imaging Service, Healthcare Institutions (hospitals, long term care, home care, mental health), Other
6h. Other Providers	Care in the Community Providers providing long term services and support.
6i. Realm	Universal

7b. Sponsoring WG Approval Date

Apr 07, 2020

7i. Steering Division Approval Date

Apr 20, 2020

Version	2
Modifier	Dave Hamill
Modify Date	Oct 15, 2019 17:00
1a. Project Name	Sharing with Protections Project Scope Statement
1b. Project ID	1566
1c. Is Your Project an Investigative Project (aka PSS-Lite)?	No
1d. Is your Project Artifact now proceeding to Normative directly or after being either Informative or STU?	No
2a. Primary/Sponsor WG	Security
2b. Co-Sponsor WG	Conformance
2c. Co-Sponsor Level of Involvement	Request periodic project updates; specify period in text box below (e.g. 'Monthly', 'At WGMs', etc.)
2d. Project Facilitator	Mike Davis
2f. Modeling Facilitator	Mike Davis
3c. Security Risk	No
3j. Backwards Compatibility	No
4a. Products	White Paper
5a. Project Intent	White Paper
5b. Project Ballot Type	Informative
5d. Joint Copyright	No
6b. Content Already Developed	50%
6c. Content externally developed?	No
6e. Is this a hosted (externally funded) project?	No
6f. Stakeholders	Clinical and Public Health Laboratories, Immunization Registries, Quality Reporting Agencies, Regulatory Agency, Standards Development Organizations (SDOs), Payors, Other
6f. Other Stakeholders	Providers, healthcare consumers
6g. Vendors	Pharmaceutical, EHR, PHR, Health Care IT, Clinical Decision Support Systems, Lab, HIS
6h. Providers	Clinical and Public Health Laboratories, Emergency Services, Local and State Departments of Health, Medical Imaging Service, Healthcare Institutions (hospitals, long term care, home care, mental health)
6i. Realm	Universal

Version	1
Modifier	Kathleen Connor
Modify Date	Aug 19, 2019 16:27
1a. Project Name	Sharing with Protections Project Scope Statement
1c. Is Your Project an Investigative Project (aka PSS-Lite)?	No
1d. Is your Project Artifact now proceeding to Normative directly or after being either Informative or STU?	No
2a. Primary/Sponsor WG	Security
2b. Co-Sponsor WG	Conformance
2c. Co-Sponsor Level of Involvement	Request periodic project updates; specify period in text box below (e.g. 'Monthly', 'At WGMs', etc.)
2d. Project Facilitator	Mike Davis
2f. Modeling Facilitator	Mike Davis
3c. Security Risk	No
3j. Backwards Compatibility	No
4a. Products	White Paper
5a. Project Intent	White Paper
5b. Project Ballot Type	Informative
5d. Joint Copyright	No
6b. Content Already Developed	50%
6c. Content externally developed?	No
6e. Is this a hosted (externally funded) project?	No
6f. Stakeholders	Clinical and Public Health Laboratories, Immunization Registries, Quality Reporting Agencies, Regulatory Agency, Standards Development Organizations (SDOs), Payors, Other
6f. Other Stakeholders	Providers, healthcare consumers
6g. Vendors	Pharmaceutical, EHR, PHR, Health Care IT, Clinical Decision Support Systems, Lab, HIS
6h. Providers	Clinical and Public Health Laboratories, Emergency Services, Local and State Departments of Health, Medical Imaging Service, Healthcare Institutions (hospitals, long term care, home care, mental health)
6i. Realm	Universal

