Integrating the Healthcare Enterprise



IHE Quality, Research and Public Health White Paper

Secondary Use Data Exchange (SU-DSX)

Revision 1.0 - Draft for Public Comment

Date: November 13, 2026

Author: Rada Hussein, Lori Fourquet

Email: QRPH@ihe.net

Please verify you have the most recent version of this document. See here for Published versions and here for Public Comment versions.

Copyright © 2026: IHE International, Inc.

Foreword

This is a white paper of the IHE Quality, Research and Regulatory domain.

This white paper is published on November 13, 2026 for Public Comment. Comments are invited and may be submitted at https://www.ihe.net/QRPH_Public_Comments. To be considered in development of the Published version of the white paper, comments must be received by December 14, 2026.

General information about IHE can be found at IHE.net.

Information about the IHE Quality, Research and Public Health domain can be found at IHE Domains.

Information about the organization of IHE Technical Frameworks and Supplements and the process used to create them can be found at Profiles and IHE Process.

The current version of the IHE Quality, Research and Public Health Technical Framework can be found at Quality, Research and Public Health Technical Framework.

 Copyright © 2026: IHE International, Inc.

CONTENTS

Introduction to This White Paper 10
Open Issues and Questions 10
Closed Issues 11
General Introduction 12
Appendix A – Actor Summary Definitions 13
Appendix B – Transaction Summary Definitions 14
Glossary 14
Volume 1 – Profiles 16
Copyright Licenses 16
Domain-specific additions 16
1 Secondary Use Data Exchange (SU-DSX) Profile 16
1.1 SU-DSX Actors, Transactions, and Content Modules 18
SU-DSX Content Modules 24
1.1.1 Actor Descriptions and Actor Profile Requirements 27
1.1.1.1 Secondary Use Agent (SUA) 28
1.1.1.2 Data Access Authority (DAA) 28
1.1.1.3 Data Access Coordinator (DAC) 28
1.1.1.4 Information Source (IS) 28
1.1.1.5 De-ID Manager 28
1.1.1.6 De-ID Policy Authority 28
1.1.1.7 De-Identifier 29
1.1.1.8 Secure Processing Environment (SPE) 29
1.1.1.9 Catalogue Service (CAT) 29
1.1.1.10 Authorization Policy Service (APS) 29
1.2 SU-DSX Actor Options 29
1.2.1 Manifest Option 30
1.2.2 Full Results Option 30
1.2.3 Embedded APS Option 30
1.2.4 Restricted Export Option 30
1.3 SU-DSX Required Actor Groupings 30
1.4 SU-DSX Overview 32
1.4.1 Concepts 32
1.4.1.1 Design Principles 34
1.4.2 Use Cases 35
1.4.2.1 Common Provisioning and Transfer Patterns 35
1.4.2.2 Use Case #1: Cross-Border Epidemiological Study Using IPS+ 39
1.4.2.2.1 Cross-Border Use Case Description 39
1.4.2.2.2 Cross-Border Process Flow 39
1.4.2.3 Use Case #2: Federated Aggregate Query and Statistical Data Request 43
1.4.2.3.1 Data Request Use Case Description 43
1.4.2.3.2 Data Request Process Flow 43
1.4.2.4 Use Case #3: Multimodal AI/ML Method Development and Validation 46
1.4.2.4.1 Data Access Use Case Description 46

 Copyright © 2026: IHE International, Inc.

1.4.2.4.2 Data Access Process Flow 46
1.4.2.4 QRPH-Aligned Output Summary 50
1.5 SU-DSX Security Considerations 51
1.5.1 Audit Considerations 51
1.6 SU-DSX Cross Profile Considerations 51
Appendices to Volume 1 53
Appendix A – Mapping to EHDS-oriented Terminology 54
Volume 2 – Transactions 55
3.1 Query Catalogue [SU-1] 55
3.1.1 Scope 55
3.1.2 Actor Roles 55
3.1.3 Referenced Standards 56
3.1.4 Messages 57
3.1.4.1 Catalogue Query 57
3.1.4.1.1 Trigger Events 57
3.1.4.1.2 Message Semantics 57
3.1.4.1.3 Expected Actions 58
3.1.4.2 Catalogue Query Response 58
3.1.4.2.1 Trigger Events 58
3.1.4.2.2 Message Semantics 58
3.1.4.2.3 Expected Actions 59
3.1.5 Security Considerations 59
3.1.5.1 Security Audit Considerations 60
3.1.5.1.1 Actor Specific Security Considerations 60
3.2 Submit Secondary Use Request [SU-2] 60
3.2.1 Scope 60
3.2.2 Actor Roles 60
3.2.3 Referenced Standards 61
3.2.4 Messages 61
3.2.4.1 Submit Secondary Use Request 61
3.2.4.1.1 Trigger Events 62
3.2.4.1.2 Message Semantics 62
3.2.4.1.3 Expected Actions 63
3.2.4.2 Request Acknowledgement 63
3.2.4.2.1 Trigger Events 63
3.2.4.2.2 Message Semantics 63
3.2.4.2.3 Expected Actions 64
3.2.5 Security Considerations 64
3.2.5.1 Security Audit Considerations 64
3.2.5.1.1 Actor Specific Security Considerations 64
3.3 Issue Permit / Access Decision [SU-3] 65
3.3.1 Scope 65
3.3.2 Actor Roles 65
3.3.3 Referenced Standards 66
3.3.4 Messages 66

 Copyright © 2026: IHE International, Inc.

3.3.4.1 Access Decision 66
3.3.4.1.1 Trigger Events 66
3.3.4.1.2 Message Semantics 67
3.3.4.1.3 Expected Actions 68
3.3.4.2 Decision Receipt Status 68
3.3.4.2.1 Trigger Events 68
3.3.4.2.2 Message Semantics 68
3.3.4.2.3 Expected Actions 68
3.3.5 Security Considerations 69
3.3.5.1 Security Audit Considerations 69
3.3.5.1.1 Actor Specific Security Considerations 69
3.4 Authorized Source Data Provision [SU-4] 69
3.4.1 Scope 69
3.4.2 Actor Roles 69
3.4.3 Referenced Standards 70
3.4.4 Messages 71
3.4.4.1 Provision Request 71
3.4.4.1.1 Trigger Events 71
3.4.4.1.2 Message Semantics 71
3.4.4.1.3 Expected Actions 72
3.4.4.2 Provision Status 72
3.4.4.2.1 Trigger Events 72
3.4.4.2.2 Message Semantics 73
3.4.4.2.3 Expected Actions 73
3.4.4.3 Provision Result and Manifest 73
3.4.4.3.1 Trigger Events 73
3.4.4.3.2 Message Semantics 73
3.4.4.3.3 Expected Actions 74
3.4.5 Security Considerations 75
3.4.5.1 Security Audit Considerations 75
3.4.5.1.1 Actor Specific Security Considerations 75
3.5 Transfer Prepared Data to SPE [SU-5] 75
3.5.1 Scope 75
3.5.2 Actor Roles 76
3.5.3 Referenced Standards 76
3.5.4 Messages 77
3.5.4.1 Prepared Data Delivery Notice 77
3.5.4.1.1 Trigger Events 77
3.5.4.1.2 Message Semantics 77
3.5.4.1.3 Expected Actions 78
3.5.4.2 Prepared Data Transfer 78
3.5.4.2.1 Trigger Events 78
3.5.4.2.2 Message Semantics 78
3.5.4.2.3 Expected Actions 79
3.5.4.3 Ingest Acknowledgement 79

 Copyright © 2026: IHE International, Inc.

3.5.4.3.1 Trigger Events 79
3.5.4.3.2 Message Semantics 79
3.5.4.3.3 Expected Actions 80
3.5.5 Security Considerations 80
3.5.5.1 Security Audit Considerations 80
3.5.5.1.1 Actor Specific Security Considerations 80
3.6 Secure Processing and Results Release [SU-6] 81
3.6.1 Scope 81
3.6.2 Actor Roles 81
3.6.3 Referenced Standards 82
3.6.4 Messages 82
3.6.4.1 Submit Processing Job 83
3.6.4.1.1 Trigger Events 83
3.6.4.1.2 Message Semantics 83
3.6.4.1.3 Expected Actions 84
3.6.4.2 Processing Status and Completion Notice 84
3.6.4.2.1 Trigger Events 84
3.6.4.2.2 Message Semantics 84
3.6.4.2.3 Expected Actions 85
3.6.4.3 Output Release Request 85
3.6.4.3.1 Trigger Events 85
3.6.4.3.2 Message Semantics 85
3.6.4.3.3 Expected Actions 86
3.6.4.4 Release Decision and Approved Output 86
3.6.4.4.1 Trigger Events 86
3.6.4.4.2 Message Semantics 87
3.6.4.4.3 Expected Actions 87
3.6.4.5 Direct Aggregate Result Release 87
3.6.4.5.1 Trigger Events 88
3.6.4.5.2 Message Semantics 88
3.6.4.5.3 Expected Actions 88
3.6.5 Security Considerations 88
3.6.5.1 Security Audit Considerations 89
3.6.5.1.1 Actor Specific Security Considerations 89
3.A1 Audit Event Logging [SU-A1] 90
3.A1.1 Scope 90
3.A1.2 Actor Roles 90
3.A1.3 Referenced Standards 90
3.A1.4 Interaction Diagram 90
3.A1.4.1 Record SU-DSX Audit Event 90
3.A1.4.1.1 Trigger Events 91
3.A1.4.1.2 Message Semantics 91
3.A1.4.1.3 Expected Actions 91
3.A1.5 Security Considerations 92
3.A1.5.1 Security Audit Considerations 92

 Copyright © 2026: IHE International, Inc.

3.A1.5.1.1 Actor-Specific Security Considerations 92
Appendices to Volume 2 93
Appendix A – Common Control Message, Correlation, and Manifest Requirements 94
A.1 Common Identifier Model 94
A.2 FHIR Control Message Envelope 94
A.3 Status, Errors, and Idempotency 95
A.4 Authorization and Version Rules 96
A.5 Common Manifest Requirements 96
A.6 Multiplicity and Distributed Fulfillment 96
Appendix B – Informative Content and Transport Binding Matrix 97
B.1 Binding Selection Principles 97
B.2 FHIR Bulk Data Realization of SU-4 98
B.3 DICOMweb Realization of SU-4 and SU-5 98
B.4 Direct Aggregate Release 98
B.5 HealthDCAT-AP and OMOP Realization Guidance 98
Volume 2 Namespace Additions 100
Volume 3 – Content Modules 101
5 Namespaces and Vocabularies 104
5.1 SU-DSX Code Systems 104
5.2 IHE FormatCode, ActCode, and RoleCode Additions 104
5.3 SU-DSX Canonical FHIR Artifacts 105
5.4 Required Value Sets 105
5.5 Message Event Codes 106
6 Content Modules 107
7 DICOM Content Modules 108
7.1 DICOM Payload Binding Requirements 108
8 FHIR and Other Content Modules 109
8.1 Content Module Inventory and Transaction Binding 109
8.2 Common FHIR Control Message Content Module (SUC) 110
8.2.1 Purpose and Conformance Statement 110
8.2.2 Common Lifecycle Identifiers 111
8.2.3 Versioning, Idempotency, and Reference Rules 111
8.3 Secondary Use Request Content Module (SURQ) 112
8.3.1 Purpose 112
8.3.2 Required Request Semantics 112
8.3.3 Conditional Governance Extensions 113
8.3.4 OMOP Scope Expression 113
8.4 Access Decision / Permit Content Module (SUAD) 113
8.4.1 Purpose 113
8.4.2 Required Decision Semantics 114
8.4.3 Conditional Governance Extensions 115
8.5 Source Provision and Manifest Content Module (SUPM) 115
8.5.1 Purpose 115
8.5.2 SU-4 Message Phases 116
8.5.3 Provision Manifest 116

 Copyright © 2026: IHE International, Inc.

8.5.4 Conditional Governance Evidence 117
8.6 Prepared Data Delivery Content Module (SUDL) 117
8.6.1 Purpose 117
8.6.2 Ingest Acknowledgement 118
8.7 Processing Job Content Module (SUPJ) 118
8.7.1 Purpose 118
8.7.2 OMOP Analytical Job 119
8.8 Results Release Content Module (SURL) 119
8.8.1 Purpose 119
8.8.2 AI/ML, Synthetic, and Other High-Dimensional Outputs 120
8.8.3 Significant-Finding Handling 120
8.9 Aggregate Result Package Content Module (SUAR) 120
8.9.1 Purpose 120
8.10 Audit Correlation Content Module (SUAC) 121
8.10.1 Purpose 121
8.11 HealthDCAT-AP Catalogue Content Binding 122
8.11.1 Status and External Dependency 122
8.12 OMOP Analytical Representation Content Binding 123
8.12.1 Status and Principles 123
8.12.2 Multimodal and Federated Realizations 123
8.13 Clinical, Imaging, and Multimodal Payload Bindings 123
8.13.1 DICOM and DICOMweb Payload Content Binding 124
8.13.2 IPS / IPS+ Research Content Binding 126
8.13.2.1 Status and Scope 126
8.13.2.2 Relationship to the SU-DSX Lifecycle 126
8.13.2.3 IPS / IPS+ Manifest Requirements 127
8.13.2.4 Bulk FHIR Realization of IPS / IPS+ Content 128
8.13.2.5 Relationship to Epidemiology-Specific and Multimodal Data 128
8.13.2.6 Relationship to OMOP Analytical Representation 129
8.13.2.7 Conformance Statement 129
8.13.3 Federated Aggregate Query and Statistical Data Content Binding 129
8.13.3.1 Status and Scope 129
8.13.3.2 Federated Query Definition 130
8.13.3.3 Node Execution and Result Evidence 130
8.13.3.4 Combination and Final Release 131
8.13.3.5 Conformance Statement 131
8.13.4 Multimodal AI/ML Content Binding 131
8.13.4.1 Status and Scope 131
8.13.4.2 Multimodal Manifest and Linkage Requirements 132
8.13.4.3 Processing-Job Requirements 133
8.13.4.4 Output Review and Release 133
8.13.4.5 Conformance Statement 133
8.13.5 Use Case to Content-Binding Mapping 134
8.14 Receiver-Safe Evidence, Security Labels, and Minimization 134
8.15 Machine-Readable Conformance Artifacts and Validation 135

 Copyright © 2026: IHE International, Inc.

8.15.1 Validation Requirements 135
8.16 Examples and Test Requirements 136
Appendices to Volume 3 137
Appendix A – Actor and Content Module Responsibilities 138
Appendix B – Cross-Transaction Content Mapping 139
Appendix C – Informative EHDS / TEHDAS2-Oriented Mapping 140
Volume 3 Namespace Additions 141
Volume 4 – National Extensions 142
4 National Extensions 143
4.1 National/Regional Extensions for EHDS (IHE-Europe) 143
4.1.1 Comment Submission 143
4.1.2 Secondary Use Data Exchange (SU-DSX) 143
4.1.2.1 Query Catalogue [SU-1] 146
4.1.2.2 Submit Secondary Use Request [SU-2] 147
4.1.2.3 Issue Permit / Access Decision [SU-3] 148
4.1.2.4 Authorized Source Data Provision [SU-4] 149
4.1.2.5 Transfer Prepared Data to SPE [SU-5] 150
4.1.2.6 Secure Processing and Results Release [SU-6] 151
4.1.2.7 Audit Event Logging [SU-A1] 152
4.1.2.8 HealthData@EU Cross-Border Routing and Orchestration 153
4.1.2.9 Security, Privacy, and Accountability 154

 Copyright © 2026: IHE International, Inc.

Introduction to This White Paper

This white paper proposes the IHE SU-DSX Integration Profile. The white paper addresses interoperable, policy-governed secondary use of health data across discovery, request submission, access decision, fulfillment coordination, de-identification, secure processing where required, release of anonymized outputs where sufficient, and auditability. This draft focuses on the actor model, transactions, options, required groupings, concepts, and use cases. It aligns with current SU-DSX issues discussed during review and with the emerging IHE De-Identification Services (DIS) proposal.

Secondary Use Data Sharing eXchange (SU-DSX) addresses a growing gap in how health data is governed and shared for secondary use—research, public health, innovation, and regulatory purposes, especially as collaboration increasingly spans organizations and borders (in Europe, an estimated ~40% of health research involves international collaboration).

Although the European Health Data Space (EHDS) provides a strong motivating implementation driver, SU-DSX is positioned as a generic, globally applicable IHE work item that can be adopted internationally wherever similar governance models exist. Today, secondary-use workflows remain fragmented and inconsistently implemented across key lifecycle steps: 1) dataset discovery, 2) structured request submission, 3) permit/authorization issuance (including de-identification requirements), 4) secure data provisioning into controlled processing environments, 5) controlled analysis with constrained results release, and 6) audit/accountability.

Open Issues and Questions

- Dependency on the emerging De-Identification Services (DIS) Profile: Should SU-DSX normatively require DIS when policy-governed de-identification is needed, while retaining SU-DSX responsibility for discovery, requests, authorization, fulfillment, secure processing, and finalization?
- Final boundaries of the SU-DSX transactions: Are the proposed SU-DSX transaction boundaries sufficiently clear? In particular:
  - Should SU-4 be named Authorized Source Data Provision rather than Authorized Source Data Export?
  - Should SU-4 include fulfilment acknowledgement, status, feasibility, manifest, errors, corrections and federated-query responses?
  - Is SU-5 a separately specified transport transaction or a profile-level outcome realized by DIS ITI-x5/ITI-x6 or existing transport profiles?
  - Should SU-6 remain one bidirectional processing-and-release transaction, or be separated into job submission, status and approved-results release interactions?
- Operational exchanges between DAC and Information Source: whether SU-4 should be modeled as an asynchronous bidirectional workflow or as a simpler source-to-recipient provision transaction?

 Copyright © 2026: IHE International, Inc.

- Catalogue publication and maintenance: Should SU-DSX standardize metadata publication from Information Source to Catalogue Service, or remain limited to requester-side catalogue discovery?

Closed Issues

- Generic profile versus EHDS-specific profile: SU-DSX is a generic, internationally applicable IHE profile. EHDS and TEHDAS are informative deployment examples and do not make the normative profile EU-specific.
- Use case selections Volume 1 contains three representative use cases, explaining the different purposes and scenarios for the secondary use of data, covering cross-border epidemiological research using IPS+R (International Patient Summary (IPS)+ Research), federated aggregate and statistical data requests, and multimodal AI/ML method development and validation.
- IPS vs IPS+: IPS provides the standardized minimal clinical summary, while IPS+ extends the IPS-based content model with research-subject, research-study and encounter context to support clinical-research and population-health use cases.Neither represents the complete EHR or all EEHRxF data categories.
- Separation of the Data Access Authority and Data Access Coordinator: DAA and DAC remain separate logical actors.
- Data Holder representation as Information Source: Health Data Holder is treated as an organizational or business role. The corresponding SU-DSX technical actor is the Information Source.
- Secure Processing Environment as a main actor: SPE remains a logical SU-DSX technical actor and is conditionally used. SPE has active responsibilities for controlled processing, supervision of data-processing actions, export control, and accountable release of outputs.
- Authoritative source of original data: The Information Source/Data Holder remains the authoritative source of original data. Temporary HDAB staging does not make the HDAB the permanent system of record.
- Candidate SUA and IS groupings with PCC-1, QEDm and Bulk FHIR are informative or conditional options, not mandatory SU-DSX actors.
- Re-identification transactions: DIS ITI-x7 and ITI-x8 are outside the normal SU-DSX flow.
- OMOP is presented as an optional analytical data-model realization

 Copyright © 2026: IHE International, Inc.

General Introduction

Update the following appendices to the General Introduction as indicated below. Note that these are not appendices to Volume 1.

 Copyright © 2026: IHE International, Inc.

Appendix A – Actor Summary Definitions

Add the following actors to the IHE Technical Frameworks General Introduction list of Actors:

Actor	Definition
Secondary Use Agent (SUA)	System acting on behalf of a health data user to discover datasets, submit requests, receive decisions, submit approved jobs, and receive approved outputs.
Catalogue Service (CAT)	System that publishes and exposes dataset metadata for discovery and request preparation.
Data Access Authority (DAA)	System operated by or for the competent authority to receive requests, evaluate them, and issue permits or other access decisions.
Data Access Coordinator (DAC)	System that operationalizes approved decisions, coordinates fulfillment, tracks provenance and manifests, and initiates downstream preparation or DIS jobs where applicable.
Information Source (IS)	System that holds or exposes authoritative source data and provides only permit-authorized data, facts, extracts, or processing-target references.
De-ID Manager	System that coordinates the DIS workflow, receives authorized de-identification requests, resolves or obtains policy, assigns tasks, tracks status, and controls approved delivery.
De-ID Policy Authority	System that provides the applicable de-identification policy artifacts, policy identifiers, versions, stage requirements, and policy constraints for a submitted authorization context.
De-Identifier	System that performs assigned de-identification tasks, such as identifier removal, pseudonymization, generalization, masking, validation, and preparation of de-id evidence.
De-Identification Requester	System that initiates a de-identification job by presenting data request authorization and the requested processing target.
De-Identified Data Receiver	System that receives or retrieves approved de-identified output and receiver-safe evidence.
De-ID Policy Administrator	Optional administrative actor or role for creating, updating, approving, activating, retiring, or governing de-identification policy artifacts
Data Source (Original)	Source system holding identifiable or source-form data, such as an EHR, PACS, VNA, modality, repository, or local export system
Data Source (De-Identified)	System or repository that stores, stages, or exposes transformed output prepared under DIS governance.
Secure Processing Environment (SPE)	Secure and controlled environment in which authorized secondary-use processing occurs when pseudonymized or otherwise protected data require controlled execution and restricted export.
Authorization Policy Service (APS)	System that evaluates access, governance, transformation, or export policy rules applicable to a request or release decision.
Audit Record Repository (ARR)	Repository that stores audit events produced by grouped security actors and systems.

 Copyright © 2026: IHE International, Inc.

Appendix B – Transaction Summary Definitions

Add the following transactions to the IHE Technical Frameworks General Introduction list of Transactions:

Transaction	Definition
Query Catalogue [SU-1]	Query dataset metadata, availability, access conditions, and related descriptors sufficient to prepare a secondary-use request.
Submit Secondary Use Request [SU-2]	Submit a structured request containing purpose, scope, requested data, safeguards, and related supporting information.
Issue Permit / Access Decision [SU-3]	Communicate a permit, denial, amendment request, or related decision from the access authority to the requesting and fulfillment actors.
Authorized Source Data Provision [SU-4]	Provide permit-authorized source data from one or more Information Source actors toward the approved preparation path.
Transfer Prepared Data to SPE [SU-5]	Transfer pseudonymized or otherwise protected prepared data and associated provenance information into the SPE.
Secure Processing and Results Release [SU-6]	Perform approved processing in the SPE and release only approved outputs in accordance with permit, policy, and disclosure-control constraints.
Audit Event Logging [SU-A1]	Record audit events correlated to request, permit, dataset, transformation, job, and release identifiers.

Glossary

Add the following glossary terms to the IHE Technical Frameworks General Introduction Glossary:

Glossary Term	Definition
Anonymization	Transformation intended to make data non-identifying for the relevant release context, taking account of residual re-identification risk.
Authorization context	Trusted reference or artifact showing that a request or export is authorized, including purpose, scope, recipient, validity, processing environment, and disclosure conditions.
Bulk FHIR	The HL7 FHIR Bulk Data Access approach for asynchronous export of large sets of structured FHIR resources.
Conditional preparation/staging store	Deployment-specific temporary storage for permit-bound extracts, intermediates, or prepared output; it is not an authoritative source and is not a new SU-DSX actor.
European Health Data Space (EHDS)	A European framework for the secure, trusted, and regulated use and reuse of electronic health data. In the secondary-use context, EHDS enables health data to be discovered, requested, prepared, and used for purposes such as research, innovation, public health, policymaking, and regulatory activities, under the oversight of Health Data Access Bodies (HDABs) and with safeguards such as pseudonymization/anonymization, secure processing environments, and auditing
Data applicant	A person applying to use electronic health data for a secondary use purpose
Data holder	Any natural or legal person, public authority or other body in the healthcare or the care sectors that has the right or obligation to provide electronic health data for secondary use purposes or the ability to make such data available

 Copyright © 2026: IHE International, Inc.

Glossary Term	Definition
De-identification	Policy-governed transformation in which identifying information is removed, replaced, generalized, pseudonymized, anonymized, or otherwise controlled.
European Electronic Health Record Exchange Format (EHRxF)	The broader European framework covers several priority health-data categories, including patient summaries, ePrescriptions, laboratory results, discharge reports, and medical imaging. Note: IPS or IPS+ addresses mainly the patient-summary and related structured clinical-data portion, not the complete EEHRxF.
Federated node	A deployment of the Information Source actor that executes an approved query locally and returns only authorized facts, aggregates, or extracts.
HealthData@EU	The EU-level secondary-use infrastructure that links national data infrastructures and national contact points to a central platform, enabling secure and efficient cross-border discovery, access, and exchange of health data under EHDS governance
Health Data Access Body (HDAB)	The authority responsible for assessing the information provided by the data user who applies for electronic health data for a secondary use purpose
HealthDCAT-AP	Metadata profile for publishing and querying health dataset descriptions in catalogues to support interoperable dataset discovery.
International Patient Summary (IPS)	A standardized, minimal clinical summary for one person. It contains essential healthcare information needed to support safe, unscheduled or cross-border care
IPS+	IPS+ is an xShare extension of the IPS concept for uses beyond the basic patient summary, especially clinical research and population health. Note: IPS+ is an IPS-based, FHIR-oriented extension that adds research and population-health context and is being aligned with the European EHR Exchange Format.
Manifest	Structured record describing a prepared data package, its provenance, transformation steps, identifiers, or release status.
Metadata	A structured description of the contents or the use of data facilitating the discovery or use of that data
National contact point (NPC)	A National Contact Point for secondary use is the organisational and technical gateway for making electronic health data available for secondary purposes, including research, innovation, policy-making, and public health. It plays a crucial role in connecting national data infrastructures to the HealthData@EU Central Platform, enabling secure and efficient data sharing across borders.
Observational Medical Outcomes Partnership Common Data Model (OMOP CDM)	An open community data standard that transforms disparate health data into a uniform structure and vocabulary to enable reliable, large-scale observational research
Permit	Machine-processable authorization decision that identifies who may access which data, for what purpose, under what conditions, for what period, and with what output restrictions.
Pseudonymization	Transformation that reduces direct identifiability while retaining controlled re-linkability or longitudinal utility where authorized.
Secondary use	Use of health data for purposes other than direct care of the data subject, including research, innovation, public health, statistics, policy-making, and regulation.
Secure Processing Environment (SPE)	Secure and controlled environment in which authorized secondary-use processing is performed and from which export is restricted according to permit, policy, and disclosure controls.
Second Joint Action Towards the European Health Data Space (TEHDAS2)	An EU-funded project unites 29 European countries to develop the practical guidelines, technical specifications, and IT standards needed to harmonise the cross-border secondary use of health data across Europe

 Copyright © 2026: IHE International, Inc.

Volume 1 – Profiles

Copyright Licenses

NA

Add the following to the IHE Technical Frameworks General Introduction Copyright section:

Domain-specific additions

NA

1 Secondary Use Data Exchange (SU-DSX) Profile

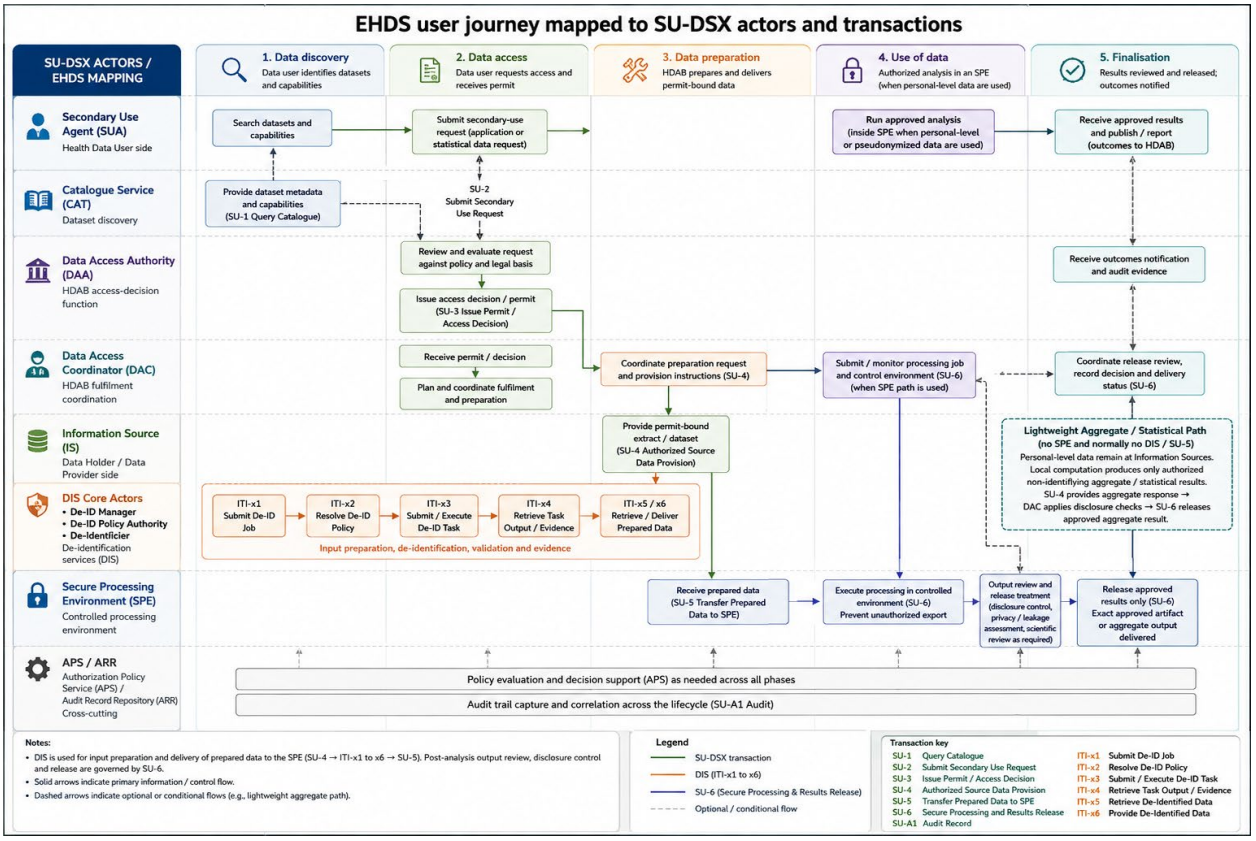
The Secondary Use Data Exchange (SU-DSX) Profile defines a workflow for interoperable and auditable secondary use of health data. The profile supports a requesting system that discovers candidate datasets, submits a structured request to a competent authority, receives a permit or other access decision, coordinates fulfillment by one or more sources, applies de-identification in accordance with policy and permit requirements, executes approved analysis within a Secure Processing Environment (SPE) when required, and receives only approved outputs.

The profile is intended for federated, cross-border, and national deployments. SU-DSX supports both: (a) workflows in which pseudonymized or otherwise protected data are processed only inside an SPE; and (b) workflows in which anonymized data, aggregate reports, or statistical outputs are released directly when they are sufficient, non-identifying in the intended context, and authorized. Actor functions may be centralized, distributed, embedded, or provided by delegated services, provided that externally visible responsibilities remain identifiable.

Example: EHDS secondary-use deployment based on the TEHDAS2 user and data journey

The following figure provides an overall view of the EHDS user journey and its mapping to SU-DSX actors and transactions.

 Copyright © 2026: IHE International, Inc.



Main business actors

Health data holders: Responsible for documenting datasets with clear metadata on purpose, methodology and limitations, and for making available the approved data to the HDAB once a data permit is granted;

Health Data Access Bodies (HDABs): Act as the national intermediaries that support both health data holders and data users throughout the data journey. They validate and publish dataset metadata received from health data holders, maintain the national dataset catalogue and manage data access applications in accordance with the EHDS regulation;

Data user: Finds the data in the dataset catalogue that fits the research needs and requests access by submitting a data access application through the HDAB. If a data permit is granted, they access and analyse the data within the Secure Process Environment (SPE) and, upon completing their work, publish the outcomes of their research and analysis.

 Copyright © 2026: IHE International, Inc.

User journey

When a data applicant applies for electronic health data for secondary use purposes, such as research and innovation activities, education, and policy-making, within the EHDS, the user journey consists of several phases. Access for certain purposes (public or occupational health, policy-making and regulatory activities, and statistics) is reserved for public sector bodies and Union institutions.

Data discovery: Before being able to use the data, the user needs to investigate whether the data needed is available, and whether it is available in the necessary format for the secondary use purpose. This phase is called data discovery. Datasets available in the EU can be found in a metadata catalogue at https://qa.data.health.europa.eu/. Once the data discovery is completed, the user can begin the process of applying for the data.

Data access: In the data access phase, the user fills in and submits a dedicated and standardised data access application or data request form to a HDAB. The user must complete the information required in the form, upload necessary documents, and provide justifications as needed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Data access application is used when the user seeks to use personal level data. Data request is for cases when the user wants to apply for anonymised statistical data.

Data preparation: During this phase, the data holder(s) deliver(s) the necessary data to the HDAB, which starts to prepare the data for secondary use. Techniques for pseudonymisation, anonymisation, generalisation, suppression, and randomisation of personal data are employed. The data minimisation principle (as per the GDPR) must be respected to ensure privacy.

Note: HDAB-controlled storage is deployment-specific. The HDAB may receive and temporarily store permit-bound extracts and intermediate or prepared datasets within its own infrastructure or within an SPE operated on its behalf. The Information Source/Data Holder remains the authoritative source of the original data. Retention and deletion of staged data are governed by the applicable permit, policy, national implementation and security requirements.

Use of data: In this phase, the user performs analyses based on the received data for the purpose defined in the application phase. Analysing personal level data must be performed in a secure processing environment (SPE).

Finalisation: This last phase of the user journey concerns data user's duties regarding analysis outcomes derived from secondary use of data. Data user must publish the results of secondary use of health data within 18 months of the completion of the data processing in a SPE or of receiving the requested health data. The results should be provided in an anonymous format. The data user must inform the HDAB of the results. In addition, the data user must mention in the output that the results have been obtained by using data in the framework of the EHDS.

1.1 SU-DSX Actors, Transactions, and Content Modules

This section defines the actors, transactions, and/or content modules in this profile. General definitions of actors are given in the Technical Frameworks General Introduction Appendix A at http://ihe.net/Technical_Frameworks.

 Copyright © 2026: IHE International, Inc.

The actors directly involved in the SU-DSX Profile are Catalogue Service (CAT), Secondary Use Agent (SUA), Data Access Authority (DAA), Data Access Coordinator (DAC), Information Source (IS), De-ID Manager, De-ID Policy Authority, De-Identifier, Secure Processing Environment (SPE), optional Authorization Policy Service (APS), and Audit Record Repository (ARR) may participate through explicit or grouped security and policy services.

Informatively, Figure 1.1-1 shows an HDAB organizational boundary across the Data Access Authority, Data Access Coordinator, and deployment-specific preparation functions. The Information Source remains a distinct technical actor representing the Data Holder / Data Provider side and remains the authoritative source of original data. The figure depicts the de-identification path using the updated De-Identification Services (DIS) core actors De-ID Manager, De-ID Policy Authority, and De-Identifier, while showing Data Source (Original) and Data Source (De-Identified) as grouped or topology elements rather than core DIS actors.

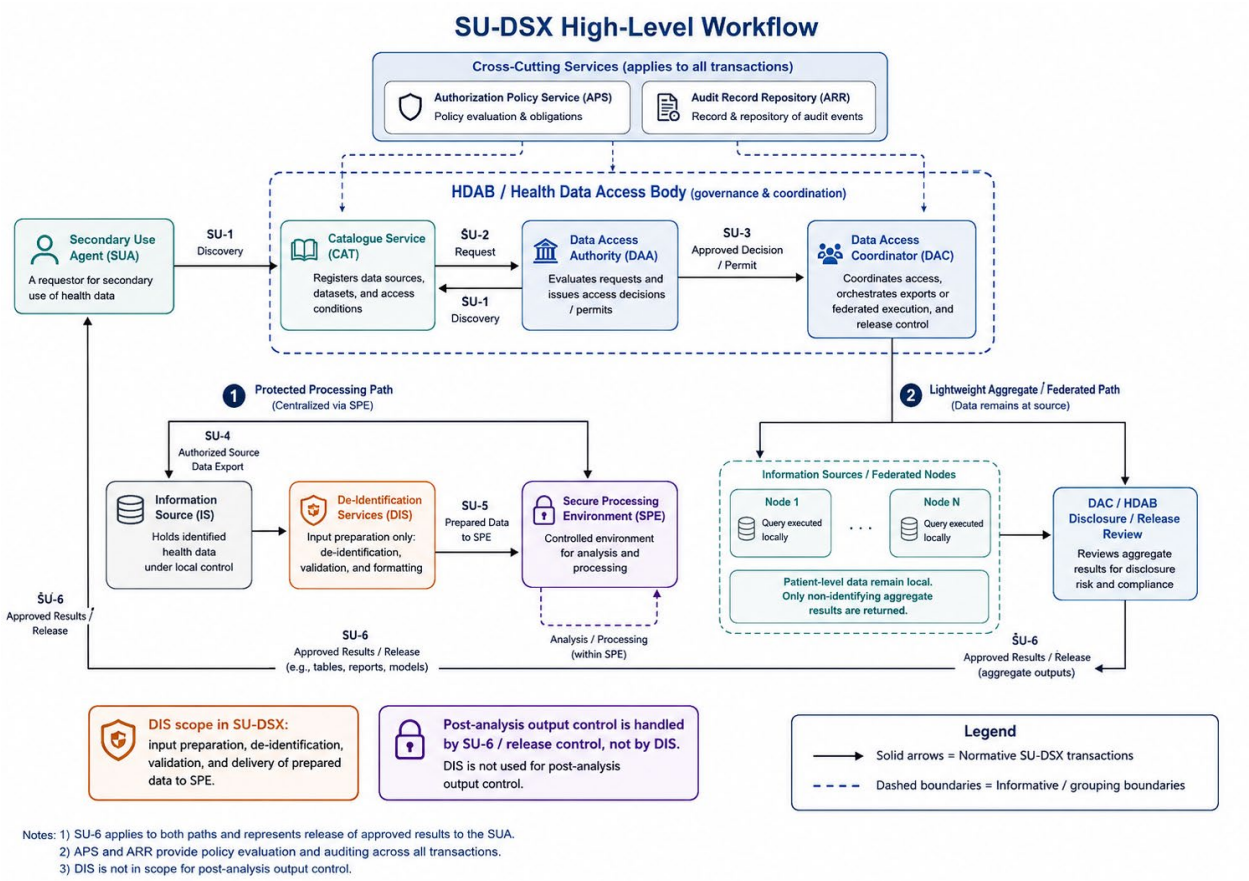


Figure 1.1-1: High-Level Workflow-The actors and transactions used by SU-DSX

Dotted boxes identify organizational boundaries, conditional components, or external/grouped roles; they do not create additional mandatory SU-DSX actors.

Informative candidate groupings for the SUA and IS may reuse PCC-1-style content exchange, QEDm-style query access, or Bulk FHIR-oriented transport. These are realization patterns, not mandatory SU-DSX actors or required baseline groupings.

 Copyright © 2026: IHE International, Inc.

- PCC-1 may support document-style exchange between a Clinical Data Source and Clinical Data Consumer when that content binding is selected.
- QEDm may support query-oriented access to profiled de-identified FHIR resources when an implementation defines the corresponding options and constraints.

Aggregate reporting or aggregate-query mechanisms may be used without the DIS input-preparation workflow when the approved result is non-identifying by design. Residual disclosure risk is handled by the authorized statistical disclosure-control and SU-6 release-control process; an SPE is used only when personal-level or otherwise protected processing is required.

In an EHDS-aligned deployment, an SPE may be used by an authorized data user to process personal electronic health data, or by an HDAB or delegated service to perform protected preparation and processing. Post-analysis output review, anonymization of results where needed, privacy-risk assessment, statistical disclosure control, and release approval are governed through the SPE/SU-6 release-control process rather than through a second DIS job.

Figure 1.1-2 shows the actors directly involved in the SU-DSX Profile and the relevant transactions between them. If needed for context, other actors that may be indirectly involved due to their participation in other related profiles are shown in dotted lines. Actors which have a mandatory grouping are shown in conjoined boxes.

 Copyright © 2026: IHE International, Inc.

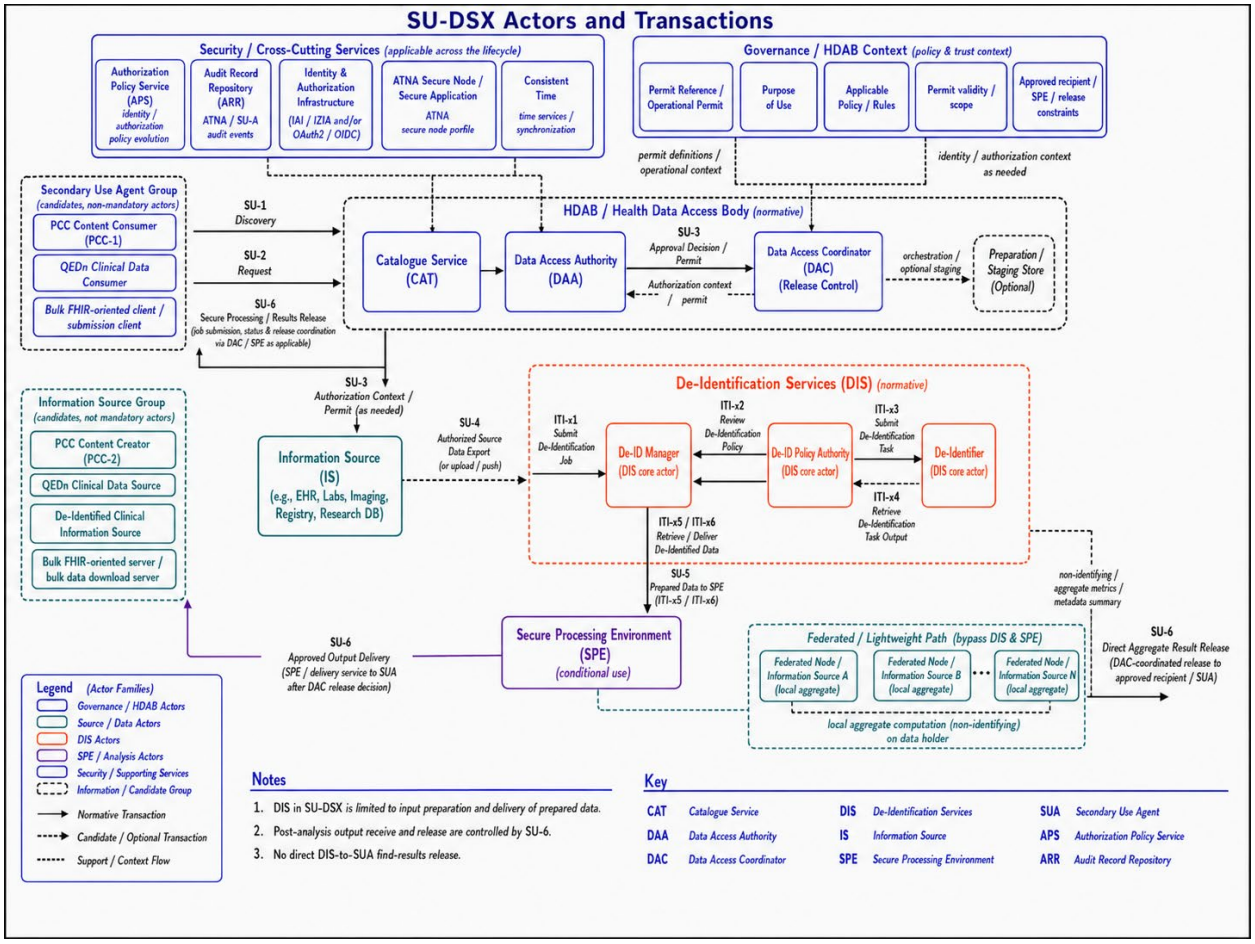


Figure 1.1-2: The actors and transactions used by SU-DSX

Dotted boxes identify organizational boundaries, conditional components, or external/grouped roles; they do not create additional mandatory SU-DSX actors.

At the DIS boundary, SU-4 may make permit-authorized data or processing-target references available for fulfillment. Reads from Data Source (Original) and writes to Data Source (De-Identified) remain external to the core DIS transaction set and are performed by the De-Identifier under the resolved policy.

The permit-bound Preparation / Staging Store is an informative deployment component, not a normative SU-DSX actor. It may temporarily hold approved extracts, intermediate data, transformed output, and provenance under the applicable permit and policy. Depending on the stage, it may be grouped with a DIS Data Source (Original) or Data Source (De-Identified). The Information Source remains the authoritative source of original data.

Notes:

1. SU-DSX supports two principal downstream patterns: (a) a protected SPE path for personal-level or pseudonymized data, and (b) a lightweight aggregate/statistical path in which personal-level data remain at the source and only approved non-identifying results are released.

 Copyright © 2026: IHE International, Inc.

2. The SPE is an active controlled-processing actor. Security, identity, authorization, and audit profiles provide the mechanisms that protect and monitor the SPE but are conceptually separate from it.
3. The SPE is required for personal-level or pseudonymized-data processing and may be omitted when an approved anonymized output can be released directly.
4. DIS begins after an authorization context exists. The DAC normally acts as, or is grouped with, the DIS De-Identification Requester when it submits ITI-x1.
5. The DIS core actors are De-ID Manager, De-ID Policy Authority, and De-Identifier. Within SU-DSX, the De-ID Manager is the orchestration hub for input preparation and controls approved delivery of the prepared de-identified dataset to the authorized processing destination, normally the SPE.
6. ITI-x2 resolves the de-identification policy; ITI-x3 submits a de-identification task; ITI-x4 retrieves task output; ITI-x5 retrieves approved de-identified data; and ITI-x6 delivers approved de-identified data.
7. Data Source (Original), Data Source (De-Identified), De-Identification Requester, and De-Identified Data Receiver are external or grouped DIS roles.
8. ITI-x7 and ITI-x8 are privileged, optional re-identification transactions and are outside the normal SU-DSX flow.
9. DIS-specific delivery evidence applies to the protected input-preparation path; post-analysis release evidence is carried by SU-6.
10. Both downstream paths preserve permit, policy, evidence, receiver, delivery-status, and audit correlation.

Mapping with the updated DE-ID proposal (the DIS proposal still under development)

SU-DSX element	DIS actor or role	Recommendation
Secondary Use Agent or DAC	De-Identification Requester	Conditional required grouping for the actor that submits ITI-x1.
Information Source	Data Source (Original)	Conditional grouping when the De-Identifier reads source data from the IS.
HDAB preparation/staging store	Data Source (Original) and/or Data Source (De-Identified)	Informative grouping determined by whether the component exposes task input, transformed output, or both.
SPE	De-Identified Data Receiver	Conditional required grouping when prepared data are retrieved or delivered through ITI-x5 or ITI-x6.
Results Consumer / SUA	De-Identified Data Receiver	Conditional required grouping for direct approved anonymized release.
HDAB policy administration function	De-ID Policy Administrator	Optional governance grouping.

 Copyright © 2026: IHE International, Inc.

TEHDAS2 Alignment for De-Identification Location and Release Control

SU-DSX distinguishes input preparation from post-analysis output release. Data preparation may include pseudonymisation, anonymisation, generalisation, suppression, and other risk-reduction techniques before authorized processing. Personal-level data analysis occurs in an SPE, while outputs are subject to the applicable anonymity and release requirements.

Project-specific pseudonymisation or de-identification may occur on the data-holder side or HDAB side before data enter the SPE. Post-analysis anonymisation, privacy-risk assessment, statistical disclosure control, synthetic-data assessment, model-leakage assessment, and other release checks are governed as SPE/SU-6 output-control functions and are not modeled as a second DIS job.

For purposes of SU-DSX, DIS is used for authorization-bound input preparation and delivery of the prepared dataset to the authorized processing environment. Post-analysis output review and release are governed separately through SU-6.

Table X.1-1 lists the transactions for each actor directly involved in the SU-DSX Profile. An actor claiming conformance to this profile shall support all required transactions listed for that actor. Optional transactions reflect permissible deployment choices such as manifest-only coordination, embedded policy evaluation, or anonymized-release workflows.

Table 1.1-1: SU-DSX Profile - Actors and Transactions

Actors	Transactions	Optionality	Reference
Catalogue Service (CAT)	Query Catalogue [SU-1]	R	
Secondary Use Agent (SUA)	Query Catalogue [SU-1]	R	
	Submit Secondary Use Request [SU-2]	R	
	Secure Processing and Results Release [SU-6]	R	
Data Access Authority (DAA)	Submit Secondary Use Request [SU-2]	R	
	Issue Permit / Access Decision [SU-3]	R	
Data Access Coordinator (DAC)	Issue Permit / Access Decision [SU-3]	R	
	Authorized Source Data Provision [SU-4]	R	
	Submit De-Identification Job [ITI-x1]	C	
	Secure Processing and Results Release [SU-6]	R	
Information Source (IS)	Issue Permit / Access Decision [SU-3]	C	
	Authorized Source Data Provision [SU-4]	R	
De-ID Manager	Submit De-Identification Job [ITI-x1]	C	

 Copyright © 2026: IHE International, Inc.

Actors	Transactions	Optionality	Reference
	Resolve De-Identification Policy [ITI-x2]	C	
	Submit De-Identification Task [ITI-x3]	C	
	Retrieve De-Identification Task Output [ITI-x4]	O	
	Retrieve De-Identified Data [ITI-x5]	O	
	Deliver De-Identified Data [ITI-x6]	O	
De-ID Policy Authority	Resolve De-Identification Policy [ITI-x2]	C	
De-Identifier	Submit De-Identification Task [ITI-x3]	C	
	Retrieve De-Identification Task Output [ITI-x4]	O	
Secure Processing Environment (SPE)	Prepared Data Delivery to SPE [SU-5]	C	
	Retrieve / Deliver De-Identified Data [ITI-x5 / ITI-x6]	C	
	Secure Processing and Results Release [SU-6]	C	

SU-DSX Content Modules

In addition to the transactions identified in Table 1.1-1, SU-DSX defines content modules that specify the control information exchanged across the secondary-use workflow.

SU-DSX uses an HL7 FHIR R4 message-based control plane for SU-2 through SU-6. These content modules carry the request, access decision, source-provisioning, prepared-data-delivery, processing, results-release, and lifecycle-correlation information required to coordinate the workflow. The content modules are independent of the underlying data-plane mechanism used to provide clinical, imaging, analytical, or other source data.

SU-DSX does not define a new clinical data model. Clinical and analytical payloads remain conformant to applicable external standards and implementation guides, including FHIR/Bulk FHIR, DICOM/DICOMweb, IHE document exchange, HealthDCAT-AP, OMOP CDM, secure file or object transfer, and federated execution patterns.

The **Common FHIR Control Message Content Module (SUC)** provides the common message envelope, workflow identity, versioning, recipient binding, provenance, lifecycle correlation, and error-handling semantics for SU-2 through SU-6. Transaction-specific modules add the content needed for the corresponding SU-DSX interaction.

Figure 1.1-2 shows the principal actors involved in creating and consuming SU-DSX content modules. It represents control-plane content exchange; clinical, imaging, bulk-data, and analytical payload transfers are not shown as separate SU-DSX content modules.

 Copyright © 2026: IHE International, Inc.

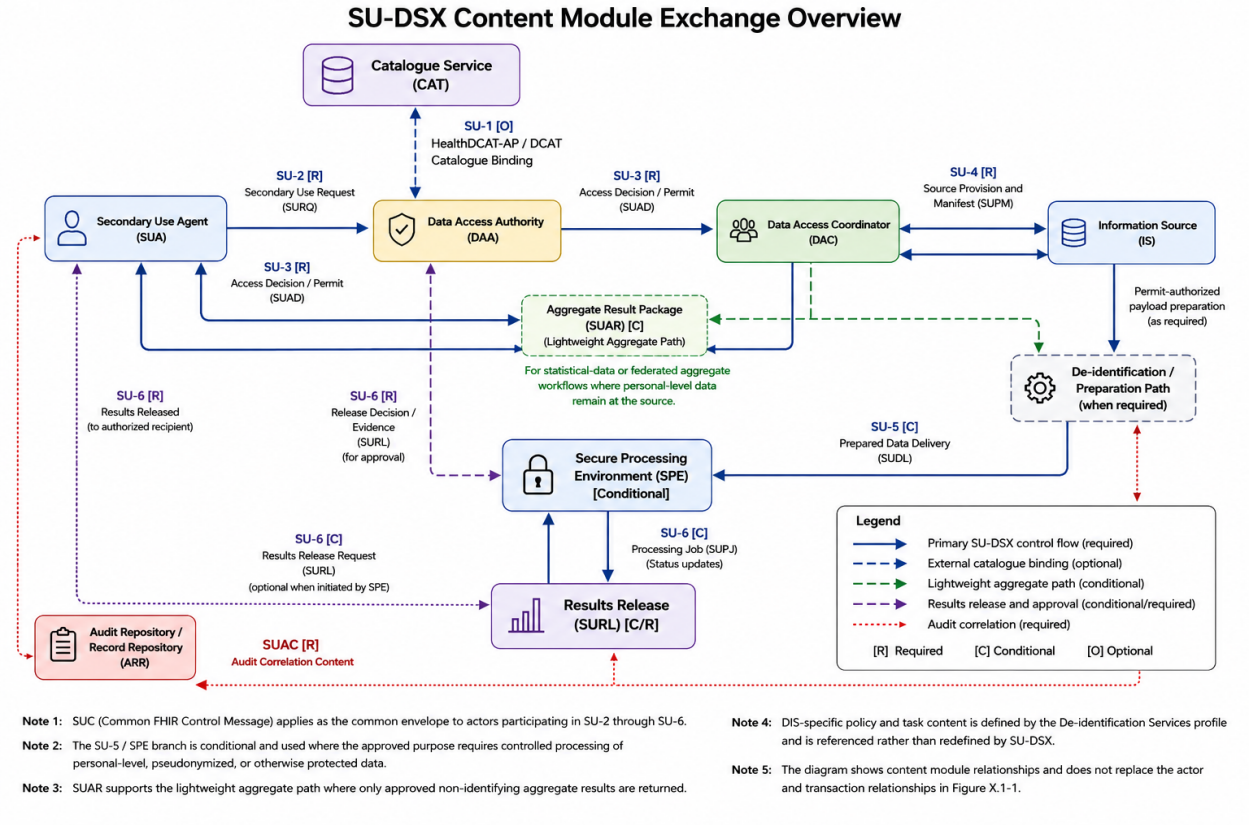


Figure 1.1-2: SU-DSX Content Module Exchange Overview

The content modules in Table X.1-2 define the semantic control information carried by the corresponding transactions. Detailed resource constraints, cardinalities, value sets, lifecycle identifiers, versioning rules, cross-border context, manifest requirements, processing-job semantics, aggregate-result evidence, release evidence, and audit-correlation requirements are specified in QRPH TF-3, Section 8.

The SU-DSX content modules do not alter the authoritative source-data representation. The Information Source remains authoritative for the original data, while the control content maintains traceability from the secondary-use request through the access decision, source fulfilment, preparation, processing, and approved release.

Table 1.1-2: SU-DSX Profile - Actors and Content Modules

Actor	Content Module / Content Role	Optionality	Reference
Catalogue Service (CAT)	HealthDCAT-AP / DCAT Catalogue Binding – Provider	O	SU-DSX TF-3: 8.1, 8.11
Secondary Use Agent (SUA)	HealthDCAT-AP / DCAT Catalogue Binding – Consumer	O	SU-DSX TF-3: 8.1, 8.11
Secondary Use Agent (SUA)	Secondary Use Request (SURQ) – Creator	R	SU-DSX TF-3: 8.3

 Copyright © 2026: IHE International, Inc.

Actor	Content Module / Content Role	Optionality	Reference
Data Access Authority (DAA)	Secondary Use Request (SURQ) – Consumer	R	SU-DSX TF-3: 8.3
Data Access Authority (DAA)	Access Decision / Permit (SUAD) – Creator	R	SU-DSX TF-3: 8.4
Secondary Use Agent (SUA)	Access Decision / Permit (SUAD) – Consumer	R	SU-DSX TF-3: 8.4
Data Access Coordinator (DAC)	Access Decision / Permit (SUAD) – Consumer	R	SU-DSX TF-3: 8.4
Information Source (IS)	Access Decision / Permit (SUAD) – source-specific Consumer	C	SU-DSX TF-3: 8.4
Data Access Coordinator (DAC)	Source Provision and Manifest (SUPM) – Creator / Consumer	R	SU-DSX TF-3: 8.5
Information Source (IS)	Source Provision and Manifest (SUPM) – Consumer / Creator	R	SU-DSX TF-3: 8.5
Data Access Coordinator (DAC) / De-ID Manager, as applicable	Prepared Data Delivery (SUDL) – Creator / Consumer	C	SU-DSX TF-3: 8.6
Secure Processing Environment (SPE)	Prepared Data Delivery (SUDL) – Consumer / acknowledgement Creator	C	SU-DSX TF-3: 8.6
Secondary Use Agent (SUA) and/or Data Access Coordinator (DAC), as permitted	Processing Job (SUPJ) – Creator	C	SU-DSX TF-3: 8.7
Secure Processing Environment (SPE)	Processing Job (SUPJ) – Consumer / Status Creator	C	SU-DSX TF-3: 8.7
Secure Processing Environment (SPE) / Secondary Use Agent (SUA), as applicable	Results Release (SURL) – Release Request Creator	C	SU-DSX TF-3: 8.8
Data Access Authority (DAA) or authorized release function	Results Release (SURL) – Reviewer / Decision Creator	R	SU-DSX TF-3: 8.8
Secondary Use Agent (SUA) / authorized recipient	Results Release (SURL) – Consumer	R	SU-DSX TF-3: 8.8
Information Source (IS), Data Access Coordinator (DAC), and Secondary Use Agent (SUA), when the aggregate path is used	Aggregate Result Package (SUAR)	C	SU-DSX TF-3: 8.9
Actors participating in SU-2 through SU-6	Common FHIR Control Message (SUC)	R	SU-DSX TF-3: 8.2

 Copyright © 2026: IHE International, Inc.

Actor	Content Module / Content Role	Optionality	Reference
Applicable SU-DSX actors	Audit Correlation Content (SUAC)	R	SU-DSX TF-3: 8.10

R = required when the corresponding transaction is implemented.
C = conditional for the applicable workflow path.
O = optional external content binding.

Note 1: SUC is the common FHIR R4 control-message envelope for SU-2 through SU-6 and is used together with the applicable transaction-specific content module.

Note 2: SUDL and SUPJ are conditional because the Secure Processing Environment is not used in every SU-DSX workflow. For example, an approved non-identifying statistical-data request may follow the lightweight aggregate path without transferring personal-level data to an SPE.

Note 3: SUAR is conditional and applies to statistical-data requests or federated aggregate workflows where personal-level data remain at the source and only authorized non-identifying aggregate results are returned.

Note 4: HealthDCAT-AP is an optional external content binding for SU-1. A deployment may use another compatible catalogue application profile where permitted.

Note 5: OMOP CDM is an optional analytical representation rather than an additional SU-DSX actor or transport mechanism. Where an OMOP realization is used, the applicable SU-DSX control content identifies the analytical model, vocabulary, transformation, provenance, and validation context. OMOP is therefore not shown as a separate actor in Figure 1.1-2.

Note 6: FHIR/Bulk FHIR, DICOM/DICOMweb, document exchange, secure file or object transfer, and controlled or federated endpoints are data-plane realizations. They do not constitute additional SU-DSX content-module actors.

Note 7: Content artifacts defined by the De-Identification Services (DIS) profile, including policy-resolution, de-identification-task, and DIS delivery artifacts, are referenced by SU-DSX where the DIS path is used and are not duplicated as SU-DSX content modules.

1.1.1 Actor Descriptions and Actor Profile Requirements

Most requirements are documented in Transactions (Volume 2) and Content Modules (Volume 3). This section documents additional requirements on SU-DSX actors that are necessary to preserve end-to-end workflow correlation and profile behavior.

Actors participating in SU-DSX shall preserve the applicable lifecycle identifiers received from preceding transactions when creating subsequent content. This enables correlation of the request, access decision, source fulfilment, manifest, de-identification activities where applicable, prepared-data delivery, processing job, results-release decision, and audit events.

The content-module responsibilities in Table 1.1-2 do not imply that clinical or analytical payloads must be represented as FHIR. The control plane may reference payloads represented using other approved content and transport mechanisms.

 Copyright © 2026: IHE International, Inc.

1.1.1.1 Secondary Use Agent (SUA)

The SUA shall discover relevant datasets, submit a structured secondary-use request, correlate decisions and permits with the request, initiate permitted processing or analysis actions, and receive only outputs approved through SU-6. Informatively, the SUA may also be grouped with PCC-1, QEDm, or Bulk FHIR requester-side actors.

1.1.1.2 Data Access Authority (DAA)

The Data Access Authority (DAA) shall receive and manage secondary-use requests and shall communicate a permit, denial, amendment request, or other access decision. The DAA shall ensure that any communicated decision includes sufficient identifiers and constraints to enable downstream coordination, policy retrieval, and release control.

1.1.1.3 Data Access Coordinator (DAC)

The DAC shall operationalize an approved access decision, coordinate fulfillment across Information Source actors, preserve request and permit traceability, and initiate downstream preparation or DIS input-preparation jobs where required. When the DAC submits ITI-x1, it shall be grouped with the DIS De-Identification Requester role.

1.1.1.4 Information Source (IS)

The Information Source (IS) shall provide only the source data elements and scope authorized by the permit and applicable policy. The IS shall reject, quarantine, or flag requests for which permit scope, timing, requester identity, or other material conditions cannot be verified. Informatively, the Information Source may be grouped with a content-creator role, including PCC-1-style exchange for de-identified content, a de-identified clinical information source using profiled QEDm options, or a Bulk FHIR-oriented source or bulk-download-server pattern, while remaining the logical SU-DSX presentation of the Data Holder / Data Provider side.

1.1.1.5 De-ID Manager

The De-ID Manager shall coordinate the de-identification workflow for an approved fulfillment event. It shall bind the authorization context to the input-preparation job, obtain the applicable de-identification policy artifacts, compile executable stages or tasks, assign work to the De-Identifier, coordinate approved delivery of the prepared dataset to the authorized processing destination, and record de-identification evidence.

1.1.1.6 De-ID Policy Authority

The De-ID Policy Authority shall maintain and resolve the authoritative set of de-identification policies used within the profile. It shall resolve policy from the supplied authorization context and any minimal policy-selection hints, but it shall not approve the underlying access request or issue the authorization decision.

 Copyright © 2026: IHE International, Inc.

1.1.1.7 De-Identifier

The De-Identifier shall execute the input-preparation de-identification tasks assigned by the De-ID Manager according to the applicable policy artifacts. These tasks may include direct identifier removal, pseudonymization, anonymization where required for the prepared dataset, suppression, redaction, date transformation, generalization, rare-case handling, DICOM-specific treatment, and other policy-governed transformations needed before authorized processing. Post-analysis disclosure control and release assessment are outside the SU-DSX use of the De-Identifier.

1.1.1.8 Secure Processing Environment (SPE)

The SPE shall receive permit-bound prepared data only through an authorized delivery path and shall execute only approved processing activities. When the SPE receives prepared de-identified data using ITI-x5 or ITI-x6, it shall be grouped with the DIS De-Identified Data Receiver role.

The SPE may host or govern post-analysis anonymization, synthetic-data assessment, privacy-risk assessment, statistical disclosure control, model-leakage assessment, scientific review, and other release-control functions for export candidates. These functions are governed through SU-6 and are not modeled as DIS de-identification jobs by SU-DSX.

1.1.1.9 Catalogue Service (CAT)

The Catalogue Service (CAT) shall expose metadata sufficient to support discovery and request preparation. At a minimum, the metadata exposed by CAT shall identify the dataset or service, relevant scope or topic, and enough contextual information to support an informed request.

1.1.1.10 Authorization Policy Service (APS)

When present as a distinct actor, the Authorization Policy Service (APS) shall evaluate applicable access, transformation, or export rules using the conveyed request context, policy references, permits, and other applicable inputs.

1.2 SU-DSX Actor Options

Options that may be selected for each actor in this profile, if any, are listed in table X.2-1. Dependencies between options when applicable are specified in notes.

Table 1.2-1:SU-DSX - Actors and Options

Actor	Option Name	Reference
Data Access Coordinator (DAC)	Manifest Option	1.2.1
Data Access Coordinator (DAC)	Full Results Option	1.2.2
Data Access Authority (DAA)	Embedded APS Option	1.2.3
Secure Processing Environment (SPE)	Restricted Export Option	1.2.4

 Copyright © 2026: IHE International, Inc.

1.2.1 Manifest Option

A Data Access Coordinator claiming the Manifest Option shall receive and manage a manifest, provenance package, or fulfillment record without necessarily receiving the prepared payload itself.

1.2.2 Full Results Option

A Data Access Coordinator claiming the Full Results Option may receive the prepared payload, released result package, or both, where permitted by policy and deployment architecture.

1.2.3 Embedded APS Option

A Data Access Authority claiming the Embedded APS Option shall perform the policy evaluation required for request review within the DAA actor boundary and need not group with an external APS.

1.2.4 Restricted Export Option

A Secure Processing Environment claiming the Restricted Export Option shall prevent unrestricted release of imported data and intermediate artifacts. It shall support only the release path authorized by permit, policy, and disclosure-control decision.

1.3 SU-DSX Required Actor Groupings

Actors shall implement the required security and conditional DIS groupings listed in Table 1.3-1. Groupings with PCC-1, QEDm, Bulk FHIR, mADX, or other content and transport patterns are informative and are described in Section 1.6.

A conditional grouping becomes required only when the corresponding DIS transaction or realization is claimed.

All networked actors shall support mutually authenticated secure communications, consistent time, and auditable event generation appropriate to the deployment. The specific ATNA, CT, identity, and authorization constraints will be finalized with the security profile design.

Table 1.3-1: SU-DSX - Required Actor Groupings

SU-DSX Actor	Actor to be grouped with	Reference	Content Bindings Reference
Catalogue Service (CAT)	ITI ATNA Secure Node or Secure Application; ITI Consistent Time Client		
Secondary Use Agent (SUA)	ITI Consistent Time Client		
Secondary Use Agent (SUA)	ITI ATNA Secure Node or Secure Application		

 Copyright © 2026: IHE International, Inc.

SU-DSX Actor	Actor to be grouped with	Reference	Content Bindings Reference
Secondary Use Agent (SUA)	Content Consumer (document-style realization), QEDm Clinical Data Consumer (de-identified FHIR realization), or Bulk FHIR-oriented client realization De-Identification Requester		These groupings are not required for all SU-DSX implementations. An implementation shall claim the grouping(s) appropriate to the content, transport, and deployment model it supports.
Data Access Authority (DAA)	ITI ATNA Secure Node; ITI Consistent Time Client		
Data Access Authority (DAA)	ITI ATNA Secure Node; ITI Consistent Time Client		
Data Access Coordinator (DAC)	ITI ATNA Secure Node; ITI Consistent Time Client De-Identification Requester		
Information Source (IS)	ITI ATNA Secure Node; ITI Consistent Time Client		
Information Source (IS)	Content Creator (document-style realization), QEDm-style source / de-identified clinical information source, or Bulk FHIR-oriented server realization DIS Data Source (Original)		These groupings are not required for all SU-DSX implementations. An implementation shall claim the grouping(s) appropriate to the content, transport, and deployment model it supports.
De-ID Manager	ITI ATNA Secure Node		
De-ID Policy Authority	ITI ATNA Secure Node		
De-Identifier	ITI ATNA Secure Node		
Secure Processing Environment (SPE)	ITI ATNA Secure Node DIS De-Identification Receiver		

Additional groupings for identity, document exchange, or national trust services may be specified by implementation guides. Unless explicitly stated otherwise, such additional groupings are informative in this draft.

 Copyright © 2026: IHE International, Inc.

1.4 SU-DSX Overview

1.4.1 Concepts

SU-DSX separates access decision-making from fulfillment and separates source-data provision from transformation. This allows governance, operational coordination, policy resolution, input de-identification, secure processing, and output release to be performed by different systems or grouped differently across jurisdictions.

A practical baseline combines catalogue discovery, structured request and decision exchange, permit-bound source provision, DIS policy and task orchestration when input de-identification is required, controlled processing in an SPE for personal-level or pseudonymized data, and SU-6-controlled release of approved outputs. A lightweight aggregate/statistical path may omit the SPE when personal-level data remain at the source.

DIS supports preparation of permit-authorized source data before controlled processing. It may perform pseudonymization, de-identification, content-specific transformation, validation, and generation of evidence, followed by delivery of the prepared dataset to the authorized processing environment.

Results generated subsequently by analysis are outside the SU-DSX use of DIS. Such results are subject to the SU-6 release-control process, which may include statistical disclosure control, privacy-risk assessment, model-leakage or reconstruction assessment, synthetic-data risk assessment, scientific review, administrative review, or other permit-defined release checks.

For federated aggregate requests, personal-level data remain at the source. Aggregate results undergo the required source-side and release-level disclosure controls and are released through SU-6 without invoking a post-query DIS job.

SU-DSX distinguishes a data-access application for personal-level data from a request for anonymized statistical data. The former normally leads to protected processing in an SPE; the latter may use a lighter federated or aggregate path when the output is non-identifying by design. Residual output risk does not by itself invoke DIS or require an SPE.

 Copyright © 2026: IHE International, Inc.

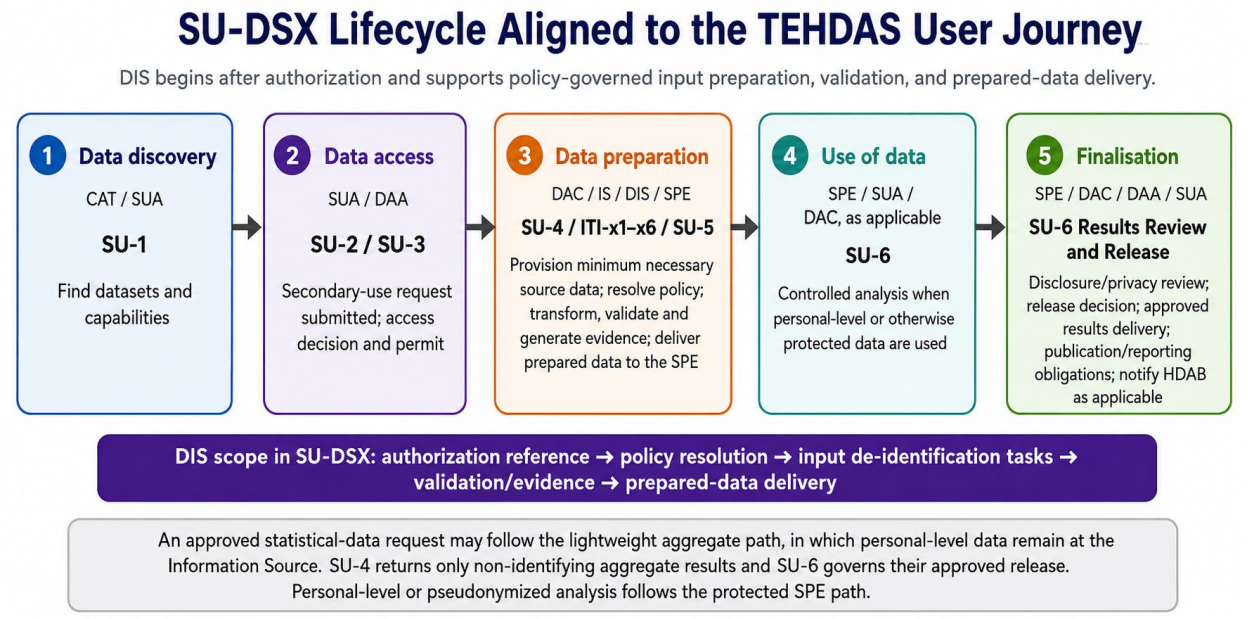


Figure 1.4-1: SU-DSX lifecycle aligned to the EHDS user journey

TEHDAS2 alignment distinguishes project-specific pseudonymization of input data from anonymization, privacy-risk assessment, and disclosure-control treatment applied to outputs or release candidates. In the TEHDAS2 user journey, data preparation begins when data holders deliver the necessary data to the HDAB, after which techniques such as pseudonymization, anonymization, generalization, suppression, and randomization may be applied as part of preparing data for secondary use. TEHDAS2 further treats personal-level analysis as taking place in a Secure Processing Environment and requires released results to be anonymous.

Project-specific pseudonymization may be performed by a data holder or HDAB-controlled service. Before controlled analysis, the approved workflow may require additional pseudonymization, linkage, minimization, or transfer into an SPE. Final anonymization, privacy-risk assessment, and disclosure control may be performed as SPE-governed functions or through a DIS-governed release job.

Data minimization is assessed across the practical dimensions of who, what, when, where, and how during request preparation, permit review, source provision, processing, and release. SU-DSX does not require a single physical placement for all preparation or de-identification functions, but it requires the authorization context and evidence chain to remain traceable.

For alignment with the TEHDAS2 user journey, SU-DSX distinguishes between a data access application for personal-level data and a data request for anonymized statistical data. This distinction does not change the overall SU-DSX orchestration pattern, but it clarifies when controlled personal-level processing in the SPE is expected and when an anonymized statistical output path is sufficient.

SU-DSX distinguishes a data-access application for personal-level data from a request for anonymized statistical data. The former normally leads to protected processing in an SPE; the latter may use a lighter federated or aggregate path when the output is non-identifying by design.

 Copyright © 2026: IHE International, Inc.

Residual small-cell, rare-category, institutional, professional, or other disclosure risks invoke the protected DIS/SPE path.

Analytical Data Models:

SU-DSX distinguishes source-data provision formats from analytical data models. Source data may be provisioned using FHIR, Bulk FHIR, document exchange, DICOM, DICOMweb, managed file transfer, database extracts or other permit-authorized mechanisms. Following provision, structured data may be transformed into an analytical data model, such as the Observational Medical Outcomes Partnership Common Data Model—OMOP CDM—as part of permit-bound preparation or inside the Secure Processing Environment.

OMOP CDM may support harmonized cohort definition, observational analysis, quality-measure calculation, distributed analytics and feature preparation for AI/ML. OMOP CDM is not a transport protocol and does not replace the source-data provision mechanisms profiled or referenced by SU-DSX.

An implementation is not required to maintain a permanent OMOP repository. Transformation to OMOP may occur at the Information Source, in an HDAB-controlled preparation environment, inside the SPE or at distributed participating nodes, according to the authorization context and deployment architecture.

1.4.1.1 Design Principles

- Request purpose, data scope, and safeguards shall remain traceable across review, provisioning, processing, and release.
- Permit identifiers and versions shall be preserved throughout the transaction chain.
- A single request may result in provisioning by multiple Information Source actors.
- The profile shall support secure processing whenever unrestricted personal-data export is not permitted.
- The protected SPE path is used where the approved purpose requires processing of personal-level or pseudonymized data.
- The profile shall also support direct release of anonymized data or anonymized aggregate outputs when such release is sufficient and authorized.
- The lightweight path is used where the approved purpose can be fulfilled by locally generated non-identifying aggregate or statistical results without transferring personal-level data.
- DIS is used by SU-DSX for input preparation and prepared-data delivery, not for post-analysis output-control jobs.
- Output review and release are governed through SU-6 and the applicable SPE/authorized release-control function.
- Auditability shall cover request submission, decision, policy retrieval, transformation, secure processing, and release of outputs.

 Copyright © 2026: IHE International, Inc.

1.4.2 Use Cases

1.4.2.1 Common Provisioning and Transfer Patterns

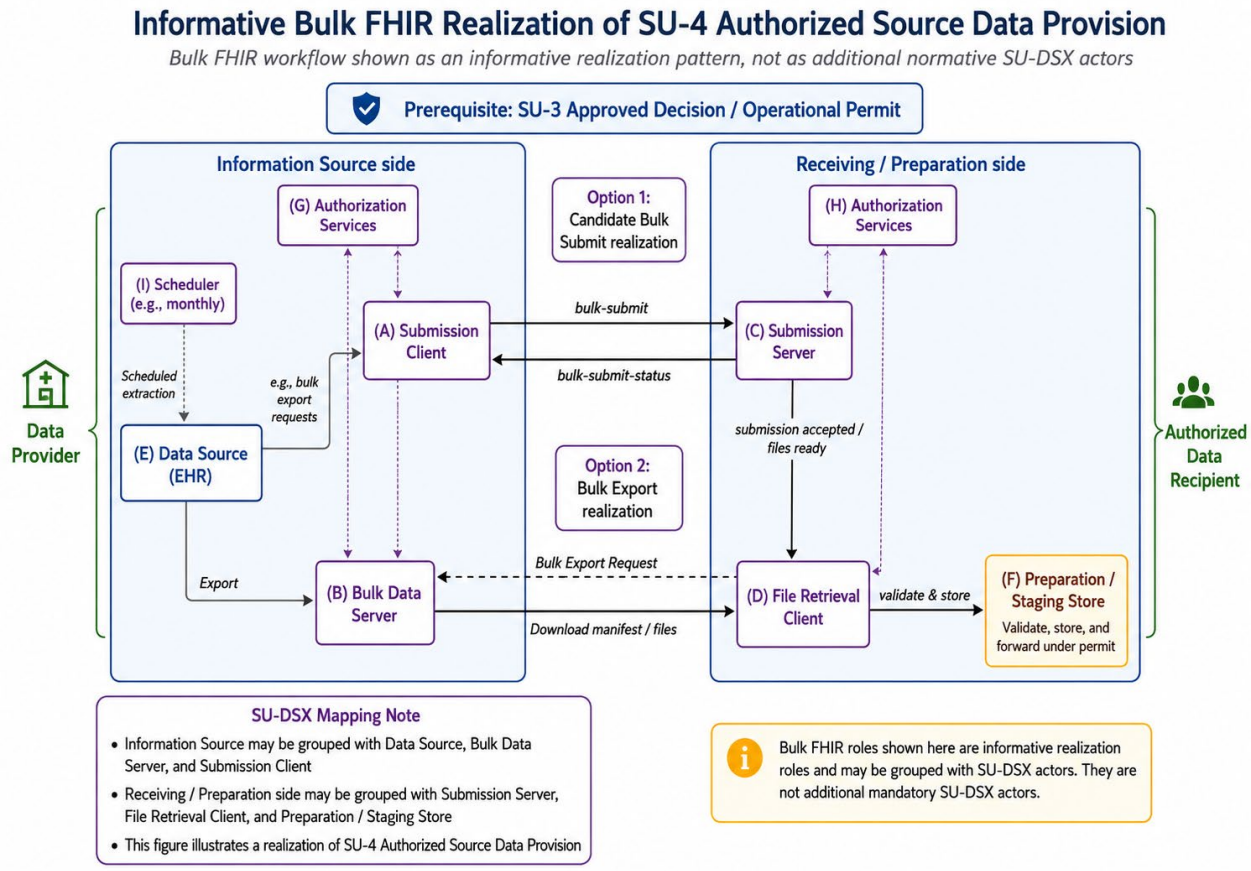
The use cases in this section may use different technical realization patterns for Authorized Source Data Provision [SU-4], depending on the data type and volume, the location of the authoritative source, the approved processing model, and the capabilities of the participating systems.

SU-DSX defines SU-4 as a technology-neutral business interaction through which one or more Information Source actors provide permit-authorized data, extracts, aggregate responses, imaging studies, multimodal packages, or processing-target references to an approved fulfilment path. The Data Access Coordinator coordinates fulfilment and preserves correlation with the request and authorization context. The Information Source remains the authoritative source of the original data.

Figures 1.4.2.1-1 and 1.4.2.1-2 illustrate an informative Bulk FHIR realization of the payload-transfer portion of SU-4. The implementation roles shown may be grouped with SU-DSX actors but are not additional normative SU-DSX actors.

The use cases in this section may use different technical realization patterns for Authorized Source Data Provision [SU-4], depending on the data type and volume, the location of the authoritative source, the approved processing model, and the capabilities of the participating systems.

 Copyright © 2026: IHE International, Inc.



865 **Figure 1.4.2.1-1: Generic Informative Bulk FHIR realization of Authorized Source Data Export [SU-4]**

 Copyright © 2026: IHE International, Inc.

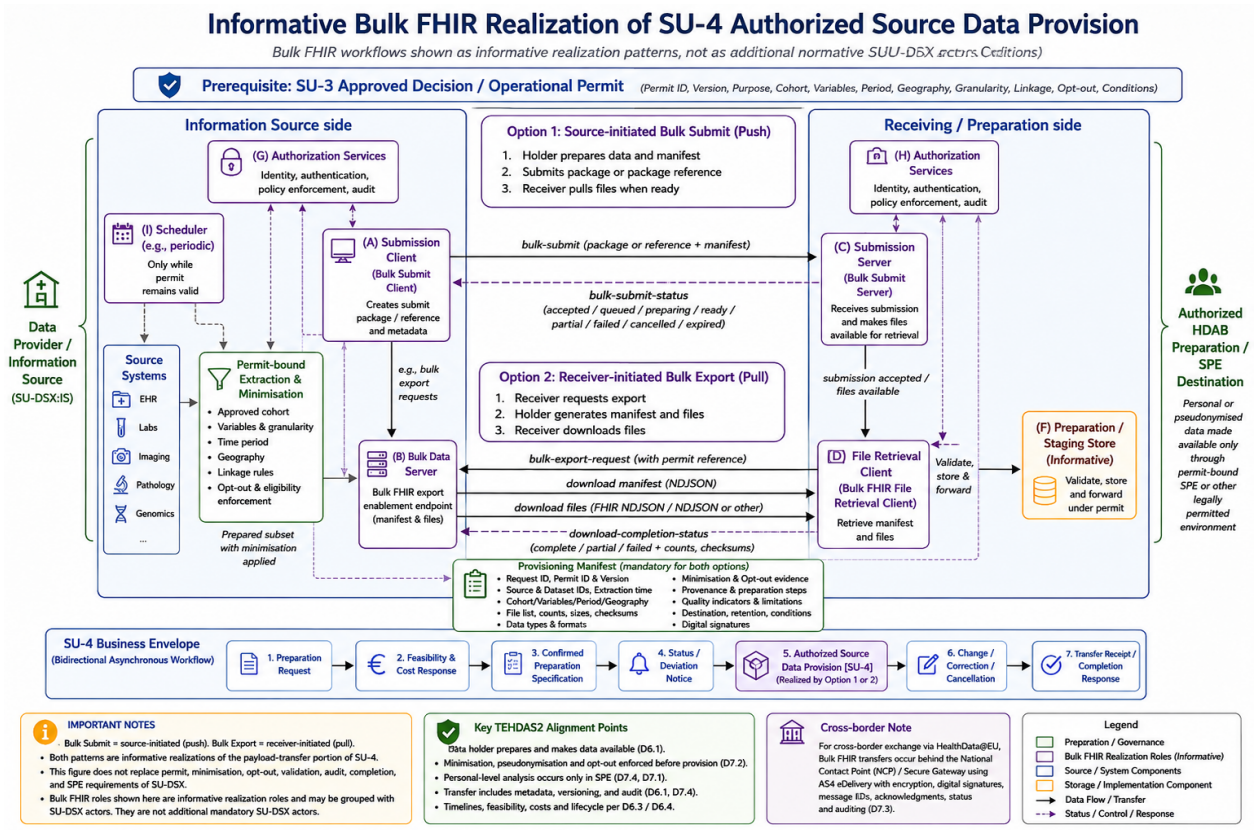


Figure 1.4.2.1-2: Detailed Informative Bulk FHIR realization of Authorized Source Data Export [SU-4]

Technical realization patterns

FHIR and Bulk FHIR may provide structured clinical resources, cohort information, manifests, provenance, and references to associated binary objects. Medical imaging and digital-pathology objects normally remain in DICOM or another approved native format and may be transferred or accessed through DICOMweb, managed file transfer, secure object-store access, secure repository access, or controlled remote access. SU-DSX does not require DICOM objects to be converted into FHIR resources.

A multimodal provision may combine structured FHIR resources, DICOM studies and derived objects, digital-pathology images, laboratory or genomic information, registry or outcome data, and manifests linking structured data with binary objects. Federated execution may also be used where data remain at the Information Source and only approved results or artifacts are returned.

Permit-bound preparation

The provisioning workflow begins only after Issue Permit / Access Decision [SU-3] has established a valid authorization context. The Information Source provides only data, images, objects, or references within the approved scope. Selection and minimization may constrain the population, variables or objects, observation period, organizational or geographical scope, level of detail, linkage method, transfer mechanism, and destination. Applicable eligibility and opt-out rules are evaluated before personal electronic health data are made available for secondary use.

 Copyright © 2026: IHE International, Inc.

Imaging preparation may need to address identifying information in both metadata and pixel content. Detailed FHIR, DICOM, imaging de-identification, manifest, validation, acknowledgement, error-handling, and conformance requirements are specified in Volume 2 or in referenced profiles.

Informative actor groupings

The Information Source may include or group with a clinical Data Source, Imaging Archive, Bulk FHIR or DICOMweb server, Submission Client, extraction or packaging service, authorization service, and permit-bound minimization function. The receiving or preparation side may include or group with a Submission Server, File Retrieval Client, imaging-retrieval client, manifest resolver, validation and ingest service, authorization service, and Preparation / Staging Store. These are informative implementation components and do not introduce additional mandatory SU-DSX actors.

Where personal-level, pseudonymized, or otherwise protected data require analysis, prepared data proceed to the Secure Processing Environment through Prepared Data Delivery to SPE [SU-5]. Where the requested output is non-identifying by design, a lighter fulfilment and release path may be used without transferring personal-level data to an SPE. The provisioned package carries or references sufficient authorization, provenance, integrity, quality, minimization, and de-identification information to support validation and audit.

Controlled and lighter processing paths

Where personal-level, pseudonymized, or otherwise protected data require analysis, the prepared data proceed to the Secure Processing Environment through Transfer Prepared Data to SPE [SU-5]. The SPE may receive a copied package, FHIR data linked to imaging objects, a DICOM or pathology package, controlled remote access to source-held data, or a federated execution target.

Where the requested output is non-identifying by design, such as an approved statistical response or disclosure-controlled aggregate, a lighter fulfilment path may be used without transferring personal-level data to an SPE.

The provisioned package carries or references sufficient authorization, provenance, integrity, quality, minimization, and de-identification information to support validation and audit. A Preparation / Staging Store may temporarily hold permit-bound extracts or intermediate packages but does not replace the Information Source as the authoritative source.

OMOP analytical realization

Where required by the approved purpose, structured source data may be transformed into OMOP CDM as part of permit-bound preparation or within the Secure Processing Environment. The transformation may include terminology mapping, structural mapping, data-quality validation and generation of provenance describing the source dataset, transformation process, OMOP CDM version and vocabulary versions.

The Catalogue Service may indicate whether a dataset already conforms to OMOP CDM or whether an OMOP transformation capability is available. OMOP does not replace FHIR, Bulk FHIR, DICOM, DICOMweb or other source-data provision mechanisms. In multimodal workflows, structured clinical information may be represented in OMOP while imaging remains

 Copyright © 2026: IHE International, Inc.

in DICOM and is associated through controlled pseudonyms, study identifiers, manifests or other governed references.

OMOP CDM is an optional analytical-data-model realization and is therefore not explicitly represented in the SU-DSX figures. Implementations may transform structured data to OMOP CDM at the Information Source, within a permit-bound preparation environment, at a federated analytical node, or inside the Secure Processing Environment, according to the approved authorization context.

The common pattern described here may support all use cases in Section X.4.2. Detailed endpoint behaviour, protocol bindings, manifests, status handling, errors, retries, validation rules, security requirements, and conformance requirements are specified in Volume 2. This subsection is informative and introduces no additional normative actors or transactions.

1.4.2.2 Use Case #1: Cross-Border Epidemiological Study Using IPS+

A research consortium conducts a cross-border epidemiological study of cancer incidence, stage at diagnosis, treatment patterns, comorbidities, and survival across several Member States.

1.4.2.2.1 Cross-Border Use Case Description

A research consortium conducts a cross-border epidemiological study combining population-based cancer-registry data with selected clinical information originally collected for healthcare delivery. The study may examine incidence, stage at diagnosis, treatment patterns, comorbidities, outcomes, and survival across participating Member States.

This use case illustrates the EHDS bridge between primary and secondary use while preserving their distinct governance contexts. Clinical data remain under primary-use governance when recorded or exchanged for care. Their reuse begins only after a secondary-use request has been assessed and an authorization context has been issued. IPS+ may provide an informative, harmonized content realization for selected clinical elements, but it does not replace registry, pathology, mortality, imaging, or other epidemiology-specific data.

Each Information Source remains authoritative for its original data. The DAC coordinates participating jurisdictions and sources. Permit-authorized extracts are minimized, linked, and pseudonymized as required, then delivered to an authorized SPE. Only approved anonymous and disclosure-controlled study results may leave the SPE.

1.4.2.2.2 Cross-Border Process Flow

- The SUA discovers relevant registries, EHR-derived datasets, and IPS+-enabled repositories through Query Catalogue [SU-1].
- The SUA submits a cross-border study request through Submit Secondary Use Request [SU-2], identifying the cohort, registry variables, IPS+ clinical elements, linkage needs, participating countries, intended analyses, and expected outputs.
- The DAA evaluates the request and issues the permit or access decision through Issue Permit / Access Decision [SU-3], including source, data-scope, linkage, SPE, de-identification, and release conditions.

 Copyright © 2026: IHE International, Inc.

- The DAC coordinates national authorities, Information Sources, and preparation services and preserves correlation among the common study context and national fulfilment actions.
- Each Information Source provides only permit-authorized registry and clinical data through Authorized Source Data Provision [SU-4]. IPS+ content may be provided through FHIR APIs, Bulk FHIR, document exchange, or another approved binding.
- When de-identification is required, the DAC acts as or groups with the De-Identification Requester and submits ITI-x1 Submit De-Identification Job.
- The De-ID Manager resolves policy through ITI-x2, submits tasks through ITI-x3, retrieves task output and evidence through ITI-x4 where required, and controls approved delivery through ITI-x5 or ITI-x6.
- The SPE performs the permitted cross-border epidemiological analyses and maintains traceability to the source, permit, preparation, and dataset versions.
- Export candidates undergo privacy-risk and statistical disclosure-control review.
- Only approved anonymous results are released and audited through Secure Processing and Results Release [SU-6].

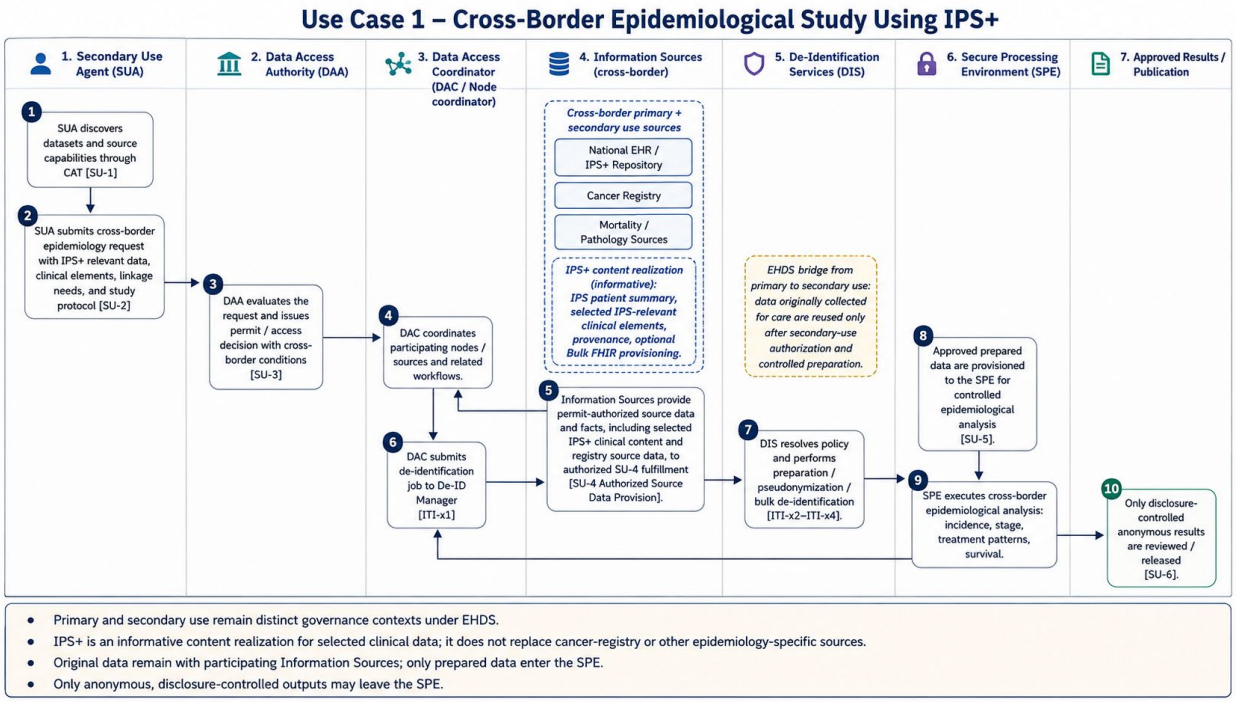


Figure 1.4.2.2.2-1: Process flow for the cross-border epidemiological study using IPS+

 Copyright © 2026: IHE International, Inc.

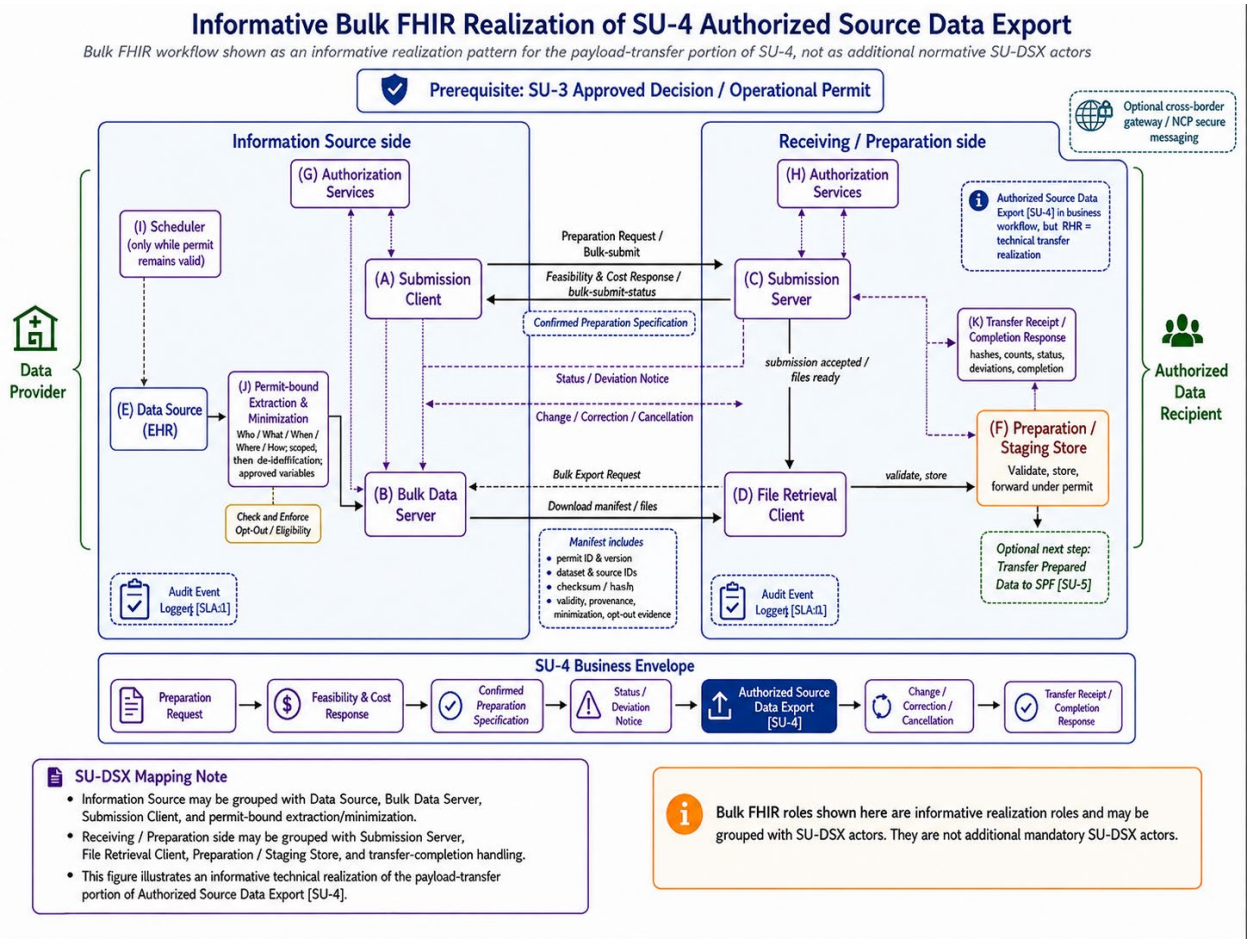


Figure 1.4.2.2.2-2: Informative IPS+ population-repository and Bulk FHIR realization of SU-4

IPS+ is an informative content realization in this use case. It supports harmonized representation of selected clinical information originally collected for care but does not replace epidemiology-specific datasets or the SU-DSX authorization, preparation, de-identification, secure-processing, and release workflow.

Structured clinical data provisioned using IPS+R, FHIR, Bulk FHIR or source-specific extracts may be transformed into OMOP CDM for harmonized cohort construction and epidemiological analysis inside the SPE. Registry-specific information not represented in the selected FHIR or IPS+R content may be mapped to appropriate OMOP domains, extension tables or linked research structures. The OMOP transformation retains provenance to the source datasets and the applicable permit.

Pre-conditions:

- A study protocol and defined epidemiological purpose exist.
- Relevant datasets and IPS+ capabilities have been described in discoverable catalogues.

 Copyright © 2026: IHE International, Inc.

- Participating authorities and Information Sources can correlate the request, permit, study, and dataset identifiers.
- A suitable SPE and de-identification workflow are available where personal-level or pseudonymized processing is required.
- IPS+ is used only for the clinical content elements covered by its profiles; additional cancer-specific content is separately identified.

Main Flow: Cross-border realization

The Secondary Use Agent discovers relevant datasets and IPS+-enabled source capabilities through national or European catalogues. The request is submitted through the appropriate DAA or HDAB workflow and may be coordinated across national contact points and participating Member States.

Each participating jurisdiction may apply its own permit, policy, preparation, and source-fulfilment responsibilities while preserving a common request and study context. The DAC coordinates fulfillment across the participating Information Sources and maintains correlation between:

- the cross-border request;
- national or joint decisions;
- participating datasets;
- IPS+ content profiles and versions;
- source-extraction manifests;
- de-identification jobs;
- SPE datasets;
- analysis jobs;
- approved results.

Cross-border interoperability is supported by using harmonized clinical definitions and content profiles, while governance and authorization remain under the applicable EHDS and national arrangements.

Post-conditions:

- The approved epidemiological dataset has been prepared and used only within the authorized environment.
- Original data remain under the control of the participating Information Sources.
- Prepared data, linkage artifacts, manifests, and processing evidence are retained or deleted according to the permit.
- Only anonymous and disclosure-controlled study outputs are released.

 Copyright © 2026: IHE International, Inc.

- Audit records correlate the request, permits, source datasets, IPS+ profile versions, de-identification actions, analysis jobs, and approved outputs.

1.4.2.3 Use Case #2: Federated Aggregate Query and Statistical Data Request

This use case represents an EHDS data request scenario.

1.4.2.3.1 Data Request Use Case Description

A public authority, statistical body, regulator, healthcare-planning organization, or authorized research sponsor requests non-identifying information from multiple Information Sources. Examples include cohort feasibility counts, prevalence or incidence summaries, service-utilization measures, laboratory or medication activity, admissions, capacity indicators, and other administrative or public-health statistics.

This use case represents an EHDS data request for anonymized statistical data rather than a data access application for personal-level records. The DAA approves the population definition, timeframe, stratifications, calculation rules, participating sources, intended recipient, and disclosure constraints. The DAC distributes the permit-bound query to participating Information Source nodes, which execute the approved computation locally.

Patient-level data remain within each Information Source. A node may use source-local Bulk FHIR to retrieve the minimum authorized FHIR resources into its local aggregation function, but record-level Bulk FHIR files are not transferred to the DAC, DAA, SUA, or requester. Each node returns only the authorized aggregate response through Authorized Source Data Provision [SU-4].

The DAC validates and, where permitted, combines the node-level results. Where the result is non-identifying by design, it is released through SU-6 without using an SPE. Where residual disclosure risk remains, the node, DAC/DAA-controlled release function, or other authorized release-control service applies the required statistical disclosure-control treatment before SU-6 release. This post-query output-control activity is not modeled as a DIS job.

1.4.2.3.2 Data Request Process Flow

- The SUA discovers relevant datasets, federated nodes, measures, and query capabilities through CAT [SU-1] and submits a structured statistical data request through SU-2.
- The DAA evaluates the request and issues the approved decision or authorization context through SU-3.
- The DAC distributes the common query definition, timeframe, stratifications, and fulfilment instructions to participating Information Source nodes.
- Each node executes the approved query locally and may use source-local Bulk FHIR for minimum cohort extraction; no record-level data leave the node.
- Each node applies local validation, aggregation, and source-level disclosure checks and returns aggregate results only through SU-4.

 Copyright © 2026: IHE International, Inc.

- The DAC validates and combines the permitted results. Outputs requiring additional disclosure control remain in the authorized release-control process until the required suppression, generalization, thresholding, rare-category handling, validation, or other treatment is completed.
- Only approved aggregate or statistical results are released through SU-6, with request, permit, node, query, disclosure-control, and release identifiers correlated in the audit trail.

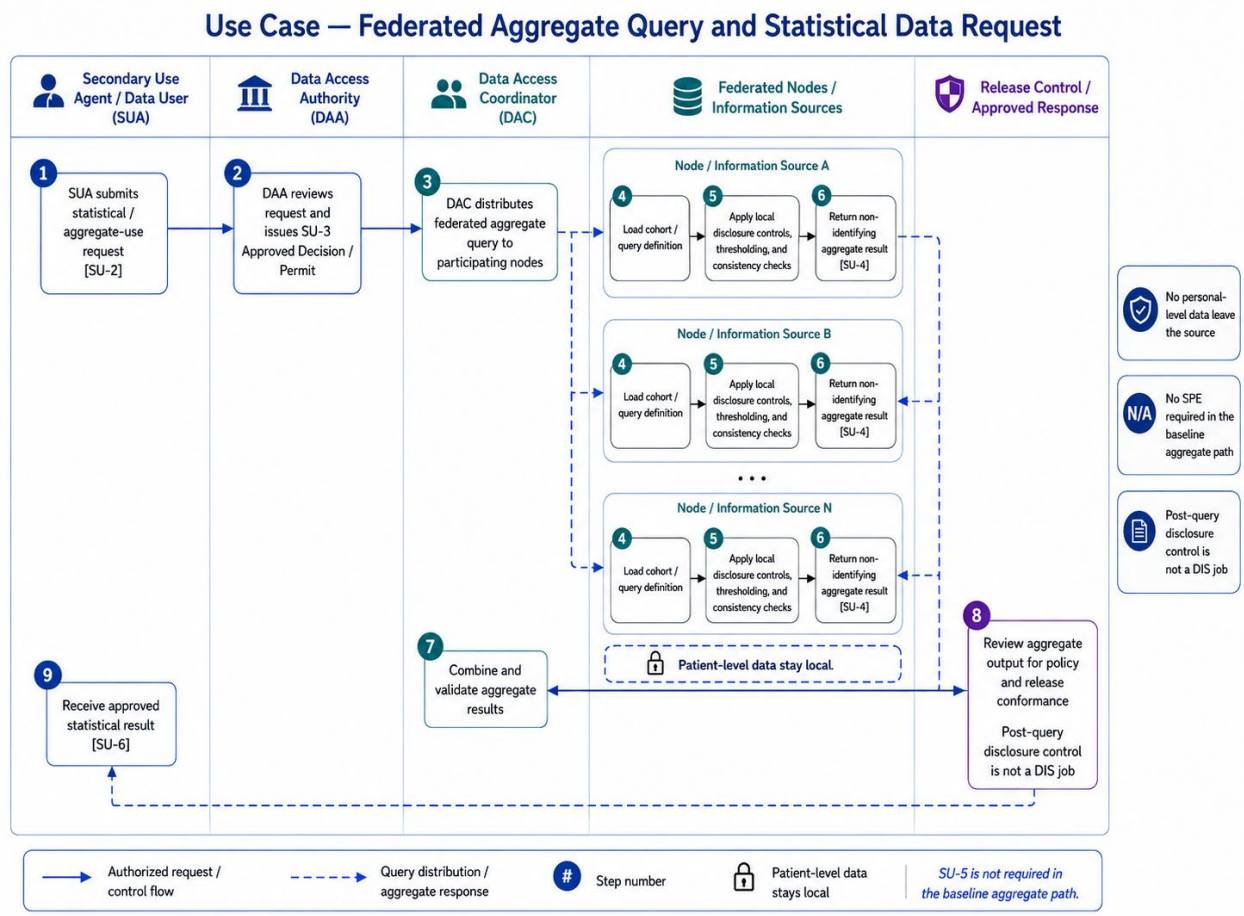


Figure 1.4.2.3.2-1: Process flow for the federated aggregate query and statistical data request

Pre-conditions:

- The requester is authorized to submit the relevant statistical or administrative data request.
- Relevant datasets, federated-query capabilities, and available measures are discoverable through CAT.
- A common query or calculation definition has been established.
- Participating Information Sources can execute the approved query locally.

 Copyright © 2026: IHE International, Inc.

- The expected result can be satisfied using non-identifying aggregate data.
- Disclosure thresholds and release rules are defined before execution.
- Where Bulk FHIR is used locally, the Information Source can constrain the export to the authorized cohort, resources, and period.

Main Flow: Federated Analysis Model

The federated analysis consists of three logical stages:

1. Common query definition: The DAC distributes a permit-bound query specification containing common cohort definitions, calculation rules, coding systems, time periods, stratification rules, and required output structure.
2. Local execution: Each Information Source executes the query against its local authoritative data. Local processing may include cohort selection, source normalization, calculation of indicators, aggregation, and source-level disclosure checks.
3. Aggregate combination and release: The DAC or an authorized aggregation function validates and combines the returned node-level results. Only the approved non-identifying aggregate package is released to the requester.

Participating nodes are multiple deployments of the Information Source actor. They are not additional normative SU-DSX actors. The federated query may be realized using one or more appropriate query or reporting patterns, including:

- profiled FHIR aggregate-query operations;
- QEDm-oriented aggregate-query capabilities;
- mADX-style aggregate reporting;
- Measure and MeasureReport-based reporting;
- jurisdiction-specific statistical-query services;
- local Bulk FHIR extraction followed by source-side aggregation.

Participating nodes may expose locally governed OMOP CDM environments. A common permit-bound cohort definition, concept set or analytical package may be distributed to the participating nodes. Each node executes the approved analysis locally and returns only the authorized aggregate result. Person-level OMOP records remain within the node-controlled boundary. Returned outputs are subject to the applicable disclosure-control policy before combination or release.

These realizations are informative cross-profile bindings. SU-DSX provides the governance, authorization, coordination, traceability, and approved-release workflow.

Post-conditions:

- Personal-level and pseudonymized data remain within the participating Information Sources.
- No central patient-level dataset has been created.

 Copyright © 2026: IHE International, Inc.

- No personal-level or pseudonymized data have been transferred to the requester.
- The SPE has not been invoked.
- Only approved non-identifying aggregate results have been released.
- Any suppressed, generalized, or rejected results are documented.
- Query, source, Bulk FHIR, aggregation, disclosure-control, and release identifiers are correlated in the audit record.
- The final result and associated publication or reporting obligations are communicated to the governing authority where required.

1.4.2.4 Use Case #3: Multimodal AI/ML Method Development and Validation

This use case represents an EHDS data access scenario because the researchers require access to personal-level or pseudonymized data rather than an anonymized statistical result.

1.4.2.4.1 Data Access Use Case Description

An AI/ML consortium develops or validates cancer models using multimodal data such as structured clinical information, radiology, digital pathology, laboratory data, genomics where applicable, annotations, and outcomes. This is a data access application because the work requires personal-level or pseudonymized data rather than only an anonymous statistical result.

The permit identifies the approved cohort, modalities, linkage requirements, data elements, tools, compute resources, SPE, validation plan, de-identification stages, and classes of exportable artifacts. FHIR Bulk Data may provide an informative realization of SU-4 for large structured FHIR datasets. Imaging and whole-slide pathology normally use DICOM, DICOMweb, or another approved native-format mechanism. FHIR Bulk Data does not replace modality-specific transport or perform de-identification.

DIS is used for input preparation within the SU-DSX workflow. An input-preparation job creates and validates a training-ready pseudonymized or otherwise appropriately de-identified multimodal dataset and delivers it to the SPE. Export candidates produced later by AI/ML processing are governed by the SU-6 output-review and release process rather than by a second DIS job.

1.4.2.4.2 Data Access Process Flow

The SUA discovers relevant datasets, federated nodes, measures, and query capabilities through CAT [SU-1] and submits a structured statistical data request through SU-2.

The DAA evaluates the request and issues the approved decision or authorization context through SU-3.

The DAC distributes the common query definition, timeframe, stratifications, and fulfilment instructions to participating Information Source nodes.

Each node executes the approved query locally and may use source-local Bulk FHIR for minimum cohort extraction; no record-level data leave the node.

 Copyright © 2026: IHE International, Inc.

Each node applies local validation, aggregation, and source-level disclosure checks and returns aggregate results only through SU-4.

The DAC validates and combines the permitted results. Outputs requiring additional disclosure control remain in the authorized release-control process until the required suppression, generalization, thresholding, rare-category handling, validation, or other treatment is completed.

Only approved aggregate or statistical results are released through SU-6, with request, permit, node, query, disclosure-control, and release identifiers correlated in the audit trail.

The SUA discovers eligible multimodal datasets, source capabilities, FHIR Bulk endpoints, imaging repositories, and access conditions through SU-1.

The SUA submits a structured data access application through SU-2 describing the cohort, modalities, linkage, approved toolchain, compute requirements, validation methodology, and expected export artifacts.

The DAA evaluates the application and issues the permit or access decision through SU-3.

The DAC coordinates permit-authorized source provision through SU-4. Structured FHIR data may use Bulk FHIR; DICOM, documents, pathology, genomics, and other payloads use approved modality-specific bindings.

The DAC submits an input-preparation job through ITI-x1. The De-ID Manager resolves policy through ITI-x2, submits payload-specific tasks through ITI-x3, and retrieves task outputs and evidence through ITI-x4 where required.

The De-Identifier performs the assigned transformations and validation, including preservation of approved cross-modal linkage and FHIR referential integrity.

The De-ID Manager controls approved delivery to the SPE through ITI-x5 or ITI-x6, realizing Prepared Data Delivery to SPE [SU-5].

Training, tuning, validation, bias assessment, robustness testing, and explainability analysis occur inside the SPE.

When an export candidate is proposed, the SPE or authorized user initiates the SU-6 output-release process. The DAC, DAA, or other authorized release-control function coordinates the required disclosure, privacy, scientific, administrative, or artifact-specific review.

Only approved non-identifying model artifacts, synthetic outputs, metrics, or reports are released and audited through SU-6.

 Copyright © 2026: IHE International, Inc.

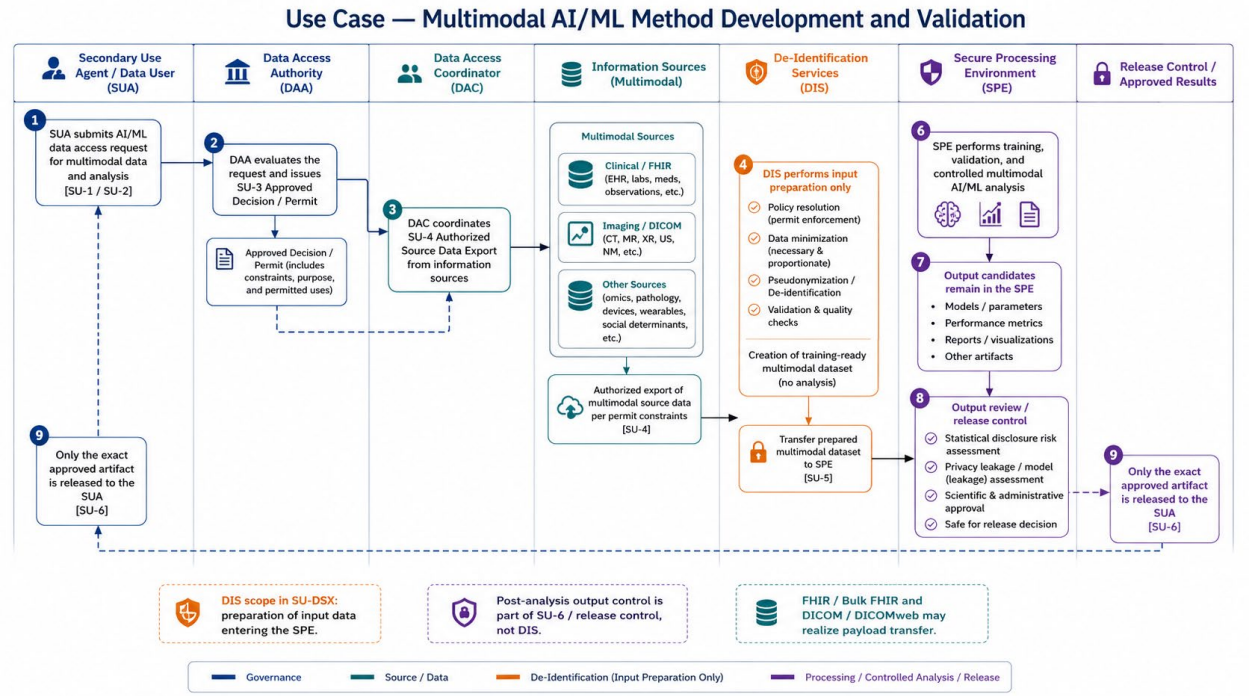


Figure 1.4.2.4.2-1: Process flow for multimodal AI/ML method development and validation

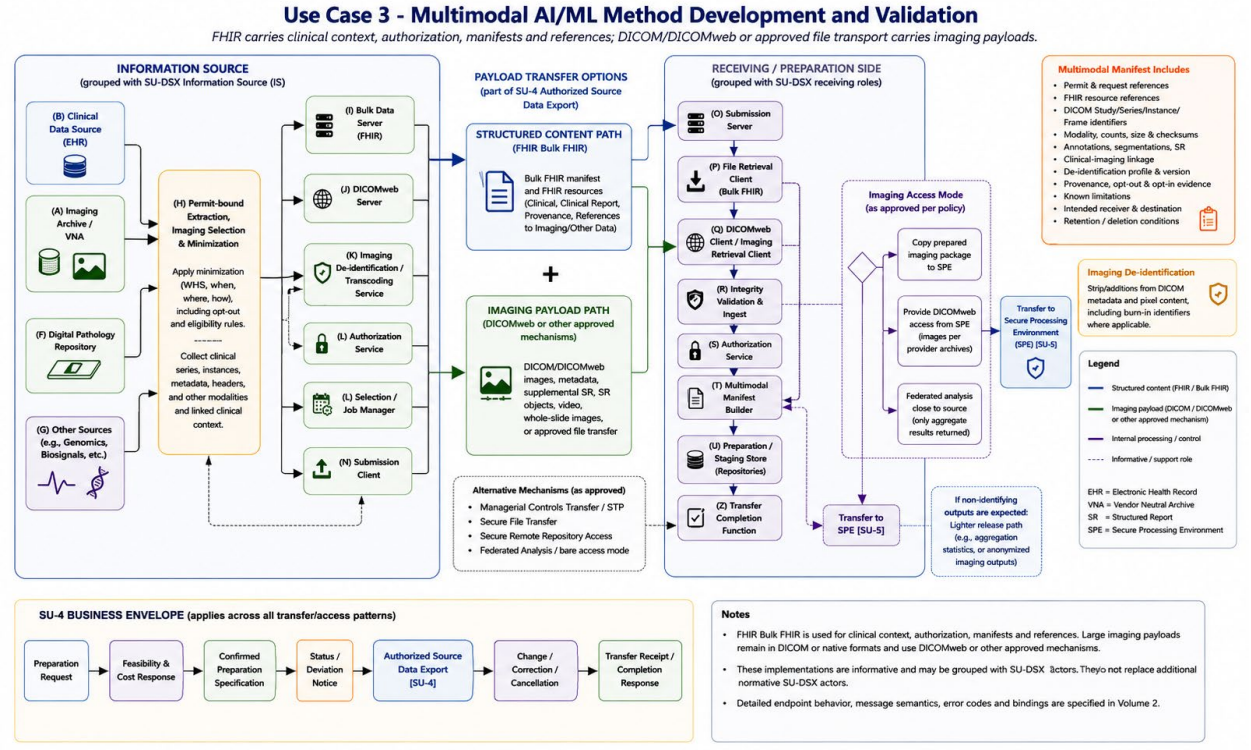


Figure 1.4.2.4.2-2: Informative FHIR, Bulk FHIR, and imaging realization of SU-4 and SU-5

 Copyright © 2026: IHE International, Inc.

The modality-specific imaging de-identification and transcoding component shown in Figure 1.4.2.3-2 is an implementation capability grouped with, or invoked by, the DIS De-Identifier. It is not an additional normative DIS actor. The complete input-preparation, controlled-processing, output-control, and results-release lifecycle is shown in Figure 1.4.2.3-1.

This use case represents a data access application involving personal-level or pseudonymized multimodal data. FHIR Bulk Data is an informative realization of SU-4 for structured FHIR resources; other modalities use appropriate bindings such as DICOMweb or governed document and file exchange. DIS is used both to prepare training-ready input data and, where required, to assess and transform model artifacts or other export candidates. Only approved non-identifying outputs may leave the SPE.

Structured clinical, treatment, laboratory and outcome data may be transformed into OMOP CDM to support cohort construction, feature engineering and reproducible model evaluation. Radiology and digital-pathology pixel data remain in DICOM or another approved native format. OMOP may contain imaging procedures, derived measurements, image-derived features and governed references to the corresponding imaging objects, but it does not replace the imaging repository or store the complete image content.

Pre-conditions:

- A defined AI/ML research or innovation purpose and protocol exist.
- The requested use requires personal-level or pseudonymized data and is processed as a data access application.
- The relevant Information Sources and data modalities have been identified.
- The permit identifies an authorized SPE and permitted processing environment.
- Approved transport and payload bindings exist for each modality.
- The DIS actors can resolve and execute the required FHIR and DICOM de-identification policies.
- The SPE supports the authorized tools, compute resources, monitoring, and export-control workflow.

Main Flow: Analysis-Output Review and Controlled Release

AI/ML export candidates may retain information about the training population even when they are not conventional patient records. Examples include model weights, checkpoints, embeddings, synthetic datasets, predictions, saliency maps, detailed subgroup metrics, validation reports, and source examples.

Post-analysis output control is not modeled as a DIS de-identification job by SU-DSX. The required review and treatment are performed within the authorized SU-6 release-control process.

1. The SPE creates an Output Release Request identifying the permit, source datasets, processing runs, model version, proposed recipient, requested artifact, intended purpose, and justification for release.

 Copyright © 2026: IHE International, Inc.

2. The Output Release Request is submitted through SU-6 to the DAC, DAA, or other authorized Release Coordinator. No new DIS job is created for the post-analysis artifact.
3. The Release Coordinator verifies the effective permit, recipient, output class, requested use, release channel, and required review route.
4. The candidate is assessed according to the applicable release policy and artifact type. Review may include statistical disclosure control, model memorization or membership-inference testing, reconstruction/leakage assessment, synthetic-data privacy risk, rare-subgroup or small-cell risk, scientific/quality/safety review, or administrative approval.
5. Where additional transformation is required, the candidate remains controlled until the authorized treatment and validation are completed. The resulting artifact receives a new identifier, version, and hash.
6. Only an artifact that satisfies the policy-defined acceptance criteria is approved for release.
7. The exact approved artifact is delivered through SU-6 to the authorized recipient using the approved channel.
8. The release decision, delivery status, receiver acknowledgement, and applicable publication or reporting obligations are recorded through SU-6 and SU-A1 audit.
9. DIS identifiers may be retained as provenance of input preparation, but they do not constitute the post-analysis release decision.

Post-conditions:

- Only permit-authorized and minimized source data have been provisioned.
- Training-ready data have been transformed, validated, and delivered to the authorized SPE.
- Personal-level and pseudonymized data remain inside the controlled environment.
- All training, validation, and output-processing actions are traceable.
- Export candidates have undergone a separate governed release assessment when required.
- Only approved non-identifying outputs have been released.
- Request, permit, FHIR Bulk, DIS, SPE, model, and release identifiers are correlated in the audit trail.

1.4.2.4 QRPH-Aligned Output Summary

Table X.4.2.4-1 summarizes how the three use cases may be enhanced with QRPH-aligned outputs while remaining within the SU-DSX workflow model.

Use Case	Primary SU-DSX Output	Optional QRPH-Aligned Output	Release Constraint
Epidemiological Study	Permit, extraction manifest, prepared-data delivery to the SPE, and approved	CRPC-style protocol package; DEX data-element package; RPE execution	Only approved anonymous, disclosure-controlled study outputs

 Copyright © 2026: IHE International, Inc.

Use Case	Primary SU-DSX Output	Optional QRPH-Aligned Output	Release Constraint
	study-output package.	definition; ADX/mADX aggregate reporting package.	may leave the SPE through SU-6.
Federated Aggregate Query and Statistical Data Request	Approved query definition, node-level aggregate responses, combined aggregate result, and release record.	ADX/mADX; FHIR Measure/MeasureReport; profiled QEDm aggregate-query definition where applicable.	No record-level data leave participating nodes. Residual disclosure risk is handled by statistical disclosure-control and SU-6 release control; no post-query DIS job is used.
AI/ML Method Development and Validation	Permit, training/validation execution package, approved evaluation report, and approved export package.	CRPC protocol package; DEX feature catalogue; RPE benchmark definition; SDC annotation forms where needed.	Only the exact artifact approved by the SU-6 release decision may leave the SPE.

1.5 SU-DSX Security Considerations

SU-DSX coordinates sensitive requests, governance decisions, de-identification steps, provisioning events, secure processing, and release of results. The profile addresses risks including unauthorized request submission, substitution or replay of permits, over-disclosure of source data, misuse of prepared data, leakage of outputs, and incomplete audit trails.

Where the approved purpose can be fulfilled by non-identifying aggregate or statistical results, SU-DSX may use the lightweight path without provision of personal-level data to the requester or transfer to an SPE. Where personal-level or pseudonymized data are required, SU-DSX shall use an SPE for controlled processing. Output release in both cases is governed by SU-6 and the applicable disclosure/privacy review requirements.

When DIS is used for input preparation, traceability shall cover authorization, policy resolution, task execution, validation, prepared-dataset references, receiver binding, and delivery to the authorized processing environment. Post-analysis SU-6 traceability shall separately cover the processing job, output candidate, disclosure/privacy review, release decision, exact approved artifact, recipient, delivery status, and release evidence.

1.5.1 Audit Considerations

- Audit events should correlate request identifiers, permit identifiers, policy identifiers, dataset references, transformation runs, manifests, analysis jobs, and release decisions.
- Audit records should be sufficient to reconstruct who accessed what, under which authority, for which purpose, and with which output or release path.
- Release of anonymized datasets, aggregate reports, model artifacts, and other non-tabular outputs should be auditable as first-class events.

1.6 SU-DSX Cross Profile Considerations

DIS – De-Identification Services. SU-DSX reuses the DIS core actor model and candidate transactions for authorization-backed input-preparation job submission, policy resolution, de-

 Copyright © 2026: IHE International, Inc.

identification task execution, task-output retrieval, validation/evidence, and approved pull or push delivery of the prepared de-identified dataset to the authorized processing environment. SU-DSX does not require post-analysis output-control activities to be implemented as DIS jobs.

Aggregate reporting and federated query. mADX-style reporting, FHIR Measure/MeasureReport, or profiled QEDm aggregate-query support may be appropriate where the approved output is non-identifying by design. Residual small-cell, rare-category, institutional, professional, or regulatory disclosure risk is handled through the applicable statistical disclosure-control and SU-6 release-control process. An SPE is required only if personal-level or otherwise protected processing is introduced, which is outside the baseline federated aggregate-query realization.

PCC-1, QEDm, and Bulk FHIR. The SUA may be informatively grouped with a PCC Content Consumer, QEDm Clinical Data Consumer, or Bulk FHIR-oriented client / submission client. The IS may be informatively grouped with a PCC Content Creator, QEDm Clinical Data Source, De-Identified Clinical Information Source, or Bulk FHIR-oriented server / bulk data download server. These are candidate realization patterns, not mandatory SU-DSX actors.

ATNA, Consistent Time, identity, authorization, and document exchange. SU-DSX implementations may reuse ATNA, CT, IUA/XUA, OAuth2/OIDC-based infrastructure, MHD, XDS, XCA, XDR, and other appropriate profiles to protect communications, convey claims, correlate audit events, and exchange permits, manifests, evidence, or result packages.

OMOP CDM is an external analytical data model maintained by the OHDSI community. SU-DSX does not constrain a specific OMOP CDM version, vocabulary release, ETL (Extract, Transform, Load) implementation or analytical tool. Implementations claiming an OMOP realization should record the OMOP CDM version, vocabulary versions, source-to-concept mappings, ETL provenance and validation results.

OMOP conformity is an implementation characteristic of a dataset or analytical environment and does not represent an IHE actor grouping. Transport, authorization, de-identification, identity, audit and controlled-release requirements remain governed by the applicable SU-DSX and referenced IHE transactions.

 Copyright © 2026: IHE International, Inc.

Appendices to Volume 1

 Copyright © 2026: IHE International, Inc.

Appendix A – Mapping to EHDS-oriented Terminology

This appendix is informative and maps SU-DSX technical actors to illustrative EHDS organizational or deployment roles.

SU-DSX Actor	Illustrative EHDS-aligned interpretation
Secondary Use Agent (SUA)	Data user-side system or delegated requester/orchestration service
Catalogue Service (CAT)	National or EU-level dataset catalogue service
Data Access Authority (DAA)	HDAB decision and permit-management function
Data Access Coordinator (DAC)	HDAB operational fulfillment coordinator; normally grouped as DIS De-Identification Requester
Information Source (IS)	Health data holder system or authorized source endpoint; grouped as Data Source (Original) when DIS reads from it
De-ID Manager	HDAB-governed or delegated orchestration service for input-preparation de-identification and delivery of the prepared dataset
De-ID Policy Authority	HDAB-governed or delegated de-identification policy-resolution service
De-Identifier	Permit-bound pseudonymization, de-identification, content transformation, validation, and preparation of evidence for data entering the authorized secondary-use environment
Secure Processing Environment (SPE)	HDAB-operated or delegated secure processing environment; grouped as the DIS De-Identified Data Receiver when it receives prepared de-identified data from the DIS input-preparation workflow

 Copyright © 2026: IHE International, Inc.

Volume 2 – Transactions

This volume uses the actor responsibilities and transaction boundaries established in SU-DSX Volume 1. It adopts a FHIR R4 message-based control plane for request, decision, fulfillment, delivery, processing, and release coordination, while retaining technology-neutral payload transfer and the optional content/transport realizations identified in Volume 1.

HealthDCAT-AP is specified as an optional catalogue metadata content binding, and OMOP CDM is specified as an optional analytical representation rather than a universal exchange format. The DIS transaction identifiers ITI-x1 through ITI-x6 and any new canonical URLs or code-system identifiers remain provisional until assigned through the IHE publication process.

Normative language: "shall" and "shall not" identify conformance requirements. "Should" identifies recommended behavior. "May" identifies permitted behavior.

3.1 Query Catalogue [SU-1]

3.1.1 Scope

This transaction enables a Secondary Use Agent to search one or more Catalogue Service actors for dataset and service metadata sufficient to identify candidate data, understand access conditions, and prepare a secondary-use request. The transaction exchanges metadata only; it does not provide record-level health data or grant access.

Publication, update, withdrawal, validation and harvesting of catalogue metadata are outside the normative scope of Query Catalogue [SU-1]. A Catalogue Service claiming an EHDS-oriented deployment shall be populated and maintained through a HealthDCAT-AP-compatible publication or harvesting mechanism. Such a mechanism may be implemented internally or through grouping with an applicable catalogue-publication profile.

3.1.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

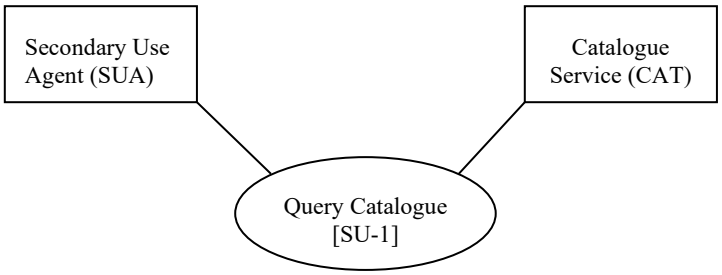


Figure 3.1.2-1: Use Case Diagram

 Copyright © 2026: IHE International, Inc.

Table 3.1.2-1: Actor Roles

Actor:	Secondary Use Agent (SUA)
Role:	Catalogue Requester: SUA formulates the discovery criteria, requests catalogue metadata, and correlates returned records with a prospective secondary-use request
Actor:	Catalogue Service (CAT)
Role:	Catalogue Provider: CAT searches its published metadata and returns matching dataset, distribution, service, quality, provenance, and access-condition descriptions.

3.1.3 Referenced Standards

- IETF RFC 9110, HTTP Semantics, for HTTP methods, representations, status codes, media types, and content negotiation. Implementations shall use Accept and Content-Type consistently with the supported metadata representations.
- W3C RDF 1.1, as the graph-based metadata model.
- W3C JSON-LD 1.1, as a JSON-based RDF serialization. Implementations may support additional RDF serializations, such as Turtle, RDF/XML, N-Triples, or TriG, and shall advertise the supported representations.
- W3C Data Catalog Vocabulary, DCAT 3, and an applicable jurisdictional or domain-specific DCAT application profile.
- HealthDCAT-AP, for implementations claiming the SU-DSX HealthDCAT-AP Content Binding. Such implementations shall conform to the declared published HealthDCAT-AP release. This specification has been validated against HealthDCAT-AP (https://healthdataeu.pages.code.europa.eu/healthdcat-ap/releases/release-7/ Release 7, May 2026). A CAT claiming a named DCAT application profile shall validate published metadata against the applicable profile constraints. Where the profile provides SHACL shapes or an equivalent validation mechanism, the CAT should expose the validation status or validation report reference.
- W3C SPARQL 1.1 Query Language and SPARQL 1.1 Protocol, when the Catalogue Service exposes a SPARQL endpoint. A Catalogue Service exposing such an endpoint should also publish a SPARQL Service Description.
- IHE Audit Trail and Node Authentication (ATNA) and IHE Consistent Time (CT), as required by the SU-DSX security and audit provisions or applicable deployment policy.

Catalogue-profile independence: SU-DSX does not require one jurisdictional catalogue application profile for all deployments. A Catalogue Service may support any declared DCAT-based application profile that satisfies the transaction's minimum discovery requirements.

A Catalogue Service claiming the HealthDCAT-AP Content Binding shall:

- identify the supported HealthDCAT-AP release;
- conform to the applicable profile constraints and controlled vocabularies;

 Copyright © 2026: IHE International, Inc.

- identify the supported RDF serialization or serializations;
- advertise the supported media types and query capabilities in endpoint metadata;
- return the applicable profile and version information in catalogue responses or associated conformance metadata; and
- preserve the semantics and cardinality constraints of the declared HealthDCAT-AP release.

A Catalogue Service not claiming the HealthDCAT-AP Content Binding may use another DCAT-based application profile. In that case, HealthDCAT-AP remains an informative EHDS-oriented example and no HealthDCAT-AP conformance claim shall be made.

3.1.4 Messages

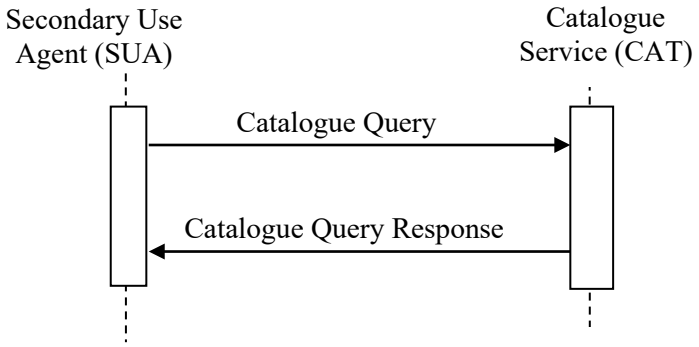


Figure 3.1.4-1: Interaction Diagram

3.1.4.1 Catalogue Query

The Catalogue Query conveys structured discovery criteria to a Catalogue Service using an HTTP GET, HTTP POST, or SPARQL query appropriate to the endpoint advertised by the Catalogue Service.

3.1.4.1.1 Trigger Events

A person or automated function acting through the SUA begins dataset discovery or refines a previous search. The SUA needs updated metadata before preparing, amending, or resubmitting a secondary-use request.

3.1.4.1.2 Message Semantics

The SUA shall address the query to a CAT endpoint whose supported query syntax and content profile are known through configuration or endpoint metadata. The query may use free text, identifiers, controlled terms, filters, or graph patterns.

The query shall support paging or another bounded result mechanism. The SUA may query multiple CAT actors; each interaction is independently correlated.

 Copyright © 2026: IHE International, Inc.

Table 3.1.4.1-1: Catalogue Query Parameters

Parameter	Requirement and meaning
Search expression	Free text, controlled terms, or graph pattern expressing the information need.
Dataset / service identifier	Optional stable identifier used to retrieve a known record or version.
Topic and data category	Clinical, registry, imaging, laboratory, genomic, administrative, public-health, or other applicable category.
Population and coverage	Optional population, geographic, organizational, and temporal criteria.
Format / capability	Optional FHIR, Bulk FHIR, DICOMweb, OMOP CDM, document, aggregate-query, SPE, native-model, transformation-service, or other advertised capability.
Access conditions	Optional filters for eligibility, permitted purpose, request path, jurisdiction, or other published access condition.
Paging and sort	Page size, continuation token or offset, and requested sort order.
Response format	Requested RDF serialization, including JSON-LD where supported.

3.1.4.1.3 Expected Actions

The CAT shall validate the query syntax and any required authorization. It shall execute the query against the metadata records visible to the requester and return either a result set or a standards-conformant error response.

The CAT shall not infer that a discovery request constitutes a data-access authorization.

3.1.4.2 Catalogue Query Response

The Catalogue Query Response returns the matching catalogue records, paging information, and any warnings or errors needed by the SUA to interpret the result.

3.1.4.2.1 Trigger Events

The CAT completes a valid catalogue query.

The CAT detects an invalid, unauthorized, or unsupported query.

3.1.4.2.2 Message Semantics

A successful response shall contain metadata conforming to the DCAT application profile advertised by the CAT. The response shall identify the profile and version used. Each record shall have a stable identifier and shall identify its version or modification date when versioning is supported.

At minimum, a returned record shall provide enough information to identify the dataset or service, understand its subject and coverage, identify the publisher or responsible organization,

 Copyright © 2026: IHE International, Inc.

locate available distributions or service endpoints, and understand the published access route and conditions.

The response may contain quality and utility information, provenance, update frequency, coding-system information, links to data dictionaries or variable-level metadata, and conformance statements for supported exchange or analytical models. It should distinguish native conformance from a transformation capability available on request. The response shall not expose personal or confidential record-level data.

Table 3.1.4.2-1: Minimum Catalogue Response Content

Element	Minimum semantics
Record identity	Persistent dataset or service identifier, record identifier, and version / modification time.
Description	Title, summary, keywords, topic, purpose, and known limitations.
Coverage	Population, geographic, organizational, and temporal coverage where known.
Publisher / contact	Responsible data holder, catalogue publisher, and contact route.
Distribution / service	Available formats, endpoints, access services, technical capabilities, and supported source-data or analytical representations.
Access conditions	Published eligibility, request procedure, permitted-use constraints, and links to application information.
Provenance and quality	Origin, update history, quality or utility labels, known data-quality limitations, and data-dictionary or variable-description references where available.
Conformance and transformation capability	Standards or model references, including applicable versions, using dct:conformsTo or the equivalent property of the advertised profile. Examples include FHIR implementation guides, OMOP CDM, and CDISC. The record should state whether conformance is native or available through a transformation service.

3.1.4.2.3 Expected Actions

The SUA shall preserve the identifiers and versions of metadata records used to prepare the request.

For a paged response, the SUA shall use only the continuation mechanism returned by the CAT and shall not assume stable ordering across independent queries.

On an error response, the SUA shall present or log the error and may reformulate the query.

3.1.5 Security Considerations

Public catalogue metadata may be exposed without user authentication when permitted. Restricted or pre-publication metadata shall be protected using the deployment's identity and authorization infrastructure.

 Copyright © 2026: IHE International, Inc.

The CAT shall validate input to prevent query injection, resource exhaustion, unauthorized graph traversal, and unintended disclosure through error messages or result counts.

3.1.5.1 Security Audit Considerations

Where catalogue access is auditable, the CAT shall record the requester identity when known, query time, endpoint, outcome, and a minimized representation or hash of the query. Search terms that could reveal sensitive project information should not be copied verbatim into a widely accessible audit repository.

3.1.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Secondary Use Agent	Protect credentials and avoid including personal data in discovery terms.
Catalogue Service	Apply metadata visibility rules, rate limits, input validation, and result minimization.

3.2 Submit Secondary Use Request [SU-2]

3.2.1 Scope

This transaction enables a Secondary Use Agent to submit a structured secondary-use request to a Data Access Authority and to receive a technical and administrative acknowledgement. It supports both a data access application for personal-level or pseudonymized data and a data request for anonymized statistical data.

3.2.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

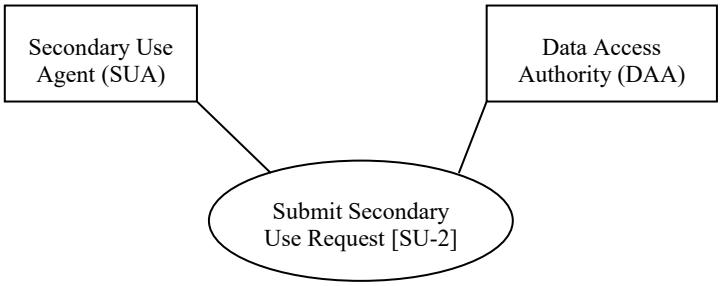


Figure 3.2.2-1: Use Case Diagram

 Copyright © 2026: IHE International, Inc.

Table 3.2.2-1: Actor Roles

Actor:	Secondary Use Agent (SUA)
Role:	Request Submitter: constructs, signs where required, submits, and versions the secondary-use request and supporting artifacts.
Actor:	Data Access Authority (DAA)
Role:	Request Receiver: receives the request, validates its structure and completeness, assigns or confirms the authoritative request identifier, and initiates the applicable review workflow.

3.2.3 Referenced Standards

- HL7 FHIR R4 RESTful exchange and FHIR messaging using a Bundle of type message.
- FHIR MessageHeader, Task, QuestionnaireResponse, ResearchStudy, PlanDefinition, DocumentReference, Binary, Provenance, Organization, PractitionerRole, and Consent where applicable.
- FHIR OperationOutcome for technical or validation errors.
- IHE IUA or XUA and OAuth 2.0 / OpenID Connect infrastructure as selected by the deployment.
- IHE ATNA and Consistent Time.

3.2.4 Messages

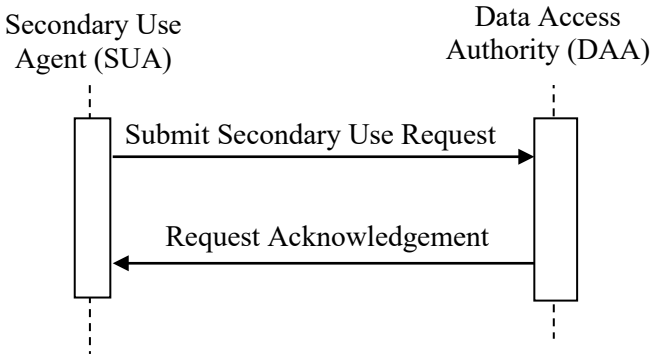


Figure 3.2.4-2: Interaction Diagram

3.2.4.1 Submit Secondary Use Request

The Submit Secondary Use Request message conveys the application, its structured data, and any supporting documents in a FHIR message Bundle.

 Copyright © 2026: IHE International, Inc.

3.2.4.1.1 Trigger Events

The applicant completes the required application or data-request information and instructs the SUA to submit it.

The applicant submits a corrected or versioned request in response to a prior request for additional information.

3.2.4.1.2 Message Semantics

The message shall be a FHIR Bundle of type message. The MessageHeader shall identify the SU-2 submission event and shall reference a Task representing the authoritative workflow instance.

The Task shall carry the request identifier and business status. Structured application answers should be represented in one or more QuestionnaireResponse resources. ResearchStudy, PlanDefinition, Group, and other resources may be included when they improve computability. Supporting documents shall be referenced using DocumentReference and Binary or an approved document-sharing profile. Provenance shall identify the submitter and time of submission.

Where appropriate to the approved purpose, the request may identify an analytical representation such as OMOP CDM and may express variable, cohort, or minimization criteria using OMOP domains, concept identifiers, concept sets, descendant rules, observation periods, temporal relationships, and exclusion criteria. Such expressions supplement rather than replace the authoritative human-readable application and catalogue references.

The request shall be self-consistent: all referenced catalogue identifiers, attachments, organizations, persons, and endpoints shall either be present in the Bundle or resolvable using authorized references.

Table 3.2.4.1-1: Required Request Semantics

Element group	Required meaning
Request identity	Globally unique request identifier, request version, creation time, and previous-version reference when amended.
Request type	Data access application or anonymized statistical data request.
Applicant	Applicant organization, authorized representative, contact person, and identity / assurance information.
Purpose and project	Permitted-purpose category, project title, public summary, scientific or operational objective, protocol, and expected public-interest contribution.
Requested data	Catalogue record identifiers, datasets, variables, records, modalities, cohort criteria, time period, geography, source organizations, and, where appropriate, OMOP domains, concept identifiers, concept sets, descendant rules, observation periods, temporal relationships, and exclusions.
Linkage and combination	Requested linkage, other data to be combined, linkage keys or strategy, and cross-border coordination needs.

 Copyright © 2026: IHE International, Inc.

Element group	Required meaning
Methods and environment	Analysis plan, tools, compute needs, SPE requirements, federated-query approach, reproducibility information, and any requested analytical representation, CDM version, vocabulary release, or transformation capability.
Data protection and safeguards	Minimization rationale, de-identification expectations, security measures, retention, deletion, and incident contacts.
Expected outputs	Expected reports, aggregates, model artifacts, synthetic outputs, publication plan, and requested release classes.
Supporting artifacts	Protocol, ethics or regulatory documents, data-management plan, contracts, declarations, and other required attachments.

3.2.4.1.3 Expected Actions

The DAA shall authenticate the submitter, validate the message structure, detect duplicates or replay, and assign the received timestamp.

The DAA shall not treat technical acceptance as approval of the request. If the request is syntactically valid but incomplete, the DAA may accept it into a pre-screening state and identify missing information in the acknowledgement.

The DAA shall preserve the original submitted version and establish version linkage for later amendments.

3.2.4.2 Request Acknowledgement

The Request Acknowledgement confirms receipt and reports the initial technical or administrative disposition without granting data access

3.2.4.2.1 Trigger Events

The DAA completes initial authentication, syntax validation, duplicate detection, and minimum completeness checks.

3.2.4.2.2 Message Semantics

The acknowledgement shall reference the submitted request identifier and version. It shall report one of the following dispositions: received, received-incomplete, duplicate, rejected-technical, rejected-unauthorized, or unsupported.

A FHIR Task shall represent the DAA-side workflow state. An OperationOutcome shall be included when there are errors or warnings. The acknowledgement may include the DAA-assigned case number, expected next step, due date, fee information, and a secure route for providing additional information.

 Copyright © 2026: IHE International, Inc.

Table 3.2.4.2-1: Acknowledgement Dispositions

Disposition	Meaning
received	Message accepted and entered into the DAA workflow.
received-incomplete	Message accepted for pre-screening but additional information is required.
duplicate	A submission with the same idempotency key or request version already exists.
rejected-technical	Message cannot be processed because of syntax, profile, reference, or transport errors.
rejected-unauthorized	The submitting identity is not authorized to create or amend the request.
unsupported	The requested transaction version, content profile, or submission channel is not supported.

3.2.4.2.3 Expected Actions

The SUA shall correlate the acknowledgement with the submitted version and shall not infer approval from a received status.

For received-incomplete, the SUA shall present the missing or invalid elements and may submit a new version. For a duplicate acknowledgement, the SUA shall continue using the authoritative request identifier returned by the DAA.

3.2.5 Security Considerations

The request may contain confidential project information, personal contact details, security plans, and commercially sensitive supporting documents. The complete message shall be protected in transit and at rest.

The DAA shall bind the authenticated identity and organization to the submission and shall preserve integrity evidence for the submitted version. Digital signatures may be required by jurisdictional policy.

3.2.5.1 Security Audit Considerations

The SUA and DAA shall record request submission, acknowledgement, version, outcome, and correlation identifiers. Audit content shall identify the transaction and request but should not duplicate the complete application or attachments.

3.2.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Secondary Use Agent	Prevent unauthorized use of applicant credentials and preserve submitted versions.
Data Access Authority	Validate sender authority, protect application confidentiality, detect replay, and preserve evidentiary integrity.

 Copyright © 2026: IHE International, Inc.

3.3 Issue Permit / Access Decision [SU-3]

3.3.1 Scope

This transaction communicates the authoritative result of request assessment. It supports approval, partial approval, denial, requests for amendment or information, suspension, revocation, expiry, and replacement of a previous permit or access decision. A decision may be delivered to the SUA, DAC, and one or more Information Sources according to their operational need.

3.3.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

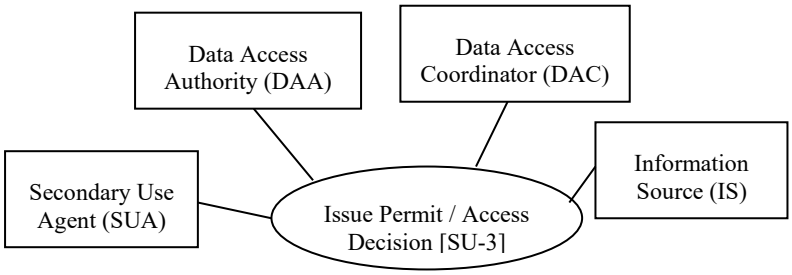


Figure 3.3.2-1: Use Case Diagram

Table 3.3.2-1: Actor Roles

Actor:	Data Access Authority (DAA)
Role:	Decision Issuer: creates, versions, signs or otherwise protects, and distributes the authoritative permit or access decision.
Actor:	Secondary Use Agent (SUA)
Role:	Applicant Recipient: receives the applicant-facing decision and obligations.
Actor:	Data Access Coordinator (DAC)
Role:	Fulfillment Recipient: receives the operational decision needed to coordinate authorized fulfillment.
Actor:	Information Source (IS) (conditionally)
Role:	Source Recipient: receives the permit subset or verification reference needed to provision authorized data.

 Copyright © 2026: IHE International, Inc.

3.3.3 Referenced Standards

- HL7 FHIR R4 messaging using Bundle, MessageHeader, Task, Contract, DocumentReference, Binary, Provenance, Organization, PractitionerRole, Endpoint, and Consent where applicable.
- FHIR Signature data type and/or jurisdictionally recognized electronic-signature mechanisms.
- FHIR OperationOutcome for validation or processing errors.
- IHE MHD, XDR, XDS, or XCA may be used to exchange a signed human-readable decision artifact while the FHIR control message carries machine-actionable references and constraints.
- IHE ATNA, Consistent Time, IUA/XUA, and deployment-specific trust services.

3.3.4 Messages

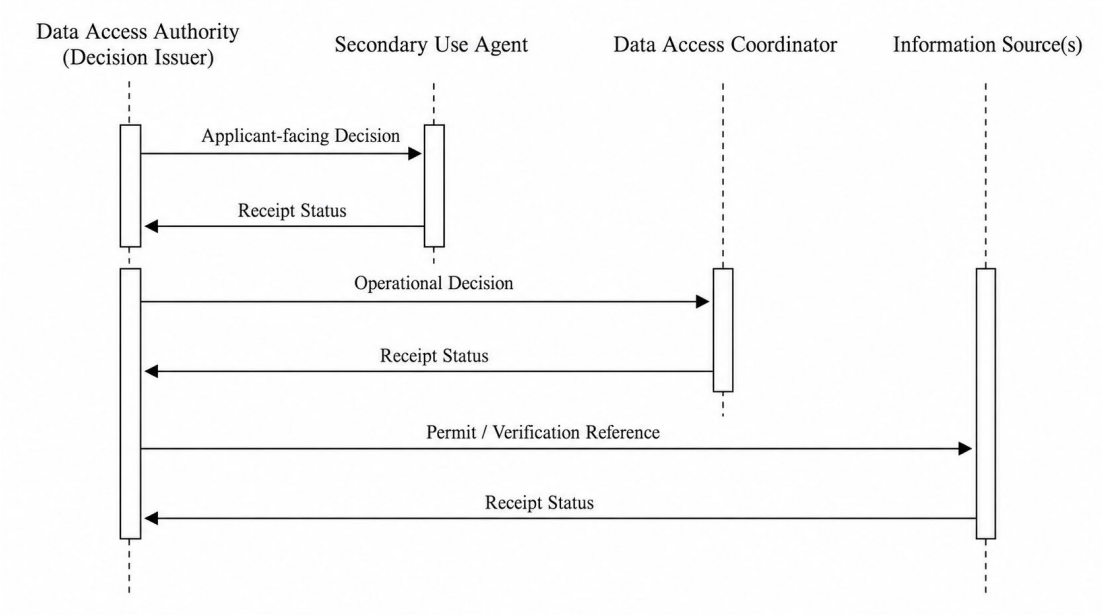


Figure 3.3.4-1: Interaction Diagram

3.3.4.1 Access Decision

The Access Decision message carries the machine-actionable decision and may reference a signed human-readable permit, denial, or amendment request.

3.3.4.1.1 Trigger Events

The DAA completes assessment of a new or amended request.

The DAA issues a replacement, suspension, revocation, correction, or expiry notice for an existing decision.

 Copyright © 2026: IHE International, Inc.

3.3.4.1.2 Message Semantics

The message shall be a FHIR Bundle of type message. The MessageHeader shall identify the SU-3 decision event and the intended recipient. A Task shall carry the decision workflow state. A Contract should represent machine-actionable terms, and a DocumentReference shall identify any signed permit or decision document. Provenance shall identify the issuer, issue time, and relationship to the request.

Each recipient may receive a role-appropriate view, but all views shall carry the same decision identifier and version and shall remain semantically consistent. Recipient-specific views shall not omit a condition that the recipient must enforce.

When the decision authorizes an OMOP-based realization, it shall identify the approved OMOP domains or concept scope, population and observation period, required CDM and vocabulary versions where known, and the permitted location of transformation or execution. The authorization shall not imply that all source systems must natively store OMOP data.

An amendment, suspension, revocation, or replacement shall use a new decision version and shall explicitly reference the decision version affected.

Table 3.3.4.1-1: Required Access Decision Semantics

Element group	Required meaning
Decision identity	Decision / permit identifier, version, issue time, effective time, expiry, and replaced decision.
Request correlation	Authoritative request identifier and version to which the decision applies.
Decision status	Approved, partially approved, denied, amendment required, suspended, revoked, expired, or replaced.
Issuer and authority	Issuing organization, responsible role, jurisdiction, and signature / integrity evidence.
Permitted purpose	Approved purpose, project, protocol, legal or policy basis, and prohibited deviations.
Authorized data scope	Datasets, sources, cohort, variables, modalities, observation period, geography, linkage, permitted transformations, and, where applicable, authorized OMOP domains, concepts, concept sets, descendant scope, and granularity.
Fulfillment and destination	DAC, authorized recipients, preparation path, SPE, endpoints, federation nodes, permitted transport mechanisms, approved analytical representation, and permitted location of any OMOP transformation or local execution.
De-identification requirements	Minimization, pseudonymization, anonymization, disclosure-control, policy identifiers, and validation requirements.
Processing and release constraints	Permitted tools and methods, retention, monitoring, output classes, export review, publication, and deletion obligations.
Administrative conditions	Fees, reporting duties, significant-finding duties where applicable, appeals, incident reporting, and other conditions.

 Copyright © 2026: IHE International, Inc.

3.3.4.1.3 Expected Actions

Each recipient shall validate the issuer, integrity, effective period, decision status, and recipient binding before acting.

The DAC shall create or update the fulfillment workflow only for an effective approved or partially approved decision. The IS shall not provision data solely on the basis of a human-readable document when a required machine-actionable verification cannot be completed.

On suspension, revocation, expiry, or replacement, recipients shall stop new actions under the superseded authorization and shall apply any required containment, deletion, or notification procedure.

3.3.4.2 Decision Receipt Status

The Decision Receipt Status reports whether the recipient accepted, rejected, or could not validate the decision message.

3.3.4.2.1 Trigger Events

A recipient receives and validates an Access Decision message.

3.3.4.2.2 Message Semantics

The response shall identify the decision identifier, version, recipient, and validation outcome. An OperationOutcome shall describe signature, recipient, version, reference, or policy errors.

Receipt status is transport and validation evidence; it does not change the substantive decision.

Table 3.3.4.2-1: Receipt Outcomes

Outcome	Meaning
accepted	Decision validated and stored by the recipient.
accepted-with-warning	Decision accepted; a non-blocking issue was recorded.
rejected-invalid	Integrity, signature, structure, reference, or recipient validation failed.
rejected-stale	A newer authoritative version is already known.
temporarily-unavailable	Recipient could not complete processing; retry may be appropriate.

3.3.4.2.3 Expected Actions

The DAA shall correlate each response with the intended recipient and may retry delivery or use an alternate authorized channel.

A recipient that rejects a decision because validation failed shall not begin or continue fulfillment under that message.

 Copyright © 2026: IHE International, Inc.

3.3.5 Security Considerations

The decision is an authorization artifact and shall be protected against substitution, unauthorized modification, replay, and disclosure to unintended recipients.

The DAA shall use a signature or equivalent integrity mechanism appropriate to the trust framework. Recipients shall verify status and validity at the time of use; possession of an expired, revoked, or superseded permit shall not authorize provisioning.

3.3.5.1 Security Audit Considerations

The DAA and each recipient shall audit issuance, delivery, validation outcome, amendment, suspension, revocation, expiry, and replacement. Audit records shall include decision and request identifiers and versions but shall not expose protected policy or pseudonym material.

3.3.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Data Access Authority	Protect signing credentials and ensure recipient-specific views remain consistent.
Data Access Coordinator	Prevent fulfillment under stale, revoked, or mismatched decisions.
Information Source	Validate permit scope, source binding, destination, and validity before provisioning.
Secondary Use Agent	Protect applicant-facing decisions and communicate obligations to the authorized user.

3.4 Authorized Source Data Provision [SU-4]

3.4.1 Scope

This transaction coordinates permit-authorized provision by one or more Information Source actors. It supports record-level extracts, imaging studies, multimodal packages, existing or permit-bound OMOP datasets, source-local aggregate results, manifests, and processing-target references. SU-4 defines the governance and control-plane interaction; the payload may use FHIR Bulk Data, DICOMweb, document exchange, secure file or object transfer, an OMOP database extract or controlled endpoint, remote access, or an approved federated-query binding.

3.4.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

 Copyright © 2026: IHE International, Inc.

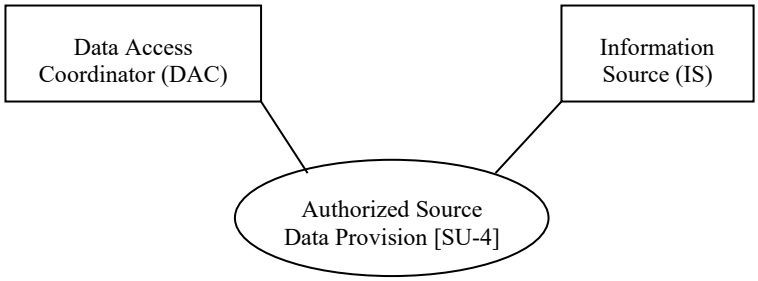


Figure 3.4.2-1: Use Case Diagram

Table 3.4.2-1: Actor Roles

Actor:	Data Access Coordinator (DAC)
Role:	Provision Coordinator: creates source-specific fulfillment instructions, identifies the authorized destination and transfer binding, tracks status, and correlates all source responses with the permit.
Actor:	Information Source (IS)
Role:	Source Provider: validates the authorization, selects and minimizes the authorized source data or executes the authorized local query, provides the payload or reference using the approved binding, and returns status and manifest information.

3.4.3 Referenced Standards

- HL7 FHIR R4 messaging using MessageHeader, Task, Group, List, Endpoint, DocumentReference, Binary, Provenance, Measure, MeasureReport, and OperationOutcome.
- HL7 FHIR Bulk Data Access for asynchronous export of large structured FHIR datasets where selected by the deployment.
- DICOM PS3.18 web services, including DICOMweb query, retrieve, and store services, for imaging and digital-pathology objects where applicable.
- IHE MHD, XDR, XDS, or XCA for document-oriented provision where applicable.
- Approved secure file-transfer, object-store, repository-access, or remote-access mechanisms for payload types not covered by an IHE profile.
- OHDSI OMOP Common Data Model and standardized vocabularies when the permit authorizes provision of an existing OMOP dataset or permit-bound transformation into OMOP. OMOP is an analytical representation and is not the SU-4 transport protocol.
- IHE ATNA, Consistent Time, and IUA/XUA or deployment-specific OAuth 2.0 / OpenID Connect authorization.

 Copyright © 2026: IHE International, Inc.

3.4.4 Messages

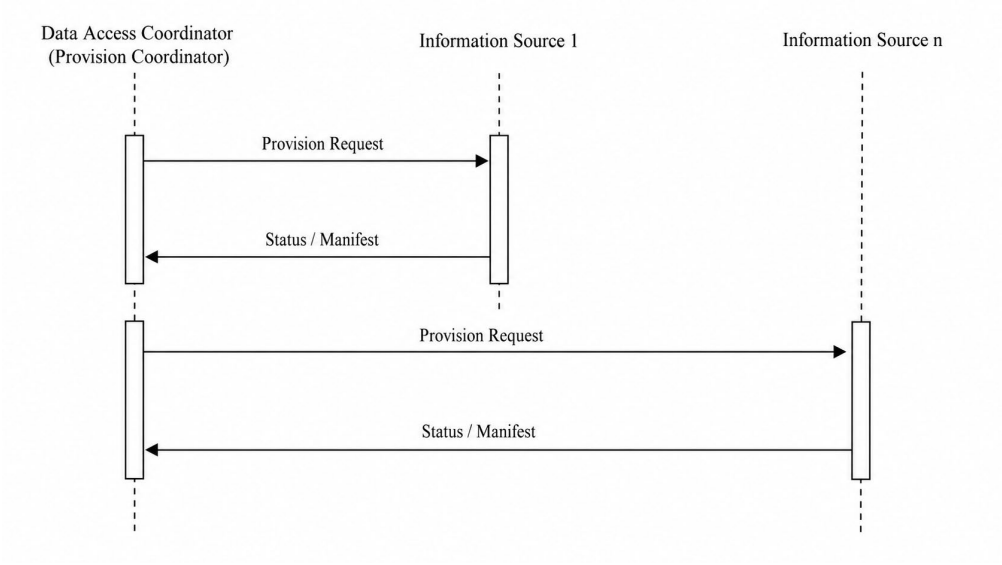


Figure 3.4.4-1: Interaction Diagram

3.4.4.1 Provision Request

The Provision Request instructs a specific Information Source to perform one permit-bound fulfillment action.

3.4.4.1.1 Trigger Events

The DAC receives an effective approval through SU-3 and decomposes the decision into one or more source-specific fulfillment actions.

A previous fulfillment action requires an authorized correction, retry, or incremental update.

3.4.4.1.2 Message Semantics

The request shall be represented by a FHIR Task in a message Bundle. It shall identify the source-specific fulfillment identifier, permit identifier and version, approved destination, requested action, content constraints, and expected evidence.

The request shall identify the payload binding and endpoint or shall reference a separately authorized endpoint-registration mechanism. It shall not require the IS to disclose data beyond the permit scope.

One permit may result in requests to multiple IS actors. Each source request shall have its own fulfillment identifier while retaining the common request and permit correlation.

Table 3.4.4.1-1: Provision Request Semantics

Element group	Required meaning
Fulfillment identity	Unique source-fulfillment identifier and idempotency key.

 Copyright © 2026: IHE International, Inc.

Element group	Required meaning
Authorization	Permit / decision identifier and version, validity, approved purpose, and verification reference.
Source scope	Information Source, dataset versions, cohort, variables, objects, modalities, period, OMOP domains or concept scope where applicable, and other minimization constraints.
Requested action	Extract, package, query, aggregate, transform, make available, or provide a processing-target reference.
Destination	Authorized preparation store, De-Identifier input, SPE, remote execution target, or other permitted endpoint.
Payload binding	Bulk FHIR, FHIR REST, DICOMweb, document exchange, secure file/object transfer, OMOP database extract or standardized files, controlled OMOP endpoint, remote access, or federated query.
Content constraints	Required profiles, coding systems, file formats, manifests, linkage rules, cross-modal referential integrity, analytical model and version, vocabulary release, ETL or mapping constraints, and required validation.
Security and timing	Token audience, endpoint identity, encryption, deadline, validity window, retry policy, and maximum volume.
Evidence requirements	Counts, checksums, provenance, extraction parameters, transformation and ETL provenance, source and model validation, errors, and required acknowledgements.

3.4.4.1.3 Expected Actions

The IS shall authenticate the DAC, verify the permit and destination, validate that the requested scope is within the source and permit, and return an initial status.

If a requested element is unavailable, outside scope, prohibited, or cannot be safely provided, the IS shall reject or partially accept the request and identify the affected element without disclosing unauthorized data.

The IS shall implement idempotent handling for the same fulfillment identifier and request version.

3.4.4.2 Provision Status

The Provision Status reports acceptance, progress, delay, need for clarification, partial fulfillment, failure, or cancellation.

3.4.4.2.1 Trigger Events

The IS validates the request, reaches a significant processing state, detects a failure, or receives a cancellation / replacement instruction.

 Copyright © 2026: IHE International, Inc.

3.4.4.2.2 Message Semantics

The message shall reference the fulfillment identifier, request and permit identifiers, source, current status, status time, and any estimated completion time. An OperationOutcome shall carry machine-processable errors and warnings.

For asynchronous Bulk FHIR or other long-running exports, the status may reference the authorized status endpoint but shall not expose credentials in the message.

Table 3.4.4.2-1: Provision Status Values

Status	Meaning
accepted	Request validated and queued or started.
needs-information	Clarification or corrected scope is required.
in-progress	Provisioning is executing.
on-hold	Processing is paused for an authorized reason.
partially-completed	Some approved scope was provided; exceptions are documented.
completed	Authorized provision completed and manifest is available.
failed	Provisioning did not complete; errors are reported.
cancelled	Work stopped before completion under an authorized cancellation.

3.4.4.2.3 Expected Actions

The DAC shall update the fulfillment state and shall not infer successful provision until it receives a completed result / manifest and, where required, destination acknowledgement.

The IS shall stop work when the permit is suspended, revoked, expired, or replaced, subject to safe transactional rollback and policy-defined containment.

3.4.4.3 Provision Result and Manifest

The Provision Result and Manifest identifies what was provided, where it was made available, and the evidence needed to validate the fulfillment.

3.4.4.3.1 Trigger Events

The IS completes, partially completes, or terminally fails the requested provision action.

3.4.4.3.2 Message Semantics

The result shall be represented as Task output references in a FHIR message Bundle. The payload itself may be embedded only when size and policy permit; normally the result references a manifest, files, resources, DICOM objects, document packages, aggregate results, or an authorized retrieval / remote-execution endpoint.

 Copyright © 2026: IHE International, Inc.

The manifest shall identify the source datasets and versions, extraction or query parameters, content profiles and formats, record/object/file counts, sizes, checksums, creation times, destination, and provenance. For an OMOP representation, it shall additionally identify the OMOP CDM version, vocabulary release, included domains, ETL or source-to-OMOP mapping version, transformation provenance, and applicable validation results. It shall identify missing or excluded content and shall preserve cross-modal linkage identifiers only as permitted.

For a federated aggregate request, the result shall contain only the approved aggregate package and source-level disclosure-control evidence. Record-level Bulk FHIR files shall remain within the source node when the approved pattern is local aggregation.

Table 3.4.4.3-1: Minimum Provision Manifest

Manifest element	Required meaning
Identity and correlation	Manifest identifier, fulfillment identifier, request and permit identifiers / versions.
Source and extraction	Source actor, dataset identifiers / versions, extraction or query time, and parameters.
Payload inventory	Files, FHIR resources, DICOM studies / objects, documents, aggregates, or endpoint references.
Integrity	Sizes, hashes / checksums, signatures where used, and packaging information.
Content conformance	Formats, profiles, implementation guides, coding systems, analytical model and version, vocabulary release, included domains, and validation results.
Minimization / transformation	Applied selection, exclusion, preliminary de-identification, terminology mapping, ETL or source-to-model transformation, and policy / evidence references.
Exceptions	Unavailable, suppressed, rejected, or failed items and their non-disclosing reason codes.
Destination and status	Authorized destination, transfer status, completion time, and expected acknowledgement.

3.4.4.3.3 Expected Actions

The DAC shall validate the manifest, status, source identity, permit correlation, and destination. It shall record partial fulfillment and shall initiate correction only through an authorized request version.

The IS shall retain or delete temporary export material according to the permit, policy, and local retention rules.

Where the payload is delivered directly to another actor, the DAC shall correlate the result with the destination acknowledgement rather than assuming receipt from source completion alone.

 Copyright © 2026: IHE International, Inc.

3.4.5 Security Considerations

The IS shall independently validate the permit, source binding, destination, requester identity, purpose, validity, and requested scope. A valid transport token alone shall not authorize data beyond the permit.

Payload transfer shall use mutually authenticated, encrypted channels. Endpoint and token audiences shall be bound to the authorized destination. Signed URLs or temporary credentials shall be short-lived and shall not be written into broadly accessible logs.

The IS shall minimize data before provision and shall prevent accidental inclusion of identifiers, hidden metadata, private tags, burned-in annotations, unsupported modalities, or unapproved linked content.

3.4.5.1 Security Audit Considerations

The DAC and IS shall audit request, acceptance, status changes, payload creation, source dataset versions, transfer initiation, manifest, completion, failure, cancellation, and destination acknowledgement. The audit event shall correlate the fulfillment identifier with the permit and request.

3.4.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Data Access Coordinator	Protect destination credentials and prevent reuse of a source request for another permit or recipient.
Information Source	Enforce minimization, destination validation, payload integrity, and safe cleanup of temporary export material.

3.5 Transfer Prepared Data to SPE [SU-5]

3.5.1 Scope

This transaction coordinates the authorized delivery and ingestion of permit-bound prepared data into a Secure Processing Environment. Prepared data may include an OMOP database extract, standardized OMOP files, or access to a controlled OMOP endpoint when authorized. SU-5 separates the SU-DSX control-plane responsibility from the underlying data-plane transport.

When DIS is used, ITI-x5 Retrieve De-Identified Data or ITI-x6 Deliver De-Identified Data provides the receiver-facing data transfer; SU-5 preserves authorization, manifest, destination, ingest, and acknowledgement correlation.

The De-ID Manager, when used, controls receiver-facing delivery of the prepared de-identified dataset and avoids exposing protected de-identification evidence. The SPE acts as the Prepared Data Receiver and validates the authorization and package before ingest or secure mount.

 Copyright © 2026: IHE International, Inc.

3.5.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

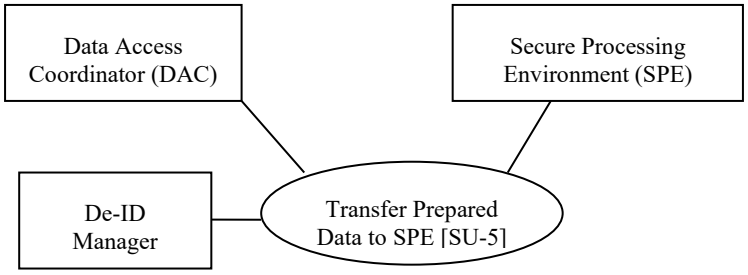


Figure 3.5.2-1: Use Case Diagram

Table 3.5.2-1: Actor Roles

Actor:	Data Access Coordinator (DAC)
Role:	Delivery Coordinator: authorizes and tracks the delivery, provides the SPE with the expected manifest and conditions, and correlates the ingest result with the permit and source fulfillment.
Actor:	De-ID Manager (conditionally)
Role:	Delivery Manager: controls approved receiver-facing delivery when DIS is used and is grouped with the applicable SU-DSX delivery coordination function.
Actor:	Secure Processing Environment (SPE)
Role:	Prepared Data Receiver: validates the authorization and package, ingests or securely mounts the prepared data, quarantines invalid content, and reports ingest status.

3.5.3 Referenced Standards

- HL7 FHIR R4 messaging using MessageHeader, Task, Endpoint, List, DocumentReference, Binary, Provenance, and OperationOutcome for the control plane.
- DIS ITI-x5 Retrieve De-Identified Data and ITI-x6 Deliver De-Identified Data when the DIS profile is used; identifiers remain provisional in this draft.
- HL7 FHIR Bulk Data, DICOMweb, IHE MHD/XDR/XDS/XCA, secure file/object transfer, OMOP database extract or standardized files, controlled OMOP endpoint, remote repository access, or another approved binding for the data plane.
- IHE ATNA, Consistent Time, and deployment-specific identity / authorization profiles.

 Copyright © 2026: IHE International, Inc.

3.5.4 Messages

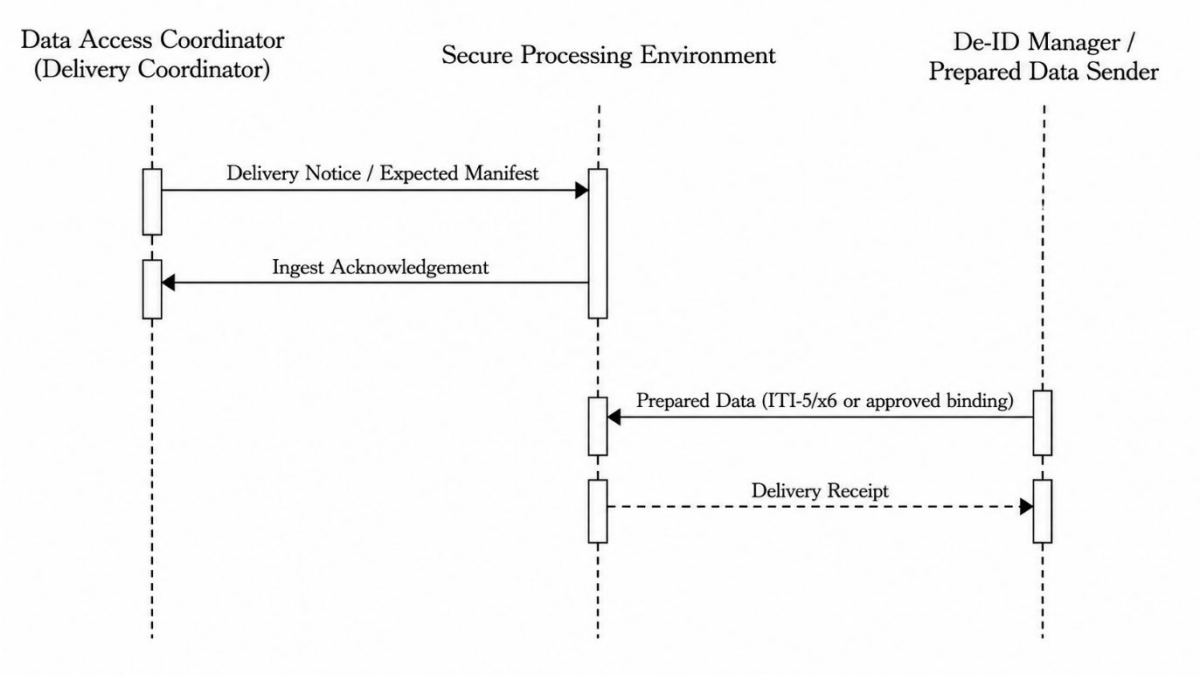


Figure 3.5.4-1: Interaction Diagram

3.5.4.1 Prepared Data Delivery Notice

The Prepared Data Delivery Notice informs the SPE of an authorized incoming or retrievable prepared-data package and the conditions under which it may be ingested.

3.5.4.1.1 Trigger Events

A prepared package has passed the required validation and is approved for delivery to the SPE.

The DAC authorizes a new, corrected, incremental, or replacement delivery.

3.5.4.1.2 Message Semantics

The notice shall identify the delivery identifier, permit and decision version, expected sender, authorized SPE, dataset / package identifier, manifest, delivery binding, retention and deletion conditions, and integrity evidence.

The notice shall identify whether the SPE shall retrieve the data, accept a push delivery, mount a protected repository, or execute against a controlled remote target. It shall not contain reusable secret credentials.

The notice may identify DIS policy and evidence references but shall not expose pseudonym mappings or re-identification material.

 Copyright © 2026: IHE International, Inc.

Table 3.5.4.1-1: Prepared Data Delivery Notice

Element	Required meaning
Delivery identity	Unique delivery identifier, version, and idempotency key.
Authorization context	Permit / decision identifier and version, effective period, purpose, and SPE binding.
Expected package	Package / dataset identifier, manifest, sender, size, format, profiles, checksums, and, where applicable, OMOP CDM version, vocabulary release, included domains, ETL / mapping version, and validation results.
Delivery method	DIS pull / push, Bulk FHIR, DICOMweb, document exchange, secure object / file retrieval, OMOP package transfer, controlled OMOP endpoint, or remote access.
Ingest constraints	Workspace, tenant, access group, quarantine rules, retention, deletion, and allowed processing period.
Evidence	Source fulfillment, de-identification policy, transformation, validation, and provenance references.

3.5.4.1.3 Expected Actions

The SPE shall authenticate the notice sender, verify that it is the authorized destination, reserve an isolated ingest context, and return an acceptance or rejection status.

The SPE shall not make the data available to an analysis workspace until the package and authorization have been validated.

3.5.4.2 Prepared Data Transfer

The Prepared Data Transfer moves or exposes the approved prepared data using the binding named in the Delivery Notice.

3.5.4.2.1 Trigger Events

The SPE accepts the Delivery Notice and the approved sender begins push delivery or enables authorized retrieval / remote access.

3.5.4.2.2 Message Semantics

When DIS is used, the De-ID Manager shall control receiver-facing transfer through ITI-x5 or ITI-x6. Otherwise the sender and SPE shall use the approved payload binding and shall preserve the SU-5 delivery identifier in the transfer metadata or manifest.

The transfer may contain copied data, FHIR resources linked to binary objects, DICOM or pathology packages, documents, an OMOP database extract or standardized files, a protected mounted repository, a controlled OMOP endpoint, or a federated / remote execution target. The transfer shall contain only the prepared content identified by the manifest.

 Copyright © 2026: IHE International, Inc.

Table 3.5.4.2-1: Data-Plane Binding Rules

Binding	SU-5 Rule
DIS ITI-x5 / ITI-x6	Use the DIS receiver and delivery evidence; correlate to the SU-5 delivery identifier.
FHIR Bulk Data	Use authorized output / file URLs, validate manifests and hashes, and import only permitted resource types and cohorts.
DICOMweb	Use authorized study / series / instance scopes; validate DICOM de-identification evidence and object integrity.
MHD / XDR / XDS / XCA	Preserve document metadata, patient / subject pseudonym scope where permitted, and package provenance.
Secure file / object transfer	Use short-lived credentials, immutable manifests, checksums, and an approved content-type / format registry.
Remote or federated access	Do not copy source data when the permit authorizes remote execution only; bind compute target and outputs to the same delivery context.
OMOP CDM	Identify the OMOP CDM version, vocabulary release, included domains, ETL or source-to-OMOP mapping provenance, and validation results. Delivery may use a database extract, standardized files, a protected mounted repository, or a controlled endpoint approved for the SPE.

3.5.4.2.3 Expected Actions

The SPE shall validate sender identity, package identity, checksums, format, conformance, and completeness. Invalid or unexpected content shall be quarantined and shall not be exposed to the data user.

The sender shall not regard network-level delivery as successful until it receives or can correlate the SPE ingest acknowledgement.

3.5.4.3 Ingest Acknowledgement

The Ingest Acknowledgement reports whether the SPE accepted, quarantined, partially accepted, or rejected the prepared package.

3.5.4.3.1 Trigger Events

The SPE completes package validation and ingest or reaches a terminal ingest error.

3.5.4.3.2 Message Semantics

The acknowledgement shall identify the delivery identifier, SPE, package and manifest identifiers, validation time, outcome, ingested inventory, and any quarantined or rejected items. An OperationOutcome shall identify errors without exposing protected content.

Acceptance shall mean that the package is available only within the authorized SPE security context; it does not mean that a user has executed an analysis or that any output is approved for release.

 Copyright © 2026: IHE International, Inc.

Table 3.5.4.3-1: Ingest Outcomes

Outcome	Meaning
accepted	All expected content validated and is available in the authorized SPE context.
accepted-partial	A permitted subset was accepted; exceptions are documented.
quarantined	Content received but not available for use pending investigation or correction.
rejected	Authorization, integrity, format, sender, destination, or policy validation failed.
failed	Ingest could not complete because of a technical failure; retry may be authorized.

3.5.4.3.3 Expected Actions

The DAC shall correlate the acknowledgement with source provisioning and DIS evidence. It shall not close the fulfillment event when the acknowledgement is missing, inconsistent, or failed.

For partial acceptance, the DAC shall determine whether analysis may proceed under the permit or whether a corrected delivery is required.

3.5.5 Security Considerations

The SPE shall enforce tenant and project isolation, receiver authorization, malware and content validation, encryption, retention, and deletion controls before making data available.

Receiver-facing evidence shall exclude pseudonym mappings, re-identification keys, hidden direct identifiers, and privileged policy material. The SPE shall prevent the data user from bypassing the authorized import path.

Temporary URLs, credentials, and mounts shall expire promptly and shall be scoped to the intended SPE and delivery.

3.5.5.1 Security Audit Considerations

The DAC, sender / De-ID Manager, and SPE shall audit delivery notice, transfer start, retrieval or push, validation, quarantine, acceptance, correction, and deletion. Events shall correlate delivery, permit, fulfillment, package, de-identification job, and SPE workspace identifiers.

3.5.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Data Access Coordinator	Ensure that the selected SPE and delivery method match the current permit.
De-ID Manager	Control receiver-facing release and avoid exposing protected de-identification evidence.
Secure Processing Environment	Validate all imports, isolate projects, and prevent use before successful ingest.

 Copyright © 2026: IHE International, Inc.

3.6 Secure Processing and Results Release [SU-6]

3.6.1 Scope

This transaction coordinates approved processing and the release of results. It supports: (a) personal-level or pseudonymized processing inside an SPE with a controlled export workflow; and (b) a lighter no-SPE path for an approved aggregate or statistical result that is non-identifying by design. Completion of an analysis does not itself authorize export.

3.6.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

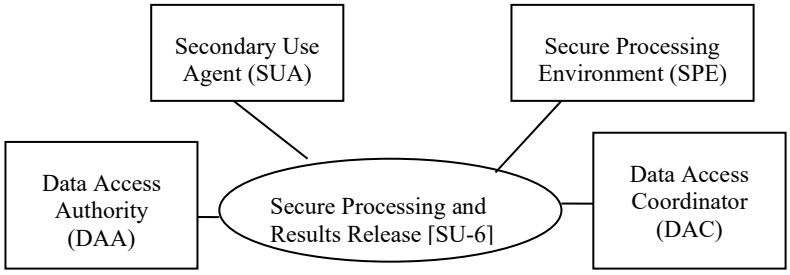


Figure 3.6.2-1: Use Case Diagram

Table 3.6.2-1: Actor Roles

Actor:	Secondary Use Agent (SUA) or DAC when acting on behalf of the approved workflow
Role:	Job Requester: submits the authorized processing definition and receives status.
Actor:	Secure Processing Environment (SPE) (conditionally)
Role:	Processor: executes the approved job, preserves traceability, creates output candidates, and prevents unauthorized export.
Actor:	Data Access Coordinator (DAC)
Role:	Release Coordinator: validates the release request, coordinates any DIS output-control job or disclosure review, records the release decision, and authorizes delivery.
Actor:	Secondary Use Agent (SUA) and, where required, Data Access Authority (DAA)
Role:	Results Recipient: receives only approved output and associated receiver-safe evidence.

 Copyright © 2026: IHE International, Inc.

3.6.3 Referenced Standards

- HL7 FHIR R4 messaging using MessageHeader, Task, PlanDefinition, ActivityDefinition, ResearchStudy, Group, Measure, MeasureReport, DocumentReference, Binary, Provenance, AuditEvent, and OperationOutcome.
- DIS ITI-x1 through ITI-x6 may be referenced for policy-governed input preparation and delivery of prepared de-identified data to the SPE. SU-6 does not require a post-analysis DIS job; output review and release are governed by the SU-6 release-control workflow.
- IHE QRPH CRPC, DEX, RPE, ADX / mADX, QEDm, SDC, and related profiles may be used as informative content or execution bindings.
- OHDSI OMOP CDM, standardized vocabularies, cohort definitions, concept sets, and approved OHDSI-compatible or other analytical packages may be used as informative analytical bindings inside an SPE or participating federated nodes.
- IHE ATNA, Consistent Time, and deployment-specific identity / authorization controls for SPE access and export approval.

3.6.4 Messages

Lighter no-SPE aggregate release path:

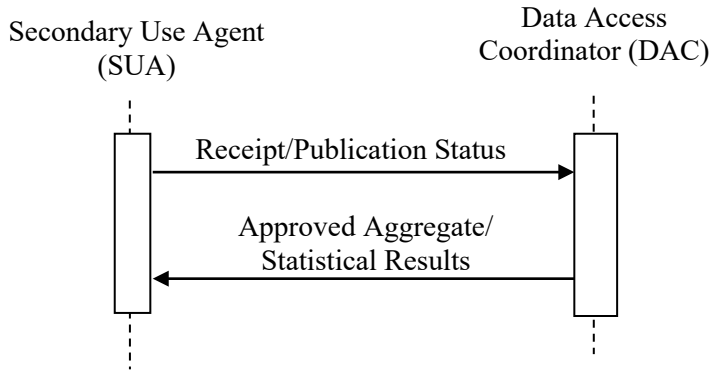
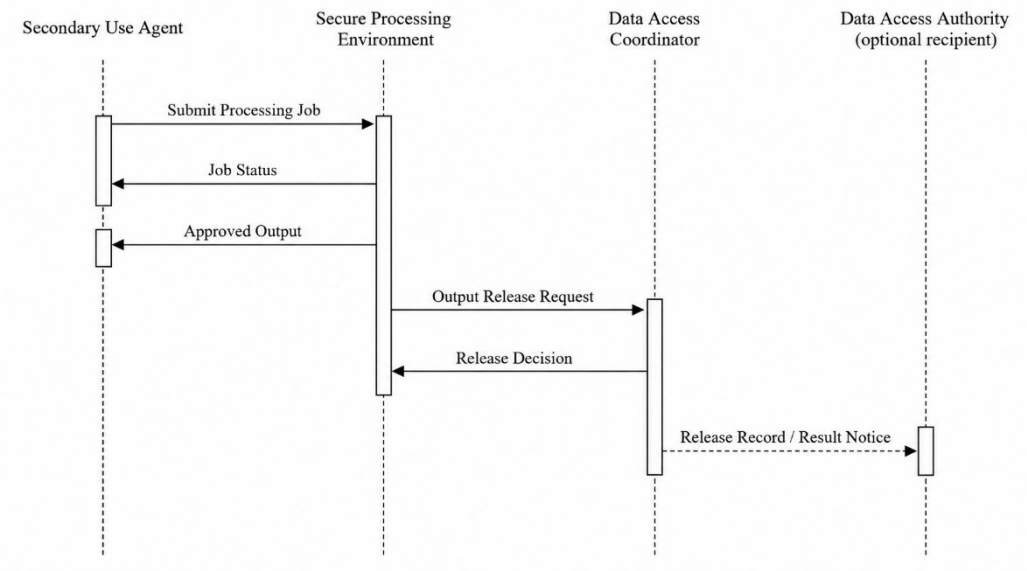


Figure 3.6.4-1: Interaction Diagram

SPE processing and controlled results release:

 Copyright © 2026: IHE International, Inc.



3.6.4.1 Submit Processing Job

The Submit Processing Job message requests execution of a permit-authorized analysis, validation, or other processing activity in the designated SPE.

3.6.4.1.1 Trigger Events

The prepared dataset has been accepted into the SPE and the authorized user or orchestration service is ready to execute an approved activity.

An authorized repeat, correction, validation run, or benchmark execution is required.

3.6.4.1.2 Message Semantics

The message shall reference the permit, SPE dataset / delivery identifiers, project, processing definition, tool or container version, input parameters, expected outputs, resource limits, and permitted output classes. It shall identify the requester, purpose, and execution validity window.

A FHIR Task shall represent the job. PlanDefinition, ActivityDefinition, ResearchStudy, Group, Measure, DocumentReference, and other resources may define the execution. An OMOP-based job may reference the CDM version, vocabulary release, cohort definition, concept sets, and approved analytical package. Large code, container images, or workflow packages should be referenced rather than embedded and shall be obtained from an approved registry.

The job shall be immutable after acceptance. Changes that affect data, method, tool version, recipient, or expected outputs shall use a new job version.

Table 3.6.4.1-1: Processing Job Semantics

Element	Required meaning
Job identity	Unique job identifier, version, retry relationship, and idempotency key.

 Copyright © 2026: IHE International, Inc.

Element	Required meaning
Authorization	Permit / decision, project, requester, purpose, and validity.
Inputs	SPE dataset / delivery identifiers, versions, cohort / partitions, approved parameters, and, where applicable, OMOP CDM version, vocabulary release, included domains, or controlled node endpoints.
Execution definition	Workflow, script, container, model, measure, protocol, cohort definition, concept sets, tool versions, approved OMOP or other analytical package, and approved network dependencies.
Resource constraints	Compute, memory, storage, accelerator, time, concurrency, and monitoring limits.
Expected outputs	Reports, measures, tables, figures, model artifacts, embeddings, synthetic data, and other candidate classes.
Release expectations	Intended recipient, requested output class, required review, and publication / reporting obligations.

3.6.4.1.3 Expected Actions

The SPE shall authenticate and authorize the requester, verify permit and dataset scope, validate the execution package, allocate the approved resources, and return a job status.

The SPE shall reject unapproved network access, tools, data, output destinations, or resource requests. It shall preserve sufficient execution metadata for reproducibility and audit.

3.6.4.2 Processing Status and Completion Notice

The Processing Status and Completion Notice reports the job lifecycle and identifies output candidates without authorizing their export.

3.6.4.2.1 Trigger Events

The SPE accepts a job, changes its significant state, completes execution, or encounters an error.

3.6.4.2.2 Message Semantics

The status shall identify the job, permit, dataset / delivery, requester, current state, timestamps, tool / workflow version, and outcome. The completion notice shall identify candidate outputs and their internal SPE references, provenance, and preliminary validation.

Output candidate references shall remain internal to the SPE until a release decision is issued. A completed status shall not include a public or unrestricted download URL.

Table 3.6.4.2-1: Processing Status Values

Status	Meaning
accepted	Job validated and queued.

 Copyright © 2026: IHE International, Inc.

Status	Meaning
running	Approved execution is active.
on-hold	Execution paused for an authorized reason.
completed	Execution completed; output candidates exist inside the SPE.
failed	Execution ended without successful completion.
cancelled	Execution stopped under an authorized cancellation.
expired	Job was not executed within the authorized period.

3.6.4.2.3 Expected Actions

The SUA and DAC shall preserve the status and shall distinguish successful execution from approved release.

On failure, the SPE shall provide a non-disclosing OperationOutcome and sufficient diagnostic information for an authorized correction.

3.6.4.3 Output Release Request

The Output Release Request asks the Release Coordinator to approve one or more output candidates for a specified recipient and purpose. The request shall identify the permit, source datasets, delivery and processing jobs, output candidate, artifact version/hash, intended recipient, purpose, justification, proposed format, requested release channel, and applicable review evidence.

The request shall include or reference applicable automated checks, statistical disclosure-control results, privacy-risk assessment, model leakage assessment, scientific or administrative review evidence, or other validation evidence required by the decision. It shall identify any authorized transformation that must be completed before release. It shall not contain a requirement to submit a DIS output-control job.

3.6.4.3.1 Trigger Events

The SPE or authorized user identifies an output candidate that should leave the controlled environment.

A prior release request requires correction, additional transformation, or a new recipient.

3.6.4.3.2 Message Semantics

The request shall identify the permit, source datasets, delivery and processing jobs, output candidate, artifact version, intended recipient, purpose, justification, proposed format, and requested release channel.

 Copyright © 2026: IHE International, Inc.

The request shall include or reference applicable automated checks, statistical disclosure-control results, privacy-risk assessment, model leakage assessment, or other validation evidence. It shall identify whether a DIS output-control job is required.

A new request version shall be used when the artifact, recipient, purpose, or release package changes materially.

Table 3.6.4.3-1: Output Release Request

Element	Required meaning
Release identity	Unique release-request identifier, version, and relationship to previous attempts.
Provenance	Source datasets, preparation / delivery, processing jobs, tool / model version, and creator.
Candidate artifact	Internal SPE identifier, artifact class, format, size, hash, and proposed package.
Recipient and purpose	Authorized organization / person / endpoint and intended permitted use.
Risk and validation	Disclosure-control, anonymization, leakage, reconstruction, quality, and utility evidence.
Requested channel	Controlled download, push delivery, document exchange, report publication, or other approved channel.

3.6.4.3.3 Expected Actions

The DAC shall verify that the output and recipient are within the permit, that the required review path was completed, and that the artifact is non-identifying for the intended release context. When further treatment is required, the DAC, SPE export-control component, or other authorized release-control function shall keep the candidate controlled, apply or coordinate only the authorized treatment, validate the resulting artifact, and shall not release the untreated candidate.

3.6.4.4 Release Decision and Approved Output

The DAC completes or coordinates the required policy, disclosure, privacy, scientific, administrative, or other permit-defined review. Post-analysis review and treatment are part of SU-6 and are not modeled as DIS jobs.

The decision shall bind the exact approved artifact/version/hash, recipient, review evidence, any authorized transformation, expiry, delivery channel, and post-release obligations. The SPE or delivery service shall release only the exact approved package to the authorized recipient.

3.6.4.4.1 Trigger Events

The DAC completes the required policy, disclosure, privacy, scientific, or administrative review, including any DIS output-control workflow.

 Copyright © 2026: IHE International, Inc.

3.6.4.4.2 Message Semantics

The decision shall reference the release request and version, permit, artifact, recipient, review evidence, decision maker or policy service, and decision time. It shall identify approved transformations, approved output package, expiry, delivery channel, and any post-release obligations.

An approved output may be represented or referenced using MeasureReport, DocumentReference, Binary, Provenance, or another content profile appropriate to the artifact. Model weights, embeddings, synthetic data, and other non-document artifacts shall be packaged with type, version, hash, provenance, and receiver-safe evidence.

Rejected or partially approved decisions shall identify the disallowed elements and required changes without exposing protected review material.

Table 3.6.4.4-1: Release Outcomes

Outcome	Meaning
approved	The identified artifact and package may be released to the named recipient.
approved-partial	Only the identified subset or transformed package may be released.
revision-required	The candidate must be changed or undergo additional review.
rejected	The candidate shall not be released.
expired / revoked	A previous approval is no longer effective and unused delivery capability shall be disabled.

3.6.4.4.3 Expected Actions

The SPE or delivery service shall release only the exact approved package to the authorized recipient. It shall prevent the recipient from substituting another artifact or retrieving an earlier unapproved version.

The SUA shall acknowledge receipt and shall comply with publication, citation, retention, onward-disclosure, and reporting obligations.

The DAC shall record completion, delivery status, and any post-release notification required by the DAA.

3.6.4.5 Direct Aggregate Result Release

The Direct Aggregate Result Release remains the baseline no-SPE pattern for authorized non-identifying aggregate/statistical results. The DAC validates the permitted aggregate results, applies or verifies the required disclosure controls, and releases only the approved aggregate package. No post-query DIS job is required.

 Copyright © 2026: IHE International, Inc.

3.6.4.5.1 Trigger Events

The DAC receives and validates the permitted aggregate results from participating Information Sources and determines that no protected personal-level processing or SPE is required for release.

3.6.4.5.2 Message Semantics

The release shall identify the request, permit, common query definition, participating sources, node-level result versions, combination method, disclosure-control checks, final aggregate package, and recipient.

The output may use MeasureReport, mADX / ADX, QEDm-oriented aggregate results, DocumentReference, or another approved statistical package. The message shall not contain record-level data or source-local Bulk FHIR files.

Table 3.6.4.5-1: Aggregate Release Evidence

Element	Required meaning
Query definition	Cohort, measures, calculation rules, time period, stratification, coding systems, analytical model and version, and concept-set or cohort-definition identifiers.
Participating nodes	Information Source identifiers, response versions, and execution times.
Combination	Validation, harmonization, weighting, aggregation, and reconciliation method.
Disclosure control	Thresholds, suppression, generalization, rare-category handling, and residual-risk decision.
Final package	Result identifier, format, version, hash, recipient, and release time.

3.6.4.5.3 Expected Actions

The DAC shall release only the approved aggregate package and shall record suppressed, generalized, rejected, or unavailable cells / strata.

The SUA shall treat the result according to the permit and shall not attempt to derive or combine information in a prohibited way.

3.6.5 Security Considerations

The SPE shall prevent unrestricted export of source data, pseudonymized data, intermediate files, logs, caches, screenshots, clipboard content, model checkpoints, and other artifacts not explicitly approved.

Jobs shall execute only with approved tools, identities, data, network routes, and resource limits. Export-control reviewers and automated services shall be separated from the data-user role where policy requires.

Release decisions shall bind the exact artifact hash, recipient, purpose, and channel. Approved delivery capability shall be short-lived and single-purpose.

 Copyright © 2026: IHE International, Inc.

AI/ML artifacts, embeddings, synthetic outputs, explainability artifacts, and detailed subgroup metrics shall be assessed for reconstruction, memorization, leakage, or rare-group disclosure risk when required. Audit records shall correlate request, permit, fulfillment, prepared-data delivery, processing job, output candidate, release decision, recipient, and delivery evidence. Where DIS was used for input preparation, the DIS job/policy/task identifiers remain input-provenance links rather than post-analysis release decisions.

3.6.5.1 Security Audit Considerations

The SUA, SPE, DAC, and DAA where applicable shall audit job submission, dataset use, execution state, tool and version, output candidate creation, release request, policy / review action, transformation, decision, delivery, receipt, publication notification, and deletion. Audit records shall correlate request, permit, fulfillment, delivery, processing job, model / artifact, release, and recipient identifiers.

3.6.5.1.1 Actor Specific Security Considerations

Actor / Role	Specific consideration
Secondary Use Agent	Use only approved identities and tools; do not bypass the export-control workflow.
Secure Processing Environment	Enforce isolation, execution controls, output quarantine, and exact-package release.
Data Access Coordinator	Validate permit, recipient, artifact, and review evidence before authorizing release.
Data Access Authority	Receive oversight or result notifications where required without becoming the uncontrolled payload recipient.

 Copyright © 2026: IHE International, Inc.

3.A1 Audit Event Logging [SU-A1]

3.A1.1 Scope

This transaction records security-relevant and governance-relevant SU-DSX events in an Audit Record Repository. It reuses the IHE ATNA Record Audit Event transaction and adds SU-DSX correlation requirements for requests, decisions, source fulfillment, de-identification, SPE processing, and results release.

3.A1.2 Actor Roles

The roles in this transaction are defined in the following table and may be played by the actors shown. Transaction text specifies behavior for each role; actor-specific behavior is stated where it goes beyond the role.

Table 3.A1.2-1: Actor Roles

Role	Actor(s) and responsibility
Audit Source	Any SU-DSX actor or grouped security application that creates an audit event for an action it performs.
Audit Repository	Audit Record Repository (ARR): receives, validates, protects, indexes, and retains audit messages according to the deployment's audit policy.

3.A1.3 Referenced Standards

- IHE ITI Audit Trail and Node Authentication (ATNA), including Record Audit Event [ITI-20].
- DICOM PS3.15 Audit Message XML schema and coded audit event conventions.
- IHE Consistent Time.
- RFC 5424 syslog transport or the transport required by the applicable ATNA edition and deployment.

3.A1.4 Interaction Diagram

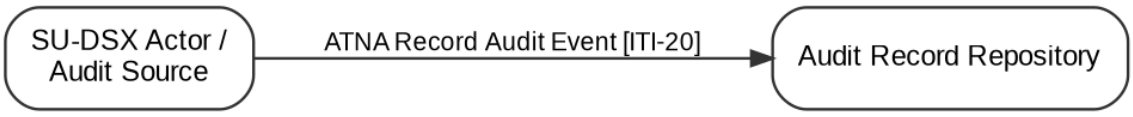


Figure 3.A1.4-1: Audit Event Logging interaction

3.A1.4.1 Record SU-DSX Audit Event

The Audit Source sends an ATNA audit message describing a completed or attempted SU-DSX action and its outcome.

 Copyright © 2026: IHE International, Inc.

3.A1.4.1.1 Trigger Events

An actor receives, sends, validates, rejects, creates, updates, executes, releases, retrieves, deletes, or cancels an SU-DSX artifact or action.

A security or policy event materially changes the authorized workflow, including permit suspension / revocation, destination validation failure, output rejection, or deletion.

3.A1.4.1.2 Message Semantics

The message shall conform to ATNA [ITI-20] and the DICOM Audit Message schema. It shall identify the event, action, outcome, event time, active participants, network access points, audit source, and relevant participant objects.

The event shall include sufficient participant-object identifiers to correlate the SU-DSX request, permit / decision, source fulfillment, DIS job, policy, prepared package, SPE delivery, processing job, output candidate, release decision, and recipient as applicable.

The audit message shall minimize protected content. It should use identifiers, hashes, coded purposes, counts, and references rather than copying complete applications, permits, clinical content, pseudonym mappings, model weights, or sensitive query text.

Table 3.A1.4.1-1: SU-DSX Audit Correlation Objects

Object	Examples of required correlation
Request	Request identifier, version, request type, and applicant organization.
Decision / permit	Decision identifier, version, status, issuer, effective period, and replacement / revocation relationship.
Source fulfillment	Information Source, fulfillment identifier, dataset version, manifest, and destination.
De-identification	DIS job, policy identifier / version, task / transformation run, evidence, and delivery status.
SPE delivery and processing	Delivery, package, workspace, dataset, job, tool / workflow version, and execution outcome.
Release	Output candidate, artifact hash / version, disclosure review, release decision, recipient, and delivery outcome.

3.A1.4.1.3 Expected Actions

The ARR shall validate the audit message, record reception time, protect it from unauthorized modification, and retain it according to policy.

The Audit Source shall detect or surface audit-delivery failures according to ATNA and local policy; failure to send an audit message shall not silently authorize an otherwise prohibited action.

 Copyright © 2026: IHE International, Inc.

Authorized audit analysis shall be able to reconstruct who did what, under which request and permit, using which source / dataset / tool, for which recipient, and with what result or release outcome.

3.A1.5 Security Considerations

Audit transport shall be mutually authenticated and integrity protected. ARR access shall be restricted to authorized audit, security, governance, and oversight functions.

Audit records may themselves be sensitive because they reveal projects, datasets, organizations, query patterns, and processing activity. Retention, access, export, and secondary analysis of audit data shall be governed.

Clock synchronization shall support reliable ordering across multiple jurisdictions and systems.

3.A1.5.1 Security Audit Considerations

This transaction is the audit transaction. In addition to the common ATNA requirements, the audit source shall include the SU-DSX transaction name and correlation identifiers appropriate to the event. Final event-type codes require IHE namespace allocation.

3.A1.5.1.1 Actor-Specific Security Considerations

Actor / Role	Specific consideration
Audit Source	Minimize audit content, ensure correct outcome codes, and monitor delivery failure.
Audit Record Repository	Protect confidentiality and integrity, preserve time ordering, enforce retention, and support authorized correlation queries.

 Copyright © 2026: IHE International, Inc.

Appendices to Volume 2

The following appendices define common cross-transaction requirements and informative binding guidance for SU-DSX Volume 2.

 Copyright © 2026: IHE International, Inc.

Appendix A – Common Control Message, Correlation, and Manifest Requirements

This appendix is normative.

A.1 Common Identifier Model

Every SU-DSX message shall carry the identifiers needed for its transaction and shall preserve the relationships among lifecycle objects. Identifiers shall be globally unique within the trust domain or shall be namespaced by the assigning authority. A versioned object shall retain a stable logical identifier and a distinct version identifier.

Table A.1-1: Common SU-DSX Identifiers

Identifier	Purpose and lifecycle
request-id / request-version	Identifies the secondary-use request and each immutable submitted version.
decision-id / decision-version	Identifies the permit or access decision and each replacement, amendment, suspension, or revocation version.
fulfillment-id	Identifies one source-specific SU-4 fulfillment action.
manifest-id	Identifies the inventory and evidence for a provision or prepared package.
deid-job-id / policy-id / task-id	Correlates the optional DIS workflow without exposing re-identification material.
delivery-id	Identifies one SU-5 delivery and ingest attempt to an SPE or other authorized receiver.
processing-job-id	Identifies one immutable analysis or processing execution.
release-request-id / release-id	Identifies the proposed artifact release and the authoritative release decision / delivery.
dataset / package / artifact id and version	Identifies the exact source data, prepared data, output candidate, and released artifact.
recipient-id / endpoint-id	Identifies the authorized receiving organization, system, and endpoint.

A.2 FHIR Control Message Envelope

For SU-2 through SU-6, the baseline control-plane binding is a FHIR R4 Bundle of type message. The first resource shall be MessageHeader. MessageHeader.focus shall reference the Task that represents the transaction instance. The Bundle shall include or securely reference the resources needed to interpret the message without ambiguous out-of-band assumptions.

- Bundle.identifier shall be unique and shall serve as the message idempotency key unless an explicit idempotency header is used.

 Copyright © 2026: IHE International, Inc.

- MessageHeader.source and destination shall identify the sending and intended receiving endpoints.
- MessageHeader.event shall identify the logical SU-DSX message event. Final event codes and canonical URLs require IHE namespace allocation.
- Task.identifier shall include the relevant SU-DSX lifecycle identifier and assigning authority.
- Task.basedOn, partOf, focus, input, output, owner, requester, restriction, and statusReason shall be used to preserve workflow relationships where applicable.
- Provenance shall identify who created or asserted the message content and when.
- OperationOutcome shall be used for machine-processable errors and warnings.
- Binary payloads shall not be embedded when size, security, or retention requirements favor an approved external transfer or document profile.

A.3 Status, Errors, and Idempotency

A receiver shall return a status that is unambiguously correlated with the incoming message. Retrying the same immutable message with the same idempotency key shall not create a second request, decision, fulfillment, delivery, job, or release action.

Table A.3-1: Common Error Categories

Category	Examples and required handling
authentication / authorization	Unknown identity, insufficient role, wrong organization, invalid purpose, wrong token audience. Reject without disclosing protected details.
integrity / signature	Invalid signature, hash mismatch, corrupted package, altered decision. Quarantine or reject and audit.
version / replay	Duplicate message, stale decision, replaced request, expired permit. Return authoritative known version where permitted.
scope / policy	Dataset, variable, period, source, destination, recipient, or output outside authorization. Reject or partially fulfill only when policy permits.
content / conformance	Unsupported profile, missing reference, invalid coding, malformed FHIR / DICOM / document package. Return OperationOutcome.
availability / capacity	Endpoint unavailable, source delay, SPE capacity, timeout. Return retry guidance without changing authorization.
disclosure / release	Residual identification risk, small cell, leakage, unapproved model artifact, wrong recipient. Block release and record reason.

 Copyright © 2026: IHE International, Inc.

A.4 Authorization and Version Rules

- Every action under SU-3 through SU-6 shall reference the current effective decision / permit version.
- A recipient shall not rely on a cached decision after its validity period or when it has knowledge of suspension, revocation, or replacement.
- A change to purpose, source data scope, destination, SPE, recipient, de-identification requirement, or release class shall require an authorized decision or request version.
- A message shall identify the assigning authority for identifiers that are not globally unique.
- Cross-border workflows may have a common request context and multiple national decisions; each national fulfillment shall identify both the common context and the applicable national decision.

A.5 Common Manifest Requirements

A manifest shall be immutable for a completed provision or delivery. A corrected package shall use a new manifest version and shall identify the package or manifest it replaces. The manifest shall include the minimum fields specified in SU-4 and SU-5 and shall additionally identify:

- content inventory and counts at a level that does not disclose prohibited cohort details;
- source dataset identifiers and versions;
- content formats, implementation guides, coding systems, and profile versions;
- analytical data model and version, vocabulary release, included domains, and ETL or source-to-model transformation provenance where applicable;
- hashes or checksums for files or logical packages;
- creation, transformation, validation, transfer, and expiry timestamps;
- authorized destination and receiver;
- minimization, de-identification, and validation evidence references;
- exceptions, omissions, suppression, or partial-fulfillment status;
- retention and deletion conditions.

A.6 Multiplicity and Distributed Fulfillment

A single SUA may interact with multiple CAT and DAA actors. A single approved request may be distributed through one DAC to multiple IS actors. Each IS fulfillment and each SPE delivery shall be separately identifiable. The DAC shall preserve the many-to-one relationship from source fulfillment and processing results back to the common request and permit context. Combining source results shall not obscure the contribution, version, error, or disclosure status of an individual source.

 Copyright © 2026: IHE International, Inc.

Appendix B – Informative Content and Transport Binding Matrix

This appendix is informative.

B.1 Binding Selection Principles

SU-DSX separates governance and lifecycle orchestration from payload representation and transfer. An implementation selects the content and transport binding appropriate to the authorized data, volume, source location, and processing model. Selection of a binding does not relax permit, minimization, destination, integrity, audit, or release-control requirements.

Table B.1-1: Informative Binding Matrix

Data / interaction	Candidate binding	SU-DSX use
Catalogue metadata	DCAT-compatible application profile; HealthDCAT-AP when the optional HealthDCAT-AP Content Binding is claimed; RDF / JSON-LD, SPARQL or REST search	SU-1 discovery and request preparation, including dataset conformance, quality / utility, data-dictionary references, and transformation capability.
Structured clinical data	FHIR REST and FHIR Bulk Data	SU-4 source provision; SU-5 ingestion where authorized.
IPS / IPS+ content	FHIR document / composition, Bulk FHIR, PCC-1 or document exchange	Informative clinical-content realization for epidemiology and research.
Documents and permit artifacts	MHD, XDR, XDS, XCA, DocumentReference / Binary	Supporting documents, signed decisions, manifests, reports, and release packages.
Radiology / digital pathology	DICOM and DICOMweb	SU-4 and SU-5 imaging provision without conversion to FHIR objects.
Large files / multimodal packages	Secure managed file transfer, object storage, protected repository access	Payload data plane with immutable manifest and short-lived credentials.
Analytical common data model	OHDSI OMOP CDM, standardized vocabularies, database extract / standardized files, controlled endpoint, cohort definitions, and approved analytical packages	Optional SU-1 discoverability, SU-2 / SU-3 scope expression, SU-4 preparation or provision, SU-5 SPE ingestion, and SU-6 local or federated analysis.
Federated aggregate query	FHIR Measure / MeasureReport, QEDm-oriented aggregate operation, ADX / mADX, local Bulk FHIR plus source-side aggregation	SU-4 aggregate response and SU-6 direct non-identifying release.
De-identification workflow	DIS ITI-x1 through ITI-x6	Input preparation, policy resolution, task execution, evidence, and approved delivery.
SPE processing	FHIR Task plus RPE / CRPC / DEX / SDC or approved workflow package	SU-6 job control and reproducibility.

 Copyright © 2026: IHE International, Inc.

Data / interaction	Candidate binding	SU-DSX use
Audit	ATNA [ITI-20] / DICOM AuditMessage	SU-A1 event logging across the lifecycle.

B.2 FHIR Bulk Data Realization of SU-4

1. The DAC sends a Provision Request identifying the permit, source-specific cohort / scope, approved resource types, time period, destination, and Bulk FHIR endpoint.
2. The IS authorizes and initiates the applicable Bulk FHIR export and returns asynchronous status information correlated to the fulfillment identifier.
3. The IS creates an output manifest identifying files, resource types, counts, hashes, errors, and provenance. File URLs use short-lived destination-bound authorization.
4. The approved preparation service or SPE retrieves the files and validates the manifest. The IS and receiver report completion to the DAC.
5. For the federated aggregate use case, Bulk FHIR may be used only inside the source node; record-level export files are not returned to the DAC or requester.

B.3 DICOMweb Realization of SU-4 and SU-5

1. The provision request identifies approved studies, series, instances, modalities, time period, and destination without requiring conversion to FHIR.
2. The IS or grouped imaging archive exposes the authorized objects through DICOMweb retrieve or pushes them through an approved store / transfer path.
3. The preparation workflow applies the permit-defined DICOM de-identification, UID handling, burned-in annotation review, private-tag handling, and validation through the DIS De-Identifier or equivalent approved function.
4. The manifest links imaging objects to permitted structured clinical and outcome data while preserving only the approved pseudonym and linkage scope.
5. The SPE validates the DICOM package and de-identification evidence before use.

B.4 Direct Aggregate Release

In the lighter path, the DAC distributes a common permit-bound query, each IS executes locally, and each IS returns only an authorized aggregate response. The DAC validates and combines the responses, applies or invokes additional disclosure control where necessary, and releases the final non-identifying result through SU-6. The SPE is not invoked unless personal-level or otherwise protected processing is introduced.

B.5 HealthDCAT-AP and OMOP Realization Guidance

HealthDCAT-AP realization. SU-1 supports DCAT-compatible catalogue metadata. Implementations claiming the optional HealthDCAT-AP Content Binding shall conform to the

 Copyright © 2026: IHE International, Inc.

applicable published HealthDCAT-AP version and shall identify that version in endpoint metadata and responses. Catalogue records should expose persistent dataset and distribution identifiers, description and coverage, data-holder and publisher information, access conditions, quality and utility information, data-dictionary or variable-description references, distributions or access services, and conformance statements. A dct:conformsTo statement may identify FHIR implementation guides, OMOP CDM, CDISC, or another applicable model. The record should distinguish native conformance from a transformation service available on request.

OMOP analytical realization. OMOP CDM is an optional harmonization and analysis model used after discovery and authorization; it is not the universal SU-DSX exchange format. A dataset may already be represented in OMOP, may be transformed during permit-bound SU-4 preparation, or may be transformed inside the SPE before SU-6 processing. The location of transformation is governed by the permit, available capabilities, and the deployment trust model.

Table B.5-1: OMOP Placement Across SU-DSX Transactions

SU-DSX stage	Role of OMOP
SU-1 Query Catalogue	Discover whether a dataset natively conforms to OMOP CDM, the supported version and vocabulary release, or whether an OMOP transformation service is available.
SU-2 Submit Request	Express requested variables, cohort criteria, observation periods, temporal rules, exclusions, or minimization scope using OMOP domains and concepts where appropriate.
SU-3 Issue Permit	Authorize the OMOP domains, concepts, population, period, granularity, version constraints, and permitted location of transformation or execution.
SU-4 Authorized Source Data Provision	Provide native source data, an existing OMOP dataset, data prepared for OMOP transformation, or a controlled local OMOP execution target.
Preparation / DIS	Perform minimization, pseudonymization, terminology mapping, ETL into OMOP, and validation when authorized; OMOP transformation is not a substitute for de-identification.
SU-5 Transfer Prepared Data to SPE	Deliver the permit-bound OMOP database extract, standardized files, protected repository, or controlled endpoint together with model, vocabulary, ETL, provenance, and validation metadata.
SU-6 Secure Processing and Results Release	Run approved OHDSI-compatible or other analytical packages against OMOP data and release only the exact disclosure-controlled outputs authorized by the release decision.
Federated aggregate path	Execute a common permit-bound analytical package at locally governed OMOP nodes and return only approved, non-identifying results and node-level provenance.

Manifest requirement. When a provision, delivery, or SPE dataset uses OMOP, the applicable SU-4 or SU-5 manifest shall identify the OMOP CDM version, vocabulary release, included domains, ETL or source-to-OMOP mapping version, transformation provenance, and validation results. These fields enable reproducibility and traceability but do not authorize content beyond the permit.

 Copyright © 2026: IHE International, Inc.

Multimodal realization. OMOP does not replace the FHIR and imaging paths. Structured clinical data may be provisioned through FHIR / Bulk FHIR and transformed into OMOP, while imaging and digital-pathology objects remain in DICOM / DICOMweb or another approved native representation. The OMOP records and native objects may be connected only through permit-bound pseudonyms, controlled identifiers, or references that preserve the authorized linkage scope.

Federated realization. Participating nodes may retain person-level data in locally governed OMOP environments. A common analytical package or query may be distributed to those nodes, executed locally, and subjected to node-level and combined disclosure control. Only the approved aggregate or other non-identifying result is returned through SU-6. SU-DSX does not require every deployment or HDAB to provide federated-computing services.

Volume 2 Namespace Additions

Add the following terms to the IHE General Introduction Appendix G:

No final OIDs, UIDs, URNs, canonical URLs, FHIR profile URLs, message event codes, or audit event-type codes are assigned in this draft. Before Trial Implementation, IHE namespace allocation is required for the SU-DSX canonical package, FHIR message events, any FHIR profiles or extensions, any value sets / code systems, and SU-DSX-specific audit event type codes. DIS ITI-x1 through ITI-x6 identifiers shall be replaced with the identifiers assigned by the final DIS profile.

 Copyright © 2026: IHE International, Inc.

Volume 3 – Content Modules

This volume defines the semantic content used by the SU-DSX control plane and the metadata/evidence that accompanies authorized payloads. Transaction sequencing, actor behavior, transport, authorization, and audit transport are defined in Volumes 1 and 2. External implementation guides remain authoritative for FHIR Bulk Data, DICOM/DICOMweb, HealthDCAT-AP, OMOP CDM, document sharing, and DIS.

SU-DSX uses a FHIR R4 message-based control plane for request, decision, source fulfillment, prepared-data delivery, processing, results release, and related lifecycle coordination. Source health-data payloads remain technology-neutral and may use FHIR/Bulk FHIR, DICOM/DICOMweb, document exchange, secure file or object transfer, an approved analytical representation such as OMOP CDM, or a controlled federated execution pattern.

Normative language. SHALL and SHALL NOT identify conformance requirements. SHOULD identifies recommended behavior. MAY identifies permitted behavior. New canonical URLs, CodeSystem identifiers, ValueSet identifiers, FHIR profiles, extensions, and audit codes are provisional until allocated through the IHE publication process.

FHIR Maturity Model

This profile incorporates content from Release 4 of the HL7® FHIR® specification (FHIR R4, version 4.0.1). HL7 assigns maturity levels to FHIR content using the FHIR Maturity Model (FMM), ranging from level 0 for the least mature content through higher maturity levels and N for Normative content. The FMM level reflects the maturity of the underlying FHIR specification content and does not represent the maturity of the SU-DSX Integration Profile itself.

The FMM levels below are those published for FHIR R4 (4.0.1) content used directly by this Volume 3. Implementers SHOULD consider the maturity of the underlying FHIR resources when assessing implementation stability and the potential effect of future FHIR-version changes.

FHIR Content	FMM Level	Use in SU-DSX Volume 3
Bundle	N	Common SUC message envelope; Normative in FHIR R4.
MessageHeader	4	Common SUC event/source/destination/focus content.
Task	2	Workflow instance and lifecycle status across SU-2 through SU-6.
Provenance	3	Submission, decision, transformation, execution, and release provenance.
OperationOutcome	N	Machine-processable errors and warnings; Normative in FHIR R4.

 Copyright © 2026: IHE International, Inc.

FHIR Content	FMM Level	Use in SU-DSX Volume 3
QuestionnaireResponse	3	Structured secondary-use application/request content.
ResearchStudy	1	Optional project/study context.
PlanDefinition	2	Optional computable processing or analysis plan.
ActivityDefinition	2	Optional executable activity definition for processing jobs.
Group	1	Optional cohort/population definition.
Organization	3	Applicant, authority, source, destination, and other organizations.
PractitionerRole	2	Authorized representatives and responsible roles.
Contract	1	Candidate machine-actionable representation of permit/access-decision terms.
Endpoint	2	Authorized source, delivery, SPE, repository, or federated endpoints.
List	1	Manifest inventory of package entries.
DocumentReference	3	Supporting documents, manifests, output candidates, and evidence packages.
Binary	N	Referenced binary/document payload where used; Normative in FHIR R4.
Measure	2	Optional aggregate/indicator/query definition.
MeasureReport	2	Aggregate/statistical result representation.
CodeSystem	N	Machine-readable SU-DSX terminology artifacts; Normative in FHIR R4.
ValueSet	N	Machine-readable SU-DSX value sets; Normative in FHIR R4.
StructureDefinition	N	Machine-readable SU-DSX profiles/extensions; Normative in FHIR R4.

Source: HL7 FHIR R4 (4.0.1) Resource Index and FHIR Maturity Model. "N" denotes Normative content.

Because Contract is FMM 1, SU-DSX does not rely on Contract alone as the authoritative permit representation. The access decision is bound through the Access Decision / Permit Content

 Copyright © 2026: IHE International, Inc.

Module (SUAD) content module using the decision identifiers and workflow context, with Contract as a candidate machine-actionable representation and DocumentReference/Provenance available for the authoritative human-readable decision and integrity evidence.

 Copyright © 2026: IHE International, Inc.

5 Namespaces and Vocabularies

Add to section 5 Namespaces and Vocabularies

No final SU-DSX OIDs, UIDs, canonical URLs, FHIR profile URLs, MessageHeader event codes, or audit event-type codes are assigned in the current draft. The entries below therefore identify the exact namespace categories that require IHE allocation before Trial Implementation.

5.1 SU-DSX Code Systems

The final codeSystem identifiers below are to be assigned by IHE. The code-system names are normative logical names for this draft. Implementations SHALL NOT treat "TBD by IHE" as a production identifier.

codeSystem	codeSystemName	Description
TBD by IHE	SU-DSX Message Event	Logical message events for SU-2 through SU-6.
TBD by IHE	SU-DSX Request Type	Distinguishes a data access application from an anonymized statistical data request.
TBD by IHE	SU-DSX Decision Status	Permit/access-decision lifecycle states.
TBD by IHE	SU-DSX Fulfillment Status	Source preparation, feasibility, provision, correction, and completion states.
TBD by IHE	SU-DSX Delivery Status	Prepared-data delivery, quarantine, acceptance, rejection, and failure states.
TBD by IHE	SU-DSX Processing Status	Permit-bound processing-job execution states.
TBD by IHE	SU-DSX Release Status	Output review, transformation, approval, rejection, delivery, and closure states.
TBD by IHE	SU-DSX Output Class	Classes of ordinary, aggregate/statistical, model, synthetic, and other controlled outputs.
TBD by IHE	SU-DSX Data Representation	FHIR/Bulk FHIR, DICOM, document, secure-file, OMOP, controlled-endpoint, and federated representations.

5.2 IHE FormatCode, ActCode, and RoleCode Additions

No additions are required to the IHE FormatCode, ActCode, or RoleCode vocabularies for SU-DSX in this draft. Where an implementation exchanges a managed document using MHD, XDS, XDR, or XCA, it SHALL use the applicable existing format code and media type. SU-DSX actors are defined as IHE actor roles in Volume 1 rather than as new IHE RoleCode values.

 Copyright © 2026: IHE International, Inc.

5.3 SU-DSX Canonical FHIR Artifacts

Table 5.3-1: Provisional canonical artifact patterns

Artifact class	Provisional logical pattern	Status
FHIR profiles	[SU-DSX-CANONICAL-ROOT]/StructureDefinition/<logical-id>	Pending IHE allocation
FHIR extensions	[SU-DSX-CANONICAL-ROOT]/StructureDefinition/<extension-id>	Only where standard FHIR elements are insufficient; pending IHE allocation
Code systems	[SU-DSX-CANONICAL-ROOT]/CodeSystem/<logical-id>	Pending IHE allocation
Value sets	[SU-DSX-CANONICAL-ROOT]/ValueSet/<logical-id>	Pending IHE allocation
Message events	[SU-DSX-CANONICAL-ROOT]/CodeSystem/message-event#<code>	Pending IHE allocation
Implementation package	ihe.qrph.su-dsx	Provisional package name

5.4 Required Value Sets

Table 5.4-1: SU-DSX value sets used by the content modules

Value set	Core codes in this draft
SU-DSX Request Type	data-access-application; anonymized-statistical-request
SU-DSX Decision Status	approved; partially-approved; denied; amendment-required; suspended; revoked; expired; replaced
SU-DSX Fulfillment Status	requested; feasibility-review; feasible; partially-feasible; not-feasible; awaiting-confirmation; preparing; delayed; blocked; completed; completed-with-deviation; corrected; cancelled; failed
SU-DSX Delivery Status	notified; transferring; quarantined; accepted; accepted-partial; rejected; failed; replaced; deleted
SU-DSX Processing Status	queued; running; paused; completed; failed; cancelled; closed
SU-DSX Release Status	requested; under-review; transformation-required; approved; rejected; delivered; delivery-failed; withdrawn; closed
SU-DSX Output Class	aggregate-result; statistical-table; report; visualization; model-artifact; synthetic-data; software-or-workflow; publication-package; ordinary-research-output; other
SU-DSX Data Representation	fhir-rest; fhir-bulk; dicomweb; ihe-document; secure-file; object-store; omop-cdm; controlled-endpoint; remote-execution; federated-aggregate

 Copyright © 2026: IHE International, Inc.

5.5 Message Event Codes

Table 5.5-1: Logical SU-DSX message event codes

Code	Meaning
submit-request	SU-2 request submission
request-acknowledgement	SU-2 technical/administrative acknowledgement
application-status-update	SU-2/SU-3 request lifecycle update where used
access-decision	SU-3 permit/access decision or later decision version
decision-receipt	SU-3 decision validation/receipt
preparation-request	SU-4 source preparation/provision request
feasibility-cost-response	SU-4 source feasibility and cost response where used
confirmed-preparation-specification	SU-4 confirmed source-preparation specification where used
provision-status	SU-4 source fulfillment status or deviation
provision-result	SU-4 terminal result and manifest
provision-change	SU-4 correction/cancellation/supersession
delivery-notice	SU-5 prepared-data delivery notice
delivery-acknowledgement	SU-5 ingest/quarantine/acceptance acknowledgement
processing-job	SU-6 processing-job submission
processing-status	SU-6 execution status
release-request	SU-6 output-candidate release request
release-decision	SU-6 authoritative release decision
released-result	SU-6 approved result delivery
aggregate-release	SU-6 direct non-identifying aggregate release
lifecycle-closure	SU-6 final closure/deletion evidence where applicable

2310

 Copyright © 2026: IHE International, Inc.

6 Content Modules

SU-DSX defines no new CDA Document, Header, Section, or Entry Content Module.

 Copyright © 2026: IHE International, Inc.

7 DICOM Content Modules

SU-DSX does not define a new DICOM IOD, SOP Class, or DICOM Content Module. DICOM and DICOMweb are external payload bindings for imaging and digital pathology. The SU-DSX manifest preserves authorized study/series/instance scope, object inventory, integrity, de-identification evidence, permitted linkage, and destination information.

7.1 DICOM Payload Binding Requirements

Table 7.1-1: DICOM payload-binding evidence

Requirement	SU-DSX constraint
Object inventory	Manifest SHALL identify study/series/SOP Instance scope, counts, relevant modalities, package/endpoint identity, and integrity information.
De-identification evidence	Where de-identification is required, evidence SHALL identify the applicable confidentiality profile or policy, processing stage, responsible service, and outcome without exposing re-identification material.
Private attributes	Handling of private attributes SHALL be declared, including retained private blocks where explicitly authorized.
Burned-in text	Assessment and treatment of burned-in or rendered identifiers SHALL be recorded where applicable.
UID transformation	The UID retention/remapping policy SHALL be recorded, including linkage-preserving behavior authorized by the permit.
Pathology images	Label images, macro images, annotations, and other potentially identifying visual content SHALL be assessed and treatment recorded.
Derived objects	Segmentation, structured reports, annotations, measurements, and derived objects SHALL preserve authorized referential linkage or document the loss of linkage.
Pixel transformation	Lossless/lossy or other pixel transformations SHALL be declared where they affect utility, fidelity, or validation.
Quality limitations	Manifest SHOULD state image-quality limitations, missing series/objects, unsupported objects, or transformations relevant to fitness for use.

 Copyright © 2026: IHE International, Inc.

8 FHIR and Other Content Modules

SU-DSX uses FHIR R4 message Bundles as the baseline control content for SU-2 through SU-6. The content modules below constrain those messages and the metadata/evidence that accompanies external payloads. They are transport-neutral: FHIR/Bulk FHIR, DICOM/DICOMweb, document exchange, secure file/object transfer, OMOP CDM, and federated execution remain external payload or analytical bindings.

8.1 Content Module Inventory and Transaction Binding

Table 8.1-1: SU-DSX content module inventory

Content module	Transaction(s)	Opt.	Principal artifacts
Common FHIR Control Message (SUC)	SU-2 through SU-6	R	Bundle, MessageHeader, Task, Provenance, OperationOutcome
Secondary Use Request (SURQ)	SU-2	R	QuestionnaireResponse, ResearchStudy, PlanDefinition, Group, DocumentReference, Organization, PractitionerRole
Access Decision / Permit (SUAD)	SU-3	R	Contract, Task, DocumentReference, Provenance, Endpoint
Source Provision and Manifest (SUPM)	SU-4	R	Task, List, DocumentReference, Endpoint, Group, Measure/MeasureReport, Provenance
Prepared Data Delivery (SUDL)	SU-5	C	Task, List, DocumentReference, Endpoint, Provenance, OperationOutcome
Processing Job (SUPJ)	SU-6	C	Task, PlanDefinition, ActivityDefinition, ResearchStudy, Group, Measure, DocumentReference
Results Release (SURL)	SU-6	R	Task, Contract, DocumentReference, MeasureReport, Provenance, OperationOutcome
Aggregate Result Package (SUAR)	SU-4 / SU-6	C	Measure, MeasureReport, DocumentReference, Provenance
Audit Correlation Content (SUAC)	SU-A1	R	ATNA / DICOM AuditMessage with SU-DSX correlation identifiers
HealthDCAT-AP Catalogue Binding	SU-1	O	External RDF/DCAT application-profile content

 Copyright © 2026: IHE International, Inc.

Content module	Transaction(s)	Opt.	Principal artifacts
OMOP Analytical Representation Binding	SU-1 through SU-6	O	External OMOP CDM/vocabulary/ETL/validation metadata

R = required when the stated transaction is used; C = conditional for the applicable workflow path; O = optional external content binding.

8.2 Common FHIR Control Message Content Module (SUC)

8.2.1 Purpose and Conformance Statement

SUC provides the common envelope, workflow identity, provenance, versioning, recipient binding, and error-handling rules for SU-2 through SU-6. A conforming FHIR control message SHALL be a FHIR R4 Bundle with type = message. The first Bundle entry SHALL be MessageHeader. MessageHeader.focus SHALL reference the Task that represents the transaction instance.

Table 8.2.1-1: Common message constraints

FHIR element / artifact	Cardinality	SU-DSX constraint
Bundle.type	1..1	Fixed to message.
Bundle.identifier	1..1	Globally unique message identifier and idempotency key unless an equivalent transport idempotency mechanism is profiled.
Bundle.timestamp	1..1	Time the immutable message instance was assembled.
Bundle.entry[0].resource	1..1	MessageHeader conforming to the SU-DSX MessageHeader profile.
MessageHeader.event[x]	1..1	Code from the SU-DSX Message Event value set.
MessageHeader.source	1..1	Sending endpoint identity.
MessageHeader.destination	1..*	Intended recipient endpoint(s); recipients SHALL be explicitly bound.
MessageHeader.focus	1..1	Reference to the authoritative SU-DSX Workflow Task.
Task.identifier	1..*	Contains the transaction-specific lifecycle identifier and assigning authority.
Task.basedOn / partOf	0..*	Preserves request, decision, fulfillment, delivery, job, and release relationships.
Provenance	1..*	Identifies who asserted the message content, when, and the affected resources/version.

 Copyright © 2026: IHE International, Inc.

FHIR element / artifact	Cardinality	SU-DSX constraint
OperationOutcome	0..1	Required when the message reports a machine-processable error or warning.

8.2.2 Common Lifecycle Identifiers

Table 8.2.2-1: Core lifecycle identifiers

Identifier	Purpose and propagation
request-id / request-version	Secondary-use request and immutable submitted version; preserved through downstream actions.
decision-id / decision-version	Permit/access decision and replacements; required for actions authorized by SU-3.
fulfillment-id	One source-specific SU-4 preparation/provision action.
manifest-id / manifest-version	Immutable or versioned inventory/evidence package; corrected packages use a new version and replacement relation.
delivery-id	One SU-5 delivery/ingest attempt.
workspace-id	Authorized SPE/project workspace where applicable.
processing-job-id	One immutable controlled execution.
release-request-id / release-id	Output review request and authoritative release decision/delivery.

Deployments MAY define additional lifecycle identifiers for application-case management, holder consultation, fees, appeals, opt-out evidence, trusted-holder recognition, intermediaries, incidents, significant findings, publication notification, deletion evidence, or cross-border decision components. Such identifiers SHALL be carried only when the applicable governance model requires them and SHALL NOT make SU-DSX jurisdiction-specific.

8.2.3 Versioning, Idempotency, and Reference Rules

- A business object SHALL retain a stable logical identifier and SHALL use a distinct immutable version identifier for each submitted, issued, corrected, replaced, suspended, or revoked version.
- Retrying an unchanged message with the same idempotency key SHALL NOT create a duplicate business action.
- A receiver that knows a newer authoritative version SHALL reject or safely ignore a stale version and SHOULD return the known authoritative version when policy permits.
- Referenced resources SHALL be contained in the Bundle, resolvable through an authorized endpoint, or exchanged through an approved document/payload binding.
- Reusable credentials, pseudonym mappings, re-identification keys, and privileged disclosure-control parameters SHALL NOT be placed in the general control Bundle.

 Copyright © 2026: IHE International, Inc.

8.3 Secondary Use Request Content Module (SURQ)

8.3.1 Purpose

SURQ represents a structured data access application or anonymized statistical data request submitted through SU-2. It captures the applicant, purpose, requested data, linkage, methods, safeguards, expected outputs, and supporting artifacts while preserving the authoritative human-readable application where required.

Table 8.3.1-1: SURQ resource constraints

FHIR element / artifact	Cardinality	SU-DSX constraint
SUC Bundle / MessageHeader / Task	1..1	Event submit-request; Task carries request-id/version.
QuestionnaireResponse	1..*	Primary structured application/request content.
ResearchStudy	0..1	Study/project context where applicable.
PlanDefinition	0..1	Analysis or processing plan when a computable representation is useful.
Group	0..*	Cohort or population definition.
Organization / PractitionerRole	1..*	Applicant organization, responsible person, team, and relevant roles.
DocumentReference	0..*	Protocol, ethics/regulatory evidence, data-management plan, contracts, declarations, or other supporting artifacts.
Provenance	1..*	Submitter, submission time, version lineage, and source of supporting evidence.

8.3.2 Required Request Semantics

Table 8.3.2-1: Required SURQ semantics

Semantic group	Required meaning
Request identity	Request identifier/version, creation/submission time, previous-version relationship, and request type.
Applicant	Applicant organization, authorized representative, contact details required by the application process, and delegation where applicable.
Purpose and project	Requested purpose category, project title, public summary where applicable, scientific or operational objective, protocol, and expected benefit.

 Copyright © 2026: IHE International, Inc.

Semantic group	Required meaning
Requested data	Catalogue identifiers/versions, datasets, variables, modalities, cohort criteria, period, geography, source organizations, and minimization scope.
Linkage and combination	Requested linkage, other data to be combined, linkage strategy, and permitted longitudinal/cross-source scope.
Methods and environment	Analysis plan, tools, compute needs, SPE/federated approach, reproducibility information, and requested analytical representation.
Data protection and safeguards	Minimization rationale, de-identification expectations, security, retention, deletion, and incident handling.
Expected outputs	Reports, aggregates, models, synthetic outputs, software/workflow artifacts, publications, and requested release classes.
Supporting artifacts	Protocol, ethics/regulatory evidence, data-management plan, contracts, declarations, and other required attachments.

8.3.3 Conditional Governance Extensions

Where required by the applicable governance model, SURQ MAY additionally carry public-interest justification, research-team qualifications, processor/subcontractor information, conflict-of-interest declarations, fee/billing context, application-case identifiers, publication/report-back plans, acceptable-use commitments, and cross-border coordination information.

8.3.4 OMOP Scope Expression

When an OMOP analytical realization is requested, SURQ MAY identify OMOP domains, concept identifiers, concept sets, descendant rules, observation periods, temporal relationships, exclusion criteria, requested CDM version, and vocabulary release. These computable expressions supplement and SHALL NOT replace the authoritative request text and catalogue references.

8.4 Access Decision / Permit Content Module (SUAD)

8.4.1 Purpose

SUAD represents the authoritative outcome of request assessment. It supports approval, partial approval, denial, amendment request, suspension, revocation, expiry, and replacement. It binds the authorized purpose, data scope, fulfillment, destination, de-identification requirements, processing constraints, and output-release conditions.

 Copyright © 2026: IHE International, Inc.

Table 8.4.1-1: SUAD resource constraints

FHIR element / artifact	Cardinality	SU-DSX constraint
SUC Bundle / MessageHeader / Task	1..1	Event access-decision; Task carries decision workflow status and relationship to the request.
Contract	1..1	Machine-actionable permit/access-decision terms and obligations.
DocumentReference	0..*	Signed human-readable permit, denial, amendment request, or referenced evidence.
Organization / PractitionerRole	1..*	Issuing authority, applicant recipient, DAC, holders/sources, reviewers, and relevant responsible parties.
Endpoint	0..*	Authorized source, recipient, SPE, intermediary, or other fulfillment endpoint.
Provenance	1..*	Issuer, decision time, signature/integrity evidence, version lineage, and authority.

8.4.2 Required Decision Semantics

Table 8.4.2-1: Required SUAD semantics

Semantic group	Required meaning
Decision identity	decision-id/version, request-id/version, status, effective period, and replacement/suspension/revocation relationships.
Issuer and authority	Issuing organization, responsible role, jurisdiction/trust domain where applicable, and integrity/signature evidence.
Authorized purpose and scope	Approved purpose, datasets, sources, cohort, variables, modalities, periods, geography, linkage, granularity, and permitted transformations.
Fulfillment and destination	DAC, Information Sources, authorized recipients, SPE/workspace requirements, endpoints, federated nodes, and processing location.
De-identification requirements	Minimization, pseudonymization, anonymization/disclosure-control requirements, policy references, and validation requirements.
Processing and release	Permitted tools/methods, monitoring, retention, output classes, review route, recipient restrictions, publication/reporting conditions, and deletion/closure obligations.

 Copyright © 2026: IHE International, Inc.

8.4.3 Conditional Governance Extensions

Where required by the applicable governance model, SUAD MAY carry holder-consultation evidence, fee/payment conditions, appeal/redress information, opt-out or privacy-preference enforcement conditions, trusted-holder or intermediary arrangements, significant-finding procedures, national decision components, and other jurisdictional restrictions. Recipient-specific views SHALL remain semantically consistent with the same authoritative decision identifier/version.

8.5 Source Provision and Manifest Content Module (SUPM)

8.5.1 Purpose

SUPM represents the bidirectional SU-4 source-preparation and Authorized Source Data Provision workflow. It binds one source-specific fulfillment action to the effective decision and may carry preparation instructions, feasibility/cost information where used, status/deviation, result/manifest, correction/cancellation, and completion evidence. The module carries metadata/evidence around the payload; the payload itself may use an approved external binding.

Table 8.5.1-1: SUPM resource constraints

FHIR element / artifact	Cardinality	SU-DSX constraint
SUC Bundle / MessageHeader / Task	1..1	Event identifies the applicable SU-4 phase; Task.identifier includes fulfillment-id.
Task.basedOn	1..*	References the effective decision/permit and request.
Group	0..*	Cohort/population definition where appropriate.
List	0..1	Manifest inventory of files, FHIR resources, DICOM objects, documents, aggregates, repositories, or endpoint references.
DocumentReference	0..*	Preparation specification, manifest, feasibility statement, data-quality statement, or evidence package.
Endpoint	0..*	Authorized retrieval/upload, protected repository, OMOP, remote, federated, or destination endpoint.
Measure / MeasureReport	0..*	Source-local aggregate query definition/result when using a statistical/federated path.
Organization	0..*	Information Source, trusted holder/intermediary where applicable, responsible authority, and destination.

 Copyright © 2026: IHE International, Inc.

FHIR element / artifact	Cardinality	SU-DSX constraint
Provenance	1..*	Source extraction/query, transformation/ETL, validation, and package creation.
OperationOutcome	0..1	Safe reasons for non-feasibility, deviation, correction, rejection, or failure.

8.5.2 SU-4 Message Phases

2405 **Table 8.5.2-1: SU-4 content phases**

Message phase	Required content
Preparation Request	Requested scope, minimization, variables/cohort, linkage, de-identification location where applicable, destination, format, due date, and acceptance criteria.
Feasibility Response	Availability, earliest delivery, effort/capacity, data-quality limitations, linkage dependencies, required transformations, and other constraints.
Confirmed Preparation Specification	Final scope, minimization, variables/cohort, linkage, preparation/de-identification path, destination, format, due date, acceptance criteria, and correction rules.
Provision Status / Deviation Notice	Status, estimated completion, delay/block reason, deviations, and correction/supersession relationships.
Provision Result and Manifest	Immutable provision result, payload inventory, data-quality/transformation evidence, destination, and source completion status.
Change / Correction / Cancellation	Versioned amendment, cancellation, corrected package/manifest, superseded version, and safe reason.

8.5.3 Provision Manifest

Table 8.5.3-1: Minimum SUPM manifest semantics

Manifest element	Required meaning
Identity and correlation	manifest-id/version; fulfillment-id; request and decision identifiers/versions; source and destination.
Source and extraction	Dataset/source identifiers/versions, extraction/query time, parameters, and applicable source/target vocabulary versions.
Payload inventory	Files, FHIR resources, DICOM studies/series/instances, documents, aggregates, OMOP repository/package, or controlled endpoint references.
Integrity	Sizes, hashes/checksums, signatures where used, packaging, and transfer-integrity evidence.

 Copyright © 2026: IHE International, Inc.

Manifest element	Required meaning
Content conformance	Formats, profiles/IGs, coding systems, analytical model/version, OMOP CDM/vocabulary versions where applicable, and validation results.
Minimization and transformation	Selection/exclusion, de-identification stage, terminology mapping, ETL/source-to-model transformation, and evidence references.
Data-quality statement	Known completeness, timeliness, coding/mapping, availability, and fitness-for-use limitations.
Exceptions	Unavailable, omitted, suppressed, rejected, failed, or unsupported items with safe reason codes.
Destination and status	Authorized destination, transfer status, completion time, acknowledgement expectation, and retention/deletion conditions.

8.5.4 Conditional Governance Evidence

Where required by the decision or applicable governance model, the manifest MAY reference privacy-preference/opt-out enforcement evidence, trusted-holder recognition, intermediary assignment, fee/cost acceptance, IP/trade-secret conditions, or other fulfillment evidence. Such evidence SHALL be minimized and SHALL NOT expose re-identification material.

8.6 Prepared Data Delivery Content Module (SUDL)

8.6.1 Purpose

SUDL represents the authorized SU-5 notice, expected package, ingest constraints, and acknowledgement for prepared data delivered to an SPE or other approved controlled destination. It preserves correlation among the decision, source fulfillment, DIS evidence where used, package manifest, delivery method, and target workspace.

Table 8.6.1-1: SUDL required semantics

Element group	Required meaning
Delivery identity	delivery-id/version, package/manifest, source fulfillment, sender, receiver, and idempotency key.
Authorization context	decision-id/version, validity period, purpose, recipient/SPE binding, and applicable destination restrictions.
Expected package	Dataset/package identity, manifest, size, format, profiles, checksums, analytical metadata, and de-identification evidence where applicable.
Workspace readiness	workspace-id, approved users/roles, validity, approved tools, compute/storage limits, network policy, and logging/monitoring controls where applicable.

 Copyright © 2026: IHE International, Inc.

Element group	Required meaning
Delivery method	DIS delivery, Bulk FHIR, DICOMweb, document exchange, secure file/object retrieval, OMOP package/repository, mount, remote access, or federated endpoint.
Activation condition	Prepared data SHALL NOT be exposed to users solely because ingest succeeded; access starts only when workspace and authorization conditions are active.
Quarantine	Reason, correction route, time limit, delete/replace rule, partial-use decision, and incident escalation where applicable.
Retention and deletion	Retention start, scheduled deletion/trigger, workspace closure, legal hold where applicable, and deletion evidence.

8.6.2 Ingest Acknowledgement

The receiving SPE or controlled destination SHALL return an outcome from the SU-DSX Delivery Status value set. For quarantined, rejected, partial, or failed outcomes, OperationOutcome SHALL identify a safe reason and the correction/replacement route.

8.7 Processing Job Content Module (SUPJ)

8.7.1 Purpose

SUPJ represents a permit-authorized analysis, validation, benchmark, model-development, or other processing activity executed in an SPE or approved controlled node. It binds the exact input data, toolchain, parameters, authorization context, and expected outputs to an immutable processing-job identifier.

Table 8.7.1-1: SUPJ required semantics

Element group	Required meaning
Job identity	processing-job-id, immutable version, submission time, requester, project, and workspace-id where applicable.
Authorization	decision-id/version, validity, purpose, processing class, and authorized user/team membership.
Inputs	Authorized delivery/dataset, source manifests, cohort, linkage scope, analytical model/version, and input versions.
Execution definition	Plan/workflow, container/package, version/digest, parameters, network policy, and reproducibility metadata.
Resources and limits	CPU/GPU/memory/storage, runtime, concurrency, and cost/quota constraints where used.
Expected outputs	Named output candidates, formats, classifications, intended recipients, and expected receiver-safe evidence.
Output restrictions	Permitted output classes, disclosure thresholds, prohibited exports, privacy/model tests, and review route.

 Copyright © 2026: IHE International, Inc.

Element group	Required meaning
Status and evidence	Queued/running/completed/failed/closed; dataset/tool versions, execution times, output hashes, and incident references where applicable.

8.7.2 OMOP Analytical Job

An OMOP-based job SHALL identify the OMOP CDM version, vocabulary release, cohort/concept-set identifiers and versions, analytical package/version/hash, input database or endpoint, relevant validation status, and any mapping or temporal/unit assumptions needed to reproduce the authorized analysis.

8.8 Results Release Content Module (SURL)

8.8.1 Purpose

SURL represents the controlled output-review and release workflow. It separates completion of processing from authorization to release and binds the exact output candidate, artifact hash/version, output class, recipient, review evidence, transformation, decision, and delivery channel. Post-analysis output review and treatment are governed by SURL/SU-6 and are not modeled as DIS de-identification jobs; DIS references may be carried only as input-preparation provenance.

Table 8.8.1-1: Output Release Request semantics

Element group	Required meaning
Request identity	release-request-id, processing job, output candidate, artifact version/hash, and requester.
Output classification	SU-DSX Output Class plus applicable sensitivity/disclosure classification.
Purpose and recipient	Permitted purpose, intended recipient organization/person/system, and delivery endpoint.
Requested release	Exact files/resources/model/synthetic artifacts, format/package, and proposed publication or use.
Disclosure/privacy evidence	Applicable statistical-disclosure, privacy/leakage, small-cell, rare-category, or other review evidence required by the decision.
Requested transformations	Aggregation, suppression, generalization, redaction, date/geography transformation, provider grouping, synthetic generation, or other output-control treatment.

 Copyright © 2026: IHE International, Inc.

Table 8.8.1-2: Output Release Decision semantics

Element group	Required meaning
Decision identity	release-id/version, decision time, reviewer/service, and relationship to the release request.
Status	requested; under-review; transformation-required; approved; rejected; delivered; delivery-failed; withdrawn; closed.
Approved artifact	Exact artifact/package identifier, version, hash, format, receiver-safe evidence, and approved recipient/channel.
Conditions	Expiry, single-use/short-lived access, publication wording, retention, onward-use restrictions, and other release conditions.
Transformation evidence	Output-control method/parameters, validation, and de-identification/anonymization or DIS evidence where applicable.
Delivery outcome	Recipient acknowledgement, delivery time, failure reason, and retry/correction relationship.
Closure	Processing/release closure, workspace deactivation, deletion or retained-artifact/legal-hold evidence where applicable.

8.8.2 AI/ML, Synthetic, and Other High-Dimensional Outputs

For model weights, embeddings, synthetic data, explainability artifacts, detailed subgroup metrics, or other high-dimensional outputs, SURL shall identify the privacy/disclosure tests required by the decision. Approval shall bind the exact artifact hash and shall not authorize later modified artifacts. Any authorized transformation performed during release control shall produce a new artifact identifier/version/hash.

8.8.3 Significant-Finding Handling

Where the applicable authorization enables significant-finding handling, SURL MAY reference a controlled significant-finding assessment and routing record. The data user SHALL NOT receive re-identification material merely to enable contact. Identification or notification, where applicable, remains subject to the authorized governance procedure and is outside the normal result-release payload.

8.9 Aggregate Result Package Content Module (SUAR)

8.9.1 Purpose

SUAR supports approved statistical-data requests and federated aggregate workflows in which personal-level data remain at the source and only authorized non-identifying results are returned. It SHALL NOT carry source-local record-level Bulk FHIR files or other person-level extracts.

 Copyright © 2026: IHE International, Inc.

Table 8.9.1-1: SUAR required aggregate evidence

Element	Required meaning
Query definition	Cohort, measures, calculation rules, period, stratification, coding systems, analytical model/version, and concept/cohort identifiers.
Participating nodes	Source identifiers, node versions, execution times, and unavailable/rejected nodes.
Compatibility	Common analytical-package hash, CDM/vocabulary compatibility where applicable, concept-set version, and execution attestation.
Combination	Validation, harmonization, weighting, aggregation, and reconciliation method; incompatible results SHALL NOT be silently combined.
Node disclosure decision	Each node's disclosure-control outcome and any local suppression/generalization where applicable.
Failure semantics	Unavailable-node handling, timeout, partial-result policy, retry/cancellation, and impact on interpretation.
Final disclosure control	Thresholds, suppression, generalization, rare-category handling, and residual-risk decision where required.
Final package	Result identifier/version/hash, format, participating-node evidence, recipient, and release time.

8.10 Audit Correlation Content Module (SUAC)

8.10.1 Purpose

SUAC constrains the SU-DSX content associated with Audit Event Logging [SU-A1]. The audit transport and base message format are defined by ATNA Record Audit Event [ITI-20] and the DICOM Audit Message schema. SUAC adds lifecycle correlation so authorized audit analysis can reconstruct the request, decision, source fulfillment, de-identification, prepared-data delivery, processing, release, recipient, and outcome as applicable.

Table 8.10.1-1: SUAC correlation objects

Object	Required correlation
Request	request-id/version, request type, applicant organization where applicable.
Decision / permit	decision-id/version, status, issuer, effective period, replacement/revocation relationship.
Source fulfillment	Information Source, fulfillment-id, dataset version, manifest/package, destination.
De-identification	DIS job/policy/task identifiers and receiver-safe evidence where DIS is used.

 Copyright © 2026: IHE International, Inc.

Object	Required correlation
SPE delivery and processing	delivery-id, workspace-id, package, dataset, processing-job-id, tool/workflow version, and execution outcome.
Release	release-request-id/release-id, output candidate, artifact hash/version, review decision, recipient, and delivery outcome.
Closure	Deletion/closure evidence and incident reference where applicable.

8.11 HealthDCAT-AP Catalogue Content Binding

8.11.1 Status and External Dependency

HealthDCAT-AP is an optional EHDS-oriented external content binding for Query Catalogue [SU-1]. SU-DSX does not reproduce or fork HealthDCAT-AP. An implementation claiming this binding SHALL identify the exact published HealthDCAT-AP release/profile URI used by each returned record. A deployment MAY instead use another declared DCAT-compatible application profile.

Table 8.11.1-1: SU-DSX catalogue expectations

Metadata category	SU-DSX expectation
Persistent identity/version	Dataset/data-service/distribution identifiers and record version/modification information.
Description and coverage	Title, summary, keywords, population/geography/organization/time, limitations, and approximate volume where published.
Publisher and holder	Responsible publisher and data-holder identity plus contact/application route.
Access path	Applicable data access application or statistical-data-request path and access conditions.
Distribution and data service	Available formats/endpoints, access service, SPE/federated capability, and transformation service where advertised.
Variable/data dictionary	Availability/reference for variable-level metadata and linkage capability/limitations.
Quality and utility	Available quality/utility labels, update frequency, and known limitations.
Conformance	Declared profile/version and native versus transformed conformance for FHIR, OMOP, DICOM, CDISC, or another model.

 Copyright © 2026: IHE International, Inc.

8.12 OMOP Analytical Representation Content Binding

8.12.1 Status and Principles

OMOP CDM is an optional external analytical representation. SU-DSX does not prescribe a universal OMOP CDM version, vocabulary release, ETL implementation, database technology, or analytical tool. OMOP transformation does not substitute for authorization, minimization, de-identification, destination control, or release review.

Table 8.12.1-1: Required OMOP manifest metadata

Metadata item	Requirement
OMOP CDM version	Exact CDM version of the provided or executed environment.
Vocabulary release	Target vocabulary release/date and relevant source-vocabulary versions; local modifications identified.
Included domains/tables	Included, excluded, or empty domains relevant to the authorized scope.
Source-to-concept mappings	Mapping package/version, provenance, and material unmapped/deprecated concept handling.
ETL/transformation	Executable/package/version, processing location, and material temporal/unit transformation rules.
Provenance	Source datasets/versions, transformation times, responsible system, and linkage to request/decision.
Validation	Structural, vocabulary, data-quality, and fitness-for-use validation performed.
Cohort/concept definitions	Cohort definitions, concept sets, descendant rules, observation periods, and temporal logic.
Native-object linkage	Permit-bound linkage to native FHIR/DICOM/pathology objects when multimodal analysis is authorized.

8.12.2 Multimodal and Federated Realizations

OMOP MAY represent structured clinical and observational data while imaging, pathology, genomics, biosignals, or other objects remain in authorized native representations. Cross-modal linkage SHALL use only permit-bound pseudonyms or controlled references. Federated OMOP execution SHALL preserve node compatibility, analytical package/version, vocabulary/CDM compatibility, execution attestation, and node-level disclosure decisions.

8.13 Clinical, Imaging, and Multimodal Payload Bindings

The bindings in this section are informative payload realizations. Their own implementation guides remain authoritative. SU-DSX adds only the governance, manifest, correlation, de-identification-evidence, integrity, and release constraints defined in this volume.

 Copyright © 2026: IHE International, Inc.

Table 8.13-1: Candidate payload bindings

Payload / interaction	Candidate binding	SU-DSX content requirement
Structured clinical data	FHIR REST / FHIR Bulk Data	Manifest SHALL identify resource types, profile versions, cohort, file inventory, hashes, extraction parameters, and source-local transformation where applicable.
IPS / IPS+ research content	FHIR document/Composition, Bulk FHIR, PCC-1, or document exchange	Manifest SHALL identify document/profile version, linkage scope, included sections/resources, and limitations.
Radiology / digital pathology	DICOM / DICOMweb	See Section 8.13.1. The manifest SHALL identify the authorized Study/Series/SOP Instance scope or equivalent inventory, object integrity, applicable de-identification evidence, permitted referential linkage, and authorized delivery context. SU-DSX does not profile the internal content of DICOM IODs.
Documents	MHD, XDR, XDS, XCA, DocumentReference/Binary	Manifest SHALL identify document identifiers, existing format codes, hashes, provenance, and signatures where applicable.
Large multimodal package	Secure file transfer, object store, protected repository	Immutable manifest, short-lived credentials, integrity, and cross-modal referential integrity.
Remote/federated execution	Controlled endpoint or distributed analytical package	Manifest SHALL identify endpoint, package/version/hash, input scope, execution evidence, disclosure controls, and returned result only.

8.13.1 DICOM and DICOMweb Payload Content Binding

DICOM and DICOMweb are external payload bindings for radiology, digital pathology, and other DICOM-based content. SU-DSX does not define a new DICOM IOD, SOP Class, Transfer Syntax, or attribute-level profile. The applicable DICOM standard remains authoritative for object content. SU-DSX constrains only the governance, manifest, provenance, de-identification evidence, integrity, referential-linkage, and authorized delivery context that accompany DICOM payloads.

An implementation using DICOM/DICOMweb for SU-4 or SU-5 SHALL satisfy the requirements below in addition to the applicable DICOM and DICOMweb specifications and the authorization, security, transport, and audit requirements defined in Volume 2.

 Copyright © 2026: IHE International, Inc.

Table 8.13.1-1: DICOM/DICOMweb payload-binding requirements

Requirement	SU-DSX constraint
Scope boundary	SU-DSX SHALL NOT redefine the internal clinical content of DICOM IODs. No new SU-DSX SOP Class, IOD, mandatory DICOM attribute, or Transfer Syntax is introduced by this binding.
Authorized object inventory	The manifest SHALL identify the authorized Study, Series, and SOP Instance scope, or an equivalent package inventory when individual identifiers are impractical. It SHALL identify package or endpoint identity and SHOULD include object counts.
SOP Class and modality	The manifest SHOULD identify relevant SOP Class UIDs and modalities when they are needed to interpret, validate, or reproduce the authorized dataset.
De-identification evidence	Where de-identification is required, receiver-safe evidence SHALL identify the applicable DICOM confidentiality profile/options or external de-identification policy, the processing stage, responsible service, time, and outcome. Re-identification keys or reversible mappings SHALL NOT be exposed.
Private attributes	The handling of private attributes or private blocks SHOULD be declared, including whether they were removed, retained under explicit authorization, or transformed.
Burned-in and rendered identifiers	Assessment and treatment of burned-in identifiers, overlays, annotations, presentation content, or other rendered identifying information SHOULD be recorded where applicable.
Digital pathology visual content	For whole-slide imaging and related pathology objects, treatment of label images, overview or macro images, annotations, and other potentially identifying visual or metadata content SHOULD be documented.
UID transformation and referential integrity	Where DICOM UIDs are remapped, the manifest SHOULD identify that remapping occurred and whether authorized cross-object and cross-modal referential integrity was preserved.
Derived objects	Segmentation objects, structured reports, measurements, annotations, parametric maps, presentation states, and other derived objects SHOULD preserve authorized references to source objects. Loss of such relationships SHOULD be declared in the manifest.
Pixel or object transformation	Lossless/lossy compression, cropping, masking, redaction, down-sampling, frame removal, or other transformations that may affect scientific utility or validation SHOULD be declared when applied.
DICOMweb delivery reference	When DICOMweb is used, the SU-DSX control content MAY reference the authorized service endpoint and permitted Study/Series/Instance retrieval scope instead of embedding DICOM objects. Reusable credentials SHALL NOT be placed in the manifest or general FHIR control message.

 Copyright © 2026: IHE International, Inc.

Requirement	SU-DSX constraint
Integrity and quality limitations	The manifest SHALL provide appropriate integrity evidence for the package or controlled repository and SHOULD record missing series/instances, unsupported objects, quality limitations, or transformations that may affect fitness for the approved secondary-use purpose.

These constraints are intentionally located in Section 8 rather than Section 7. Section 7 would become appropriate only if a future SU-DSX revision defines IHE-specific constraints on DICOM IODs, modules, attributes, or SOP Classes beyond the requirements of the DICOM standard itself.

8.13.2 IPS / IPS+ Research Content Binding

8.13.2.1 Status and Scope

IPS and IPS+ are external clinical-content bindings that MAY be used in SU-DSX when selected clinical information originally collected for care is reused for an authorized secondary-use purpose. SU-DSX does not define, reproduce, or fork the IPS or IPS+ content specification. The implementation guide, profile, canonical identifier, and version declared by the Information Source SHALL remain authoritative for the clinical content.

Neither IPS nor IPS+ represents the complete EHR or every data category that may be required for secondary use. Additional registry, pathology, mortality, imaging, genomic, administrative, or other authorized data MAY therefore accompany IPS/IPS+ content using another SU-DSX payload binding. Use of IPS or IPS+ SHALL NOT replace the SU-DSX request, access-decision, minimization, de-identification, source-provision, manifest, secure-processing, results-release, or audit requirements.

8.13.2.2 Relationship to the SU-DSX Lifecycle

Table 8.13.2-1: IPS / IPS+ relationship to SU-DSX transactions

SU-DSX transaction	IPS / IPS+ content requirement
SU-1 Query Catalogue	A Catalogue Service MAY advertise that a dataset, repository, or data service supports IPS or IPS+ and SHOULD identify the applicable profile or implementation-guide version when available.
SU-2 Submit Secondary Use Request	SURQ SHOULD identify the required clinical-content scope, cohort, time period, and relevant IPS/IPS+ sections or resource classes. Requested content SHALL remain limited to the minimum necessary for the approved purpose.
SU-3 Issue Permit / Access Decision	SUAD SHALL constrain the authorized clinical-content scope, cohort, period, source, linkage, permitted transformations, destination, and applicable IPS/IPS+ profile requirements where these form part of the approved data specification.

 Copyright © 2026: IHE International, Inc.

SU-DSX transaction	IPS / IPS+ content requirement
SU-4 Authorized Source Data Provision	The Information Source SHALL provide only permit-authorized IPS/IPS+ content and SHALL create a SUPM manifest identifying the actual profile/version, included content, linkage scope, provenance, transformations, integrity, and limitations.
SU-5 Prepared Data Delivery	Where the protected/SPE path is used, the IPS/IPS+ package or resources SHALL be correlated with the effective decision, SUPM manifest, delivery identifier, destination, and applicable de-identification evidence.
SU-6 Secure Processing and Results Release	Processing jobs using IPS/IPS+ content SHALL reference the applicable delivered dataset/package and version. Only outputs approved under SURL may leave the controlled environment.
SU-A1 Audit Event Logging	Audit correlation SHOULD preserve the request, decision, Information Source, IPS/IPS+ profile/version, manifest, preparation/de-identification actions, processing job, and released output identifiers as applicable.

8.13.2.3 IPS / IPS+ Manifest Requirements

Table 8.13.2-2: IPS / IPS+ manifest requirements

Manifest element	SU-DSX requirement
Profile identity and version	SHALL identify the IPS/IPS+ implementation guide, profile, canonical identifier, and version used by the provisioned content.
Content realization	SHALL identify whether the provision is represented as a FHIR document/Composition, a FHIR resource package, Bulk FHIR output, PCC-1 content, or another approved exchange realization.
Content inventory	SHALL identify included clinical sections, FHIR resource types, documents, logical packages, or equivalent content classes.
Cohort and population scope	SHALL identify the permit-bound cohort or population scope without exposing unnecessary or prohibited cohort details.
Subject and research linkage scope	SHALL identify the permitted subject, study, encounter, longitudinal, or research-context linkage required for the approved purpose.
Clinical time scope	SHALL identify the relevant observation or encounter period when needed to interpret the dataset.
Terminology and profile conformance	SHOULD identify material coding systems, terminology versions, conformance profiles, and validation results needed to interpret the clinical content.
Provenance	SHALL identify the Information Source, source dataset/version, extraction or assembly time, responsible system, and lineage to the applicable request and decision.

 Copyright © 2026: IHE International, Inc.

Manifest element	SU-DSX requirement
Minimization and transformation	SHALL identify relevant selection, exclusion, transformation, terminology mapping, pseudonymization, or other permit-authorized preparation.
Integrity	SHALL identify hashes, checksums, signatures, or equivalent integrity information appropriate to the selected package or transfer mechanism.
Known omissions and limitations	SHALL identify unavailable, intentionally omitted, unsupported, or incomplete sections/resources and other limitations material to fitness for use.
Additional non-IPS content	SHALL separately identify registry, pathology, imaging, mortality, genomic, administrative, or other accompanying data that are not part of the declared IPS/IPS+ profile.
Destination and authorization correlation	SHALL identify or reference the decision/version, fulfillment identifier, authorized destination, and delivery identifier where applicable.

8.13.2.4 Bulk FHIR Realization of IPS / IPS+ Content

IPS/IPS+ describes clinical-content semantics and does not require one physical transport mechanism. For population-level or large-cohort secondary-use workflows, an Information Source MAY use FHIR Bulk Data to provide permit-authorized FHIR resources that conform to the applicable IPS/IPS+ content constraints.

- The request and decision SHALL define the permitted population and clinical-content scope.
- The Information Source SHALL export only the authorized resource types and records.
- The SUPM manifest SHALL identify the applicable IPS/IPS+ profile/version and the relationship between the exported resources and the declared clinical-content model.
- The manifest SHALL identify Bulk FHIR files, resource types, counts, hashes, extraction parameters, provenance, and errors or omissions.
- Access URLs or credentials SHALL be destination-bound and appropriately time-limited.
- Use of Bulk FHIR SHALL NOT relax the IPS/IPS+ content constraints, permit scope, minimization requirements, or SU-DSX release-control requirements.

8.13.2.5 Relationship to Epidemiology-Specific and Multimodal Data

IPS/IPS+ SHALL be used only for clinical information represented by the declared IPS/IPS+ profiles. The epidemiology realization MAY additionally require registry variables, mortality information, pathology content, imaging, or other research-specific information. Such data SHALL be separately identified in the request, decision, and manifest and SHALL use the appropriate SU-DSX payload binding.

 Copyright © 2026: IHE International, Inc.

Where multiple representations are combined, the manifest SHALL preserve sufficient permit-bound linkage information to correlate IPS/IPS+ clinical content with the additional authorized data without exposing unauthorized identifiers.

8.13.2.6 Relationship to OMOP Analytical Representation

IPS/IPS+ and OMOP serve different purposes within SU-DSX. IPS/IPS+ MAY provide a harmonized clinical source-content representation, while OMOP MAY provide a harmonized analytical representation inside the authorized processing environment. Where IPS/IPS+ content is transformed into OMOP CDM, the source profile/version, OMOP CDM and vocabulary versions, ETL/source-to-model transformation, provenance, material mapping limitations, and permit-bound linkage to native data SHALL remain identifiable.

8.13.2.7 Conformance Statement

- An implementation claiming an IPS / IPS+ Research Content Binding SHALL identify the external IPS/IPS+ profile and version that it claims.
- The clinical content SHALL conform to that declared external specification.
- The implementation SHALL satisfy the applicable SU-DSX request, decision, manifest, provenance, minimization, delivery, processing, release, and audit requirements.
- The implementation SHALL distinguish IPS/IPS+ content from additional non-IPS research data.
- The applicable request, decision, fulfillment, dataset, and profile/version correlation SHALL be preserved throughout the secondary-use lifecycle.
- IPS/IPS+ conformance alone SHALL NOT be interpreted as authorization for secondary use.

8.13.3 Federated Aggregate Query and Statistical Data Content Binding

8.13.3.1 Status and Scope

This binding supports the lightweight federated aggregate/statistical path in which the approved purpose can be fulfilled without transferring person-level or pseudonymized source records to the DAC, DAA, SUA, or requester. Each participating Information Source executes the permit-bound computation locally and returns only an authorized aggregate or statistical result. An SPE is not required in the baseline path.

Candidate external realizations include profiled FHIR aggregate-query operations, QEDm-oriented aggregate-query capabilities, mADX-style aggregate reporting, FHIR Measure/MeasureReport, jurisdiction-specific statistical-query services, and source-local Bulk FHIR followed by local aggregation. SU-DSX provides the governance, authorization, query correlation, node evidence, disclosure-control, and approved-release framework around those realizations.

 Copyright © 2026: IHE International, Inc.

8.13.3.2 Federated Query Definition

Table 8.13.3-1: Federated aggregate query-definition requirements

Query element	SU-DSX requirement
Query identity and version	SHALL identify the permit-bound query and immutable query version.
Decision correlation	SHALL reference the effective decision/version and authorized statistical-data purpose.
Cohort/population definition	SHALL define the minimum population criteria needed for local execution.
Measure/calculation definition	SHALL identify numerator, denominator, calculation rules, measure definition, or equivalent analytical logic.
Timeframe	SHALL identify the approved observation/reporting period.
Stratification	SHALL identify approved grouping dimensions such as age band, sex, geography, provider, or other permitted strata.
Terminology and concept sets	SHOULD identify coding systems, concept-set versions, value sets, or OMOP concept definitions needed for consistent node execution.
Participating nodes	SHALL identify the Information Sources or federated nodes authorized to execute the query.
Expected output structure	SHALL identify the expected aggregate/statistical result schema, units, confidence/quality fields where applicable, and required provenance.
Disclosure constraints	SHALL identify applicable small-cell, rare-category, suppression, generalization, threshold, or other output-control requirements.

8.13.3.3 Node Execution and Result Evidence

Table 8.13.3-2: Node result and compatibility evidence

Evidence item	Required meaning
Node identity	Information Source/federated-node identifier and execution endpoint or environment.
Query/package version	Exact query, Measure, analytical package, container, or script version/hash executed at the node.
Local representation	FHIR, local Bulk FHIR, OMOP, relational/statistical store, or other authorized local representation used for execution.
Terminology/model compatibility	Relevant FHIR profile, OMOP CDM/vocabulary, concept-set, or coding-system versions needed to interpret compatibility.
Execution time and status	Execution timestamp, completion status, timeout, rejection, or partial-result status.

 Copyright © 2026: IHE International, Inc.

Evidence item	Required meaning
Aggregate result	Only the authorized aggregate/statistical result; person-level or pseudonymized source records SHALL NOT be included.
Node disclosure decision	Applicable local thresholding, suppression, generalization, rejection, or disclosure-control outcome.
Quality/fitness information	Known missing periods, incomplete sources, coding/mapping limitations, or other constraints affecting interpretation.
Provenance	Node, input dataset/version, analytical definition, and generated result lineage.

8.13.3.4 Combination and Final Release

- The DAC or authorized aggregation function SHALL verify that returned node results correspond to the approved query and compatible analytical definition before combination.
- Incompatible, stale, rejected, or disclosure-failed node results SHALL NOT be silently combined.
- The combined output SHALL preserve participating-node, query-version, analytical-version, and node-disclosure evidence.
- Where the result is non-identifying by design and satisfies the release conditions, it may proceed directly to SU-6 without SU-5 or an SPE.
- Where residual disclosure risk remains, the authorized statistical disclosure-control or release-control function shall apply the required suppression, generalization, thresholding, rare-category handling, validation, or rejection before SU-6 release. This post-query treatment is not modeled as a DIS job.
- The final result shall be represented through SUAR/SURL as applicable and correlated to the request, decision, query, participating nodes, disclosure decisions, and audit trail.

8.13.3.5 Conformance Statement

A conformant lightweight Federated Aggregate Query and Statistical Data Content Binding SHALL NOT transfer person-level or pseudonymized source records outside the participating Information Source when the approved workflow is the aggregate/statistical path. Use of source-local Bulk FHIR is permitted only as a local execution mechanism; record-level Bulk FHIR files SHALL NOT be returned to the DAC, DAA, SUA, or requester in this path.

8.13.4 Multimodal AI/ML Content Binding

8.13.4.1 Status and Scope

This binding supports multimodal AI/ML method development and validation requiring access to protected person-level or pseudonymized data inside an SPE or other permit-authorized controlled environment. It composes the SU-DSX DICOM/DICOMweb, FHIR/Bulk FHIR,

 Copyright © 2026: IHE International, Inc.

optional IPS/IPS+, optional OMOP, manifest, prepared-data delivery, processing-job, results-release, and audit content modules rather than defining a new AI data format.

Multimodal content SHALL remain in the representation appropriate to each modality. SU-DSX does not require DICOM, pathology, genomic, laboratory, waveform, annotation, or other native content to be converted to FHIR solely for participation in the SU-DSX workflow.

8.13.4.2 Multimodal Manifest and Linkage Requirements

Table 8.13.4-1: Multimodal AI/ML manifest requirements

Manifest element	SU-DSX requirement
Modality/content type	SHALL identify each structured, imaging, pathology, laboratory, genomic, annotation, outcome, or other modality included.
Native content binding	SHALL identify the applicable representation and profile/version, such as FHIR/Bulk FHIR, IPS/IPS+, DICOM/DICOMweb, OMOP, secure file/object package, or another authorized binding.
Source dataset/version	SHALL identify the source dataset, registry, repository, or package version for each modality.
Cohort and longitudinal scope	SHALL identify the permit-bound cohort, follow-up period, and longitudinal scope.
Cross-modal linkage	SHALL identify the permitted pseudonymous or controlled-reference linkage scheme and SHALL NOT expose unauthorized direct identifiers or re-identification material.
Training/validation partition	SHOULD identify training, validation, test, hold-out, or external-validation partitions where material to reproducibility or bias assessment.
Annotation/ground-truth provenance	SHOULD identify annotation source, version, reviewer/process provenance, and material quality limitations.
Preprocessing/transformation	SHALL identify material normalization, resampling, cropping, redaction, feature extraction, terminology mapping, ETL, or other preprocessing affecting scientific interpretation.
DICOM evidence	Where DICOM is used, SHALL satisfy Section 8.13.1 and preserve the authorized object/linkage scope.
OMOP evidence	Where OMOP is used, SHALL satisfy Section 8.12 and record CDM/vocabulary/ETL/provenance metadata.
Integrity	SHALL identify artifact/package hashes, checksums, signatures, or equivalent integrity evidence.
Known limitations	SHALL identify unavailable modalities, missing time periods, incomplete labels, mapping limitations, image-quality limitations, or other material constraints.

 Copyright © 2026: IHE International, Inc.

8.13.4.3 Processing-Job Requirements

Table 8.13.4-2: AI/ML processing-job requirements

Element group	Required meaning
Processing-job identity	SUPJ processing-job-id and immutable workflow version.
Authorization context	Effective decision/version, approved purpose, permitted team, workspace, validity period, and processing class.
Input dataset versions	Exact FHIR, DICOM, OMOP, annotation, registry, or other manifest/package versions used.
Software/toolchain	Framework, software/package, container/image, dependency set, and version/digest needed for reproducibility.
Model configuration	Model architecture/version, initialization or pretrained-model identifier where relevant, hyperparameters, and material preprocessing configuration.
Training/validation plan	Training, validation, bias/fairness, calibration, robustness, or other evaluation steps authorized by the decision.
Execution evidence	Start/end time, hardware/environment, logs, random seed or reproducibility metadata where applicable, and execution outcome.
Output candidates	Exact model weights, embeddings, metrics, reports, visualizations, synthetic outputs, or other candidate artifacts with identifiers/hashes.

8.13.4.4 Output Review and Release

- Completion of model training or validation does not itself authorize export from the controlled environment.
- Each model artifact, embedding, synthetic output, detailed subgroup metric, visualization, or other output candidate enters the SURL release workflow when external release is requested.
- Where additional transformation or disclosure control is required, the approved transformation is applied within the SU-6 release-control process, not as a second DIS job, and the resulting artifact receives its own identifier/version/hash.

8.13.4.5 Conformance Statement

An implementation claiming the Multimodal AI/ML Content Binding SHALL preserve the relationship among the request, decision, multimodal source manifests, de-identification evidence, SPE delivery, processing-job inputs, software/tool versions, output-candidate hashes, review evidence, release decision, and audit records. Native modality content SHALL remain governed by its authoritative external specification.

 Copyright © 2026: IHE International, Inc.

8.13.5 Use Case to Content-Binding Mapping

This subsection is informative. It provides traceability from the three Volume 1 use cases to the reusable content modules and bindings defined in this Volume 3. It does not restate the Volume 1 use-case narratives or process flows.

Table 8.13.5-1: Use case to Volume 3 content mapping

Volume 1 use case	Fulfillment path	Principal Volume 3 modules/bindings	Distinctive content evidence
Use Case 1 – Cross-border Epidemiology	Protected/SPE path	SUC, SURQ, SUAD, SUPM, SUDL, SUPJ, SURL, SUAC; IPS/IPS+ Research Content Binding; FHIR/Bulk FHIR; optional OMOP; DICOM or other native content where authorized.	Permit-bound longitudinal/pseudonymous clinical and registry content; IPS/IPS+ profile/version; cohort/linkage scope; source manifest; optional source-to-OMOP transformation; SPE processing; approved aggregate/research-output release.
Use Case 2 – Federated Aggregate Query and Statistical Data Request	Lightweight aggregate/statistical path	SUC, SURQ, SUAD, SUPM, SUAR, SURL, SUAC; Federated Aggregate Query and Statistical Data Content Binding; Measure/MeasureReport, QEDm/mADX, local Bulk FHIR, or optional local OMOP realization.	Common query definition; node identity; local execution version; aggregate result only; node compatibility; disclosure decision; final combination and release. SU-5/SPE normally not used.
Use Case 3 – Multimodal AI/ML Method Development and Validation	Protected/SPE path	SUC, SURQ, SUAD, SUPM, SUDL, SUPJ, SURL, SUAC; Multimodal AI/ML Content Binding; DICOM/DICOMweb; FHIR/Bulk FHIR; optional IPS/IPS+ and OMOP.	Multimodal manifest; cross-modal pseudonymous linkage; DICOM de-identification evidence; preprocessing provenance; reproducible training/validation job; exact model/output hashes; privacy/leakage review; controlled artifact release.

The protected SPE path is used where the approved purpose requires processing of person-level or pseudonymized data. The lightweight aggregate/statistical path is used where the approved purpose can be fulfilled by locally generated non-identifying results without transferring person-level data. Federated execution does not by itself determine which path is used; federated protected processing may still involve SPE-controlled nodes.

8.14 Receiver-Safe Evidence, Security Labels, and Minimization

Evidence delivered to an SUA, SPE, recipient, or downstream system SHALL be sufficient to validate the authorized content and lifecycle status without exposing privileged policy material, pseudonym mappings, re-identification keys, or attack-sensitive privacy parameters.

 Copyright © 2026: IHE International, Inc.

- Receiver-safe evidence SHOULD identify the effective decision, package/artifact, applied transformation class, validation outcome, responsible service, time, destination, and release status.
- Detailed rules, thresholds, pseudonymization secrets, key material, and attack-sensitive risk-assessment internals MAY remain in protected governance or audit stores.
- FHIR security labels MAY represent confidentiality, purpose, sensitivity, handling, or compartment constraints, but SHALL NOT broaden authorization beyond the effective decision.
- At each lifecycle stage, the content SHALL remain limited to the minimum data and metadata necessary for the approved purpose and recipient role.

8.15 Machine-Readable Conformance Artifacts and Validation

Table 8.15-1: Artifacts required before Trial Implementation

Artifact type	Provisional logical ID	Purpose
StructureDefinition	su-dsx-message-bundle	Common SUC Bundle
StructureDefinition	su-dsx-message-header	SU-DSX MessageHeader
StructureDefinition	su-dsx-workflow-task	Common lifecycle Task
StructureDefinition	su-dsx-secondary-use-request	SURQ request content
StructureDefinition	su-dsx-access-decision	SUAD Contract/decision content
StructureDefinition	su-dsx-manifest-documentreference	Manifest DocumentReference
StructureDefinition	su-dsx-manifest-list	Manifest inventory List
StructureDefinition	su-dsx-processing-job	SUPJ processing Task
StructureDefinition	su-dsx-release-request	SURL release request
StructureDefinition	su-dsx-release-decision	SURL release decision
StructureDefinition	su-dsx-aggregate-result	SUAR aggregate result
CodeSystem / ValueSet	su-dsx-*	Codes and value sets defined in Section 5

8.15.1 Validation Requirements

- A conformant sender SHALL validate each message against the applicable SU-DSX content profile and required external content binding before transmission.
- A conformant receiver SHALL perform structural, terminology, reference, authorization-context, version, recipient-binding, and lifecycle validation appropriate to its actor responsibilities.

 Copyright © 2026: IHE International, Inc.

- Validation failure SHALL produce a safe OperationOutcome or applicable audit/transport error and SHALL NOT disclose protected cohort, policy, or security detail.
- A structurally valid message SHALL NOT override an expired, revoked, suspended, replaced, or otherwise ineffective authorization.
- Payload validation SHALL include the applicable FHIR, DICOM, document, file-package, OMOP, federated, manifest, integrity, and destination checks.

8.16 Examples and Test Requirements

1. Cross-border epidemiological request using catalogue discovery, SURQ request, SUAD decision, Bulk FHIR provision, optional DIS preparation, SPE delivery, controlled processing, and disclosure-controlled release.
2. Multimodal AI/ML request using FHIR clinical data plus DICOM/DICOMweb imaging, permit-bound pseudonymous linkage, controlled model execution, privacy/leakage review, and vetted model-artifact release.
3. Federated aggregate/statistical request using a common Measure or OMOP analytical package at multiple nodes, compatibility checks, node-level evidence/disclosure decisions, combination, and direct non-identifying release.
4. Negative tests for stale or revoked decision, mismatched recipient, out-of-scope variable, corrupted package, unsupported profile, missing manifest, inactive workspace, disclosure-risk rejection, and replayed message.

 Copyright © 2026: IHE International, Inc.

Appendices to Volume 3

 Copyright © 2026: IHE International, Inc.

Appendix A – Actor and Content Module Responsibilities

This appendix is normative for the content responsibilities shown. Transaction behavior remains in Volume 2.

Table A-1: Actor/content responsibilities

Actor	Content role	Opt.	Responsibility
Catalogue Service (CAT)	DCAT / HealthDCAT-AP Provider	O	Produce catalogue responses conforming to the advertised application profile/version.
Secondary Use Agent (SUA)	SURQ Creator / SUAD Consumer / SURL Consumer	R	Create/version requests, receive decisions, submit permitted processing where applicable, and receive only approved outputs.
Data Access Authority (DAA)	SURQ Consumer / SUAD Creator	R	Validate/preserve requests and create/version authoritative access decisions.
Data Access Coordinator (DAC)	SUAD Consumer / SUPM Creator-Consumer / SURL Coordinator	R	Operationalize effective decisions, coordinate source fulfillment, and coordinate controlled release.
Information Source (IS)	SUPM Consumer-Creator	R	Perform permit-authorized source fulfillment and create source status/manifest/evidence.
De-ID Manager / De-Identifier	DIS content roles	C	Use the DIS profile when policy-governed input preparation or de-identification is required before authorized processing; SU-DSX references rather than duplicates DIS artifacts.
Secure Processing Environment (SPE)	SUDL Consumer-Creator / SUPJ Consumer / SURL Participant	C	Validate prepared-data delivery, enforce controlled processing, and produce output candidates subject to release control.
All SU-DSX actors	SUAC Audit Source	R	Emit minimized but correlatable audit evidence for applicable lifecycle actions.

 Copyright © 2026: IHE International, Inc.

Appendix B – Cross-Transaction Content Mapping

2705 **Table B-1: Lifecycle content mapping**

Lifecycle object	Created / asserted in	Referenced by
Catalogue record	SU-1 external binding	SURQ requested-data references and later manifests.
Request	SURQ / SU-2	SUAD, SUPM, SUDL, SUPJ, SURL, SUAC.
Decision / permit	SUAD / SU-3	Every authorized action under SU-3 through SU-6.
Fulfillment	SUPM / SU-4	Provision phases, manifest, delivery, processing, audit.
Manifest / package	SUPM or SUDL	SPE ingest, processing job, release evidence, audit.
DIS job / policy / task	DIS profile	SUPM/SUDL receiver-safe evidence and SUAC audit where DIS is used. SURL may reference DIS identifiers only as provenance of input preparation; DIS artifacts do not constitute the post-analysis release decision.
Processing job	SUPJ / SU-6	Status, output candidate, release request, audit.
Release request / release decision	SURL / SU-6	Approved artifact delivery, recipient receipt, audit, finalization.

 Copyright © 2026: IHE International, Inc.

Appendix C – Informative EHDS / TEHDAS2-Oriented Mapping

This appendix is informative. SU-DSX remains internationally applicable. EHDS/TEHDAS2 terminology illustrates one deployment model and does not change the normative IHE actor or content model.

Table C-1: Informative EHDS-oriented interpretation

SU-DSX content	Illustrative EHDS-oriented interpretation
SURQ request	Data access application or anonymized statistical data request submitted to an HDAB/DAAMS.
SUAD decision	Data permit, denial, amendment, suspension, revocation, or related HDAB decision; may also carry applicable opt-out, fee, appeal, and cross-border conditions.
SUPM source fulfillment	Health data holder consultation, preparation, minimization/de-identification evidence, data-quality evidence, manifest, and correction/completion.
SUDL delivery	Prepared-data ingest into an HDAB-operated or delegated SPE with workspace, quarantine, retention, and deletion controls.
SUPJ processing	Permit-bound analysis in an SPE or controlled federated node.
SURL release	HDAB-controlled output review, disclosure-control evidence, approved release, publication/report-back, significant-finding routing where applicable, and closure.
HealthDCAT-AP binding	National/European health dataset catalogue content.
OMOP binding	Optional harmonized analytical representation for centralized or federated analysis.

 Copyright © 2026: IHE International, Inc.

Volume 3 Namespace Additions

Add the following terms to the IHE Namespace:

No final OIDs, UIDs, URNs, canonical URLs, FHIR package identifiers, MessageHeader event codes, CodeSystem URLs, ValueSet URLs, or SU-DSX-specific audit codes are assigned in this Public Comment working draft. Before Trial Implementation, IHE namespace allocation is required for:

- the SU-DSX canonical package root;
- FHIR StructureDefinition canonical URLs listed in Section 8.15;
- FHIR extensions required only where standard FHIR elements are insufficient;
- SU-DSX MessageHeader event codes;
- SU-DSX CodeSystem and ValueSet canonical identifiers from Section 5;
- SU-DSX-specific audit event/category codes where required;
- any new URNs used to identify SU-DSX content bindings or implementation-guide packages.

The placeholder [SU-DSX-CANONICAL-ROOT] SHALL be replaced before Trial Implementation. External identifiers owned by HL7, DICOM, W3C, OHDSI, HealthDCAT-AP, and other IHE profiles SHALL retain their authoritative namespaces. Provisional DIS transaction identifiers ITI-x1 through ITI-x6 SHALL be replaced by the identifiers assigned by the final DIS profile.

 Copyright © 2026: IHE International, Inc.

Volume 4 – National Extensions

This Volume 4 section defines additional requirements for deployments of the Secondary Use Data Exchange (SU-DSX) Integration Profile in the European Health Data Space (EHDS). The extension adds requirements above the base SU-DSX profile; it does not relax or replace the international profile requirements.

 Copyright © 2026: IHE International, Inc.

4 National Extensions

This proposed European regional extension applies when an implementation claims conformance to SU-DSX for an EHDS-oriented national or cross-border HealthData@EU deployment. EHDS terminology is used in this section as a regional deployment constraint; the base SU-DSX profile remains globally applicable.

4.1 National/Regional Extensions for EHDS (IHE-Europe)

The base SU-DSX profile remains the source of normative actor, transaction, content, and security requirements. This Volume 4 extension only adds constraints, evidence, status values, deployment dependencies, and testing expectations that apply when an implementation claims conformance to the EHDS regional deployment. The extensions are based on the TEHDAS2 guidelines and recommendations, particularly for catalogue dependencies, Data Access Application Management System (DAAMS) application lifecycle, holder coordination, opt-out evidence, fees and appeals, SPE operation, anonymity evidence, significant findings, cross-border HealthData@EU routing, publication duties, and lifecycle closure.

Note: In TEHDAS2, DAAMS is the technical system used by a Health Data Access Body (HDAB) to manage the end-to-end lifecycle of applications and requests for secondary use of health data.

4.1.1 Comment Submission

This proposed extension has been prepared as part of the SU-DSX profile-development activity in the IHE Quality, Research and Public Health (QRPH) domain. The supplied assessment material does not establish a separate formal IHE Europe sponsor for this Volume 4 extension. Comments on the SU-DSX profile should therefore be directed through the QRPH profile-development channel: QRPH@ihe.net.

4.1.2 Secondary Use Data Exchange (SU-DSX)

The following disposition is normative for the extension: the existing profile actors and transactions are retained, while their EHDS-specific requirements are constrained by the subsequent sections.

SU-DSX component	EHDS extension disposition
Secondary Use Agent (SUA)	Add complete application content, user-conduct evidence, workspace prerequisites, and post-access/publication obligations.
Catalogue Service (CAT)	Add HealthDCAT-AP publication/harvesting dependency, metadata validation, and EHDS catalogue response requirements.
Data Access Authority (DAA)	Add DAAMS lifecycle, holder consultation, fees, appeals, opt-out, significant-finding, and multi-country decision semantics.
Data Access Coordinator (DAC)	Add feasibility/cost coordination, preparation confirmation, correction, receipt, and completion evidence.
Information Source (IS)	Add holder feasibility, data quality, opt-out, imaging, trusted-holder,

 Copyright © 2026: IHE International, Inc.

SU-DSX component	EHDS extension disposition
	intermediary, and completion evidence.
Secure Processing Environment (SPE)	Add workspace activation, onboarding, operational controls, federation, retention, and deletion evidence.
Audit Record Repository (ARR)	Extend audit categories for governance, fees, non-compliance, incidents, publication, and deletion.
De-ID Manager / DIS grouping	Retain conditionally. Use for policy-governed transformation and de-identification evidence when applicable.

Transaction	EHDS extension disposition
Query Catalogue [SU-1]	Declare catalogue publication/harvesting as a dependency and strengthen metadata response/validation.
Submit Secondary Use Request [SU-2]	Extend application content, DAAMS lifecycle states, public-summary, and fee semantics.
Issue Permit / Access Decision [SU-3]	Add holder-consultation, fees, appeals, opt-out, significant findings, and jurisdiction-specific decision components.
Authorized Source Data Provision [SU-4]	Add bidirectional preparation, feasibility/cost, confirmation, deviation, correction, receipt, and completion messages.
Transfer Prepared Data to SPE [SU-5]	Add workspace readiness/activation, quarantine, federation, retention, and deletion controls.
Secure Processing and Results Release [SU-6]	Strengthen anonymity/synthetic-data evidence, publication, significant findings, and closure.
Audit Event Logging [SU-A1]	Extend governance, fee, usage, non-compliance, incident, publication, and deletion events.

Common EHDS Identifiers and Evidence

Correlation identifiers: The following identifiers SHALL be carried or referenced when applicable so that records can be correlated across the full secondary-use lifecycle.

- application-case-id
- public-summary-id
- holder-consultation-id
- fee-estimate-id
- invoice-id
- appeal-id
- opt-out-evidence-id
- trusted-holder-recognition-id
- intermediary-assignment-id
- workspace-id
- incident-id

 Copyright © 2026: IHE International, Inc.

- significant-finding-id
- publication-notification-id
- deletion-evidence-id
- cross-border-common-context-id
- national-decision-component-id

Common evidence objects: The extension uses the following reusable evidence objects. Each object MAY be embedded or referenced, but the authoritative version SHALL remain resolvable for the permitted lifecycle.

Evidence object	Minimum content / purpose
Applicant qualification evidence	Applicant authority, responsible person, team roles, qualifications, processors/subcontractors, and required expertise.
Ethics / regulatory evidence	Ethics approval or exemption, regulatory authorization, DPIA status, study/device references, and applicable registration.
Data-management plan	Data handling, software, external data, linkage, retention/deletion, incident response, collaboration, and publication commitments.
Holder feasibility statement	Availability, effort, timing, quality limitations, linkage dependencies, transformations, capacity and constraints.
Cost statement	Tariff version, eligible components, estimate/final amount, invoicing/payment recipient, status and dispute reference.
Data-quality statement	Completeness, missing periods/sources, terminology versions, mapping limitations, latency, anomalies and fitness caveats.
Opt-out evidence	Rule version, eligibility source, verification timestamp, effective date, exclusion result, exception basis and enforcement result.
Preparation specification	Final cohort, variables, minimisation, linkage, format, destination, due date, acceptance, correction and cost confirmation.
Anonymity evidence package	Policy, transformation log, privacy risk, residual threshold, utility/fidelity, reviewer/decision, audience/context and output hash.
Synthetic-data evidence package	Generation method/version, source scope, privacy/memorisation testing, fidelity/utility, rare-record risk, limitations and release decision.
Workspace manifest	Workspace ID, users/roles, validity, tools, limits, network/collaboration policies, monitoring and activation state.
Output-review record	Artifact hash, release context, reviewer/decision, disclosure controls, classification and release restrictions.
Deletion certificate	Deletion trigger, scope, completion time, retained/legal-hold exceptions and responsible actor.

Common error categories: Transactions SHALL be able to represent the following conditions without exposing unnecessary sensitive content.

- fee/payment condition
- opt-out/eligibility failure
- holder feasibility failure
- cross-border jurisdiction mismatch

 Copyright © 2026: IHE International, Inc.

- workspace not activated
- user onboarding incomplete
- retention/deletion conflict
- significant-finding handling error
- intermediary authorization failure

4.1.2.1 Query Catalogue [SU-1]

SU-1 remains the SUA-to-CAT query transaction. Publication, update, withdrawal, validation, harvesting, and national-to-European catalogue synchronization are dependencies rather than new SU-DSX transactions.

- A Catalogue Service claiming this extension SHALL be populated and maintained through a HealthDCAT-AP-compatible publication or harvesting mechanism.
- Publication, update, withdrawal, metadata validation, harvesting, and synchronization MAY be implemented internally or through grouping with another applicable catalogue-publication mechanism.
- The deployment SHALL preserve stable dataset identifiers and version correlation across publication, update, withdrawal, harvesting, and query.
- A CAT claiming a named DCAT application profile SHALL validate published metadata against the applicable profile constraints.
- Where SHACL shapes or an equivalent validation mechanism are available, the CAT SHOULD expose the validation status or a reference to the validation report.
- For HealthDCAT-AP records, the query response SHALL identify the exact HealthDCAT-AP release and profile URI used by the record.

Minimum EHDS catalogue response: Where applicable, the SU-1 response SHALL include or reference:

- EHDS secondary-use dataset category
- data-holder identity distinct from catalogue publisher
- legal or governance basis for availability
- data-access-application versus anonymized statistical-data-request path
- availability of variable-level descriptions
- quality and utility labels
- update frequency
- last source update and last metadata update
- distinction between dataset, distribution and data service/access service

 Copyright © 2026: IHE International, Inc.

- territorial or jurisdictional limitations
- opt-out applicability
- expected preparation or transformation capability
- approximate volume
- linkage availability and limitations
- SPE or federated-analysis capability

4.1.2.2 Submit Secondary Use Request [SU-2]

Application content: The request SHALL support the information needed for a high-quality EHDS application, rather than only the technical extraction scope.

- applicant legal identity and authority to apply
- principal investigator or responsible person
- project team members and roles
- qualifications and relevant expertise
- subcontractors and processors
- conflicts of interest where required
- justification for why the purpose cannot reasonably be achieved with less data or anonymous data
- expected societal/public-health/scientific/regulatory benefit
- methodological justification, feasibility and proportionality
- dissemination and publication plan
- ethics approval or exemption where applicable
- regulatory authorization and study/device references where applicable
- Data Protection Impact Assessment (DPIA) status and applicable research registration
- data-management plan
- software/packages/containers and compute requirements
- external data to be imported and intended linkage datasets
- collaboration arrangements and incident-response contacts
- retention/deletion plan and expected workspace duration

User conduct: The request SHALL record the following acknowledgements or commitments:

- acceptable-use acknowledgement
- prohibition on re-identification

 Copyright © 2026: IHE International, Inc.

- prohibition on prohibited linkage or onward disclosure
- publication and acknowledgement obligations
- commitment to report incidents
- commitment to report possible significant findings through the authorized process

DAAMS lifecycle states: The common application state model SHALL support these states or semantically equivalent coded values:

draft, submitted, received, pre-screening, incomplete, additional-information-requested, applicant-response-received, under-assessment, holder-consultation, fee-estimate-pending, fee-acceptance-pending, decision-pending, approved, partially-approved, denied, appealed, amended, withdrawn, suspended, expired, revoked, closed.

Public-information component: SU-2 SHALL support an optional public-summary element suitable for transparency publication. It SHOULD include applicant organization, project title, plain-language purpose, requested data categories, public-interest justification, expected duration, and publishable decision status. The summary SHALL exclude confidential protocols, security-sensitive details, trade secrets, and personal contact information.

Fee semantics: Where fees apply, SU-2 acknowledgement/task semantics SHALL represent whether a fee applies, tariff version, estimate status, payment recipient, payment milestone, exemption/reduction, dispute route, and whether assessment may continue before payment.

4.1.2.3 Issue Permit / Access Decision [SU-3]

Holder consultation: The decision SHALL include or reference the authoritative holder-consultation record, including the following where applicable:

- holders consulted and consultation dates
- holder feasibility responses
- data-availability limitations
- preparation estimates
- linkage dependencies
- quality limitations
- unresolved objections
- intellectual-property or trade-secret conditions

Fees and payment: Administrative conditions SHALL represent:

- tariff and calculation version
- eligible cost components
- estimated and final amount
- invoicing entity and payment recipient

 Copyright © 2026: IHE International, Inc.

- payment deadline and whether payment is a prerequisite for activation
- refund rules
- dispute procedure
- consequences of non-payment

Appeals: The decision SHALL state whether appeal is available, appeal authority, deadline, submission route, suspensive effect, whether provisioning may begin during appeal, and finality status. The lifecycle SHALL support appeal-pending, confirmed-after-appeal, modified-after-appeal, and annulled-after-appeal, preferably as later decision versions.

Opt-out conditions: Where applicable, the decision SHALL identify whether opt-out applies, rule/policy version, relevant data categories, effective-date rule, authoritative eligibility source, lawful exceptions, re-check frequency for recurrent provision, and evidence required from the IS.

Significant findings: When enabled by the permit, the decision SHALL identify the applicable significant-finding threshold/classification rule, responsible authority, validation/escalation route, controlled-contact mechanism, prohibition on direct re-identification by the data user, and reporting time limits.

Multi-country decisions: A cross-border workflow MAY use one common decision context and one jurisdiction-specific decision component for each participating country/authority. Each component SHALL identify local datasets, holder obligations, opt-out rules, fees, SPE requirements, and output restrictions. Fulfilment SHALL NOT begin for a source unless the applicable national component is valid and consistent with the common context.

4.1.2.4 Authorized Source Data Provision [SU-4]

SU-4 remains technology-neutral and SHALL support the full bidirectional holder-coordination dialogue needed for preparation and completion. The following business message phases are added within SU-4 without creating a new transaction identifier:

SU-4 message phase	EHDS extension requirement
Preparation Request	DAC requests source preparation and identifies the permit, source scope, destination, requested representation and due conditions.
Feasibility and Cost Response	IS reports availability, earliest delivery, effort, eligible cost, quality limitations, linkage dependencies, required transformations, IP/trade-secret concerns, volume/capacity limits and need for a trusted holder/intermediary.
Confirmed Preparation Specification	DAC confirms final cohort/variables, minimisation, linkage, opt-out responsibility, de-identification location, destination, format, due date, acceptance criteria, cost acceptance and correction rules.
Provision Status / Deviation Notice	Supports delayed, blocked, expired, corrected, superseded, awaiting-fee-confirmation and awaiting-destination-readiness, in addition to base status values.
Provision Result and Manifest	Carries final source-side result and manifest with provenance, permit/policy, data-quality, opt-out, payload and fulfilment evidence.
Change / Correction / Cancellation	Provides versioned amendment semantics for changed, corrected or cancelled preparation.

 Copyright © 2026: IHE International, Inc.

SU-4 message phase	EHDS extension requirement
Transfer Receipt / Completion Response	Destination or DAC acknowledges receipt/ingest/completion; source completion alone does not prove destination receipt.

Trusted health data holder: When trusted-holder status is used, SU-4 SHALL identify recognition authority, recognition identifier, validity period, simplified steps permitted, controls that remain mandatory, and revocation status. Trusted-holder status SHALL NOT remove permit verification, minimisation, destination validation, manifest, audit, or accountability.

Health-data intermediation: When a health-data intermediation entity participates, SU-4 SHALL identify the intermediary organization, delegated function, legal/contractual basis, data handled, processing location, responsible holder, responsible HDAB, and evidence/audit duties. The intermediary SHALL NOT displace holder or HDAB responsibilities.

Opt-out evidence: Where opt-out applies, the SU-4 manifest SHALL include or reference the opt-out rule version, matching/eligibility service, verification timestamp, effective date, exclusion count where disclosure-safe, exception basis where applicable, and enforcement result.

Data-quality statement: The manifest SHALL include or reference completeness limitations, missing periods/sources, coding-system versions, mapping limitations, temporal latency, extraction anomalies, fitness-for-purpose caveats, and holder attestation/validation outcome.

Imaging evidence: For imaging, the manifest SHALL include or reference private DICOM attribute handling, burned-in text assessment, UID transformation policy, pathology label/macro-image handling, annotation/segmentation linkage, lossless/lossy transformation declaration, image counts by study/series/object, and imaging-quality limitations.

Completion semantics: Source-side preparation or transfer completion SHALL NOT be interpreted as proof that the destination has received, ingested, or accepted the data. The fulfilment case SHALL remain open until the applicable receipt/ingest acknowledgement is correlated, unless an explicit deployment rule defines another closure condition.

4.1.2.5 Transfer Prepared Data to SPE [SU-5]

Workspace readiness: The SU-5 delivery notice or associated workspace manifest SHALL identify:

- workspace/project identifier
- approved users and roles
- workspace validity
- approved tools
- compute and storage limits
- network policy
- external-data import policy
- collaboration policy

 Copyright © 2026: IHE International, Inc.

- logging and monitoring requirements
- user training/onboarding status
- acceptable-use acknowledgement

Activation conditions: Successful ingest SHALL NOT by itself expose prepared data to a data user. Access SHALL begin only after workspace activation confirms authorized users, roles, tools, purpose, validity period, and applicable acceptable-use conditions.

Quarantine lifecycle: When quarantine occurs, the SPE SHALL record quarantine reason, authorized investigator, correction route, time limit, deletion/replacement action, whether partially accepted content may be used, and audit/incident escalation requirements.

Retention and deletion: SU-5 acknowledgement or associated lifecycle evidence SHALL identify retention start, scheduled deletion, deletion trigger, source-package cleanup status, workspace closure conditions, legal-hold status, and required deletion evidence.

Federated SPE / remote endpoint: For federated or remote processing, SU-5 SHALL identify or reference node identity, attestation, software/container hash, local policy version, data-location constraint, prohibited export classes, node-level disclosure-control obligation, and node-completion evidence.

4.1.2.6 Secure Processing and Results Release [SU-6]

Job submission controls: Before job execution, SU-6 SHALL verify user training/onboarding, acceptable-use acknowledgement, authorized team membership, approved software, external package/dependency controls, network restrictions, collaboration permissions, incident status, and workspace expiry where applicable.

Anonymity and disclosure evidence: The Output Release Request SHALL include or reference, where applicable:

- de-identification/anonymisation policy version
- transformation log
- privacy-risk metric
- residual-risk threshold
- utility assessment
- fidelity assessment
- reviewer identity or automated-policy decision
- release context
- intended audience
- anonymity-context statement
- suppression/generalisation decisions

 Copyright © 2026: IHE International, Inc.

- exact output hash

Note: Anonymous status is assessed in the release context, including the intended recipient and available auxiliary information; it is not determined solely by the output artifact in isolation.

Synthetic data: For synthetic-data output, the evidence package SHALL include generation method/version, source dataset scope, privacy evaluation, memorisation or nearest-neighbour testing, fidelity/utility metrics, rare-record risk, intended-use limitations, a prohibition on representing the output as original data, and the release decision.

Publication and reporting: The release decision SHALL identify, where applicable, publication obligations, acknowledgement/citation requirements, reporting of publications and resulting assets, report-back deadline, permitted onward disclosure, intellectual-property conditions, and repository-deposit requirements.

Significant findings: When significant-finding handling is enabled, SU-6 SHALL support the classifications ordinary research output, possible significant finding, validated significant finding, rejected as significant finding, and urgent finding (or semantically equivalent coded values). A possible or validated finding SHALL NOT be released to the data user as a means of identifying or directly contacting the natural person; it SHALL be routed through the authorized HDAB-controlled validation/notification pathway.

Closure and deletion: The final SU-6 lifecycle state SHALL record job closure, outputs released/rejected, workspace deactivation, temporary-file deletion, retained artifacts, legal hold, removal of user access, and deletion evidence.

4.1.2.7 Audit Event Logging [SU-A1]

Additional event categories: In addition to base SU-A1 events, the extension SHALL support coded audit events for:

- application state change
- request for additional information
- holder consultation
- fee estimate issued
- fee accepted or disputed
- invoice issued
- payment received
- permit suspended or revoked
- opt-out evaluation
- trusted-holder procedure used
- intermediary action

 Copyright © 2026: IHE International, Inc.

- workspace activation/deactivation
- user onboarding/acceptable-use acknowledgement
- tool or data import
- security incident
- output review
- significant-finding routing
- publication notification
- retention/deletion
- non-compliance and corrective action

Fees and non-compliance evidence: SU-A1 SHALL be able to correlate audit records with tariff version, cost estimate, invoice, payment, exemption, refund, dispute, non-compliance finding, suspension/revocation, and penalty reference without itself calculating the legal fee or penalty.

Usage metering: Where deployment policy requires metering, audit or associated evidence SHOULD record storage use, compute use, transfer volume, preparation effort, review effort, workspace duration, and fee-relevant service category. Metering evidence SHALL be separated from sensitive clinical/research content.

4.1.2.8 HealthData@EU Cross-Border Routing and Orchestration

SU-DSX defines the business transaction semantics and payload references. In a HealthData@EU deployment, messages may be carried through National Contact Points (NCPs) and the common cross-border infrastructure. The SU-DSX transaction does not replace those routing, trust, messaging, acknowledgement, retry, validation, or conformance mechanisms.

- The deployment SHALL preserve a common request context and the applicable jurisdiction-specific decision components.
- Cross-border messages SHALL carry or reference sender and receiver nation identifiers, NCP identifiers, a message identifier, and a conversation/correlation identifier.
- The cross-border infrastructure SHALL provide acknowledgement plus routing/processing status and national validation outcome appropriate to the deployed common infrastructure.
- Retry and duplicate handling SHALL preserve idempotent correlation to the original SU-DSX business context.
- A national validation failure SHALL be visible to the responsible orchestration component and SHALL NOT silently advance the business lifecycle.
- Cross-border audit SHALL correlate the SU-DSX transaction, NCP/common-infrastructure message, national decision component, and end-to-end conformance evidence.

 Copyright © 2026: IHE International, Inc.

Note: NCP routing, AS4 or equivalent secure messaging, common message identifiers, acknowledgements, retries, national validation, and end-to-end conformance testing are infrastructure requirements around SU-DSX; they are not redefined as new SU-DSX transactions in this extension.

4.1.2.9 Security, Privacy, and Accountability

- Additional evidence introduced by this extension SHALL be protected according to its sensitivity and SHALL follow data-minimisation principles.
- Audit records SHALL correlate business events without unnecessarily copying clinical content, research content, or confidential application material.
- Opt-out evidence SHALL be versioned and time-bound when temporal applicability is relevant
- The SPE SHALL prevent data-user access before workspace activation and SHALL enforce the approved user, tool, network, collaboration, and validity constraints.
- Output release SHALL be bound to the exact output artifact/hash and SHALL consider release context, intended audience, privacy risk, utility, and applicable policy.
- A data user SHALL NOT use significant-finding handling as a route to re-identify or directly contact a natural person.
- Deletion and workspace closure SHALL produce auditable evidence, including any justified legal-hold or retained-artifact exception.
- Cross-border routing SHALL preserve message integrity, source/destination identity, correlation, duplicate/replay handling, national validation outcomes, and end-to-end auditability.

 Copyright © 2026: IHE International, Inc.