Unique Ballot ID:
PRIV_SEC_CLASS_SYS_R1_N1_2013SEP

Guide to the HL7 Healthcare Privacy and Security Classification System (HCS) Release 1

January 2014

HL7 Informative Guidance Release 2

Sponsored by:
Security Work Group
Co-chairs:

John "Mike" Davis, Bernd Blobel, John Moehrke, Trish Williams

Modeling and Vocabulary Facilitators:

John "Mike" Davis, Kathleen Connor, Duane Decouteau

Table of Contents

1.

Parking Lot

Mention ONC IGs

1. Overview

The Healthcare Privacy and Security Classification System Guide (HCSG) provides informative material intended to be of use for implementing the HL7 Health Care Privacy and Security Classification System (HCS). HSCG describes a Healthcare Privacy and Security Classification System (HCS) suitable for automated privacy and security labeling and segmentation of protected health information (PHI) for privacy policy enforcement through security access control services (ACS).

Within a security domain, these requirements are fulfilled by information classification system guidance issued by domain authorities. Security labels are key access control information (ACI) applied by policy within a security domain as attributes of security principal “Initiators” requesting access to information and system resources; the resource “Targets”[i] for which access is sought; the request and the context in which it is made; and the asserted policy rationale, e.g., purpose of use, for access.
Security labels should be standardized and computable where semantic interoperability is required for electronic cross-enterprise exchange and to enforce and document policy compliance.

2. Goal

The goal of this guide is to provide an informative supplement to the HL7 HCS. It contains amplifying information regarding the content of the HCS, which is intended to be of use to architects and developers of security labeling services required to implement a HCS.

3. Policy Considerations

Application of security and privacy labels may require careful policy consideration to account for the distinct possibility that providers may receive incomplete information. Achievement of the proper balance between clinical need and patient privacy is needed to ensure that patient safety is not compromised. Some points of consideration include:

- To address providers' concerns regarding incomplete information, it has been suggested that masked or redacted information should be flagged as such in order to increase provider trust in the contents (GWU). If flagging notice of redacted content is permitted under applicable policy, then security labels may convey that a clinical fact has been redacted by using codes such as the HL7 Security Observation vocabulary for Data Alteration,

- As an alternative, PHI can be masked such that only authorized recipients can decrypt it using keys based on their clearances. For ensuring patient safety while preserving privacy to the greatest extent possible:
- Unmasked PHI may be consumed by clinical decision support system such as a drug-drug interaction application, which would alert a non-authorized clinician of potential safety impact.
- Policies may permit overrides such as "Break the Glass" in order to access masked PHI under these conditions. The intent of such notifications is always to achieve a workable balance between patient privacy and patient safety.
- Patients may allow a provider to access masked PHI on an ad hoc basis, e.g., when the provider inquires about a "mask flag" or a drug-drug interaction alert, using a "shared secret" capability to retrieve the mask's decryption key.
- Masking offers options not available through redaction. Redacted information is not recoverable.

4. Assumptions

In developing the HL7 HCS, certain assumptions regarding the use and interrelationship of clinical and security tagging have been made:

- A segmenting EHR system is capable of:
- Disaggregating health information into clinical data elements, which are the most granular level of clinically relevant information,
- Retrieving *clinical* attributes about the patient, clinical information category, and provenance such as information source and encoding clinical vocabulary,
- Applying clinical attributes as metadata tags on clinical data elements to generate *clinical facts* in accordance with clinical rules.
- Clinical facts have no intrinsic security or privacy value. The sensitivity of a clinical fact is determined by matching clinical attributes with the criteria for governance under privacy policies, including patient consent directives. For example, if the provenance indicates that a clinical fact was generated in the course of treatment in a U.S. realm 42 CFR Part 2 facility, then the clinical fact is governed under 42 CFR Part 2,
- Security labels can convey the relative risk associated with disclosure of clinical information based upon standardized security and privacy vocabularies applied to a HCS. For example, if the provenance indicates that a clinical fact was generated

in the course of treatment in a U.S. realm 42 CFR Part 2 facility, then the clinical fact is labeled with a sensitivity code indicating that it is related to substance abuse and that its confidentiality level is “Restricted” because patient consent is required prior to disclosure,

- Nothing in the application of sensitivity labels prevents the appropriate disclosure of information affecting patient safety.

5. Technical Foundations

A healthcare information classification system provides standard, computable, and semantically interoperable means to apply sufficiently descriptive ACI (metadata) *about* healthcare information so that rights of access can be established, and appropriate access control decisions can be made at each layer of security services.

This includes access control governing:

- End users within the custodian’s enterprise,
- Disclosure by the information custodian, including:
- Segmentation by redaction, masking, and encryption of content “payload“,
- Controlling access to metadata appropriate to the security, business (inner) and transport (outer) envelopes encapsulating the payload,
- Specification of minimally disclosing payload metadata for use in federated Registry and Repository exchange architectures.
- Receipt, storage, routing, and re-disclosure by intermediaries acting on behalf of information custodians such as health information exchanges, health information service providers, clearinghouses, and gateways,
- Access, use, and any further re-disclosure by end users within the Receiver’s System.   In addition, the HCS security labels are intended to support other information management decisions such as audit, accounting of disclosure, and record management requirements such as compliance with record retention and breach notification policies.

6. Label-based[1] Access Control

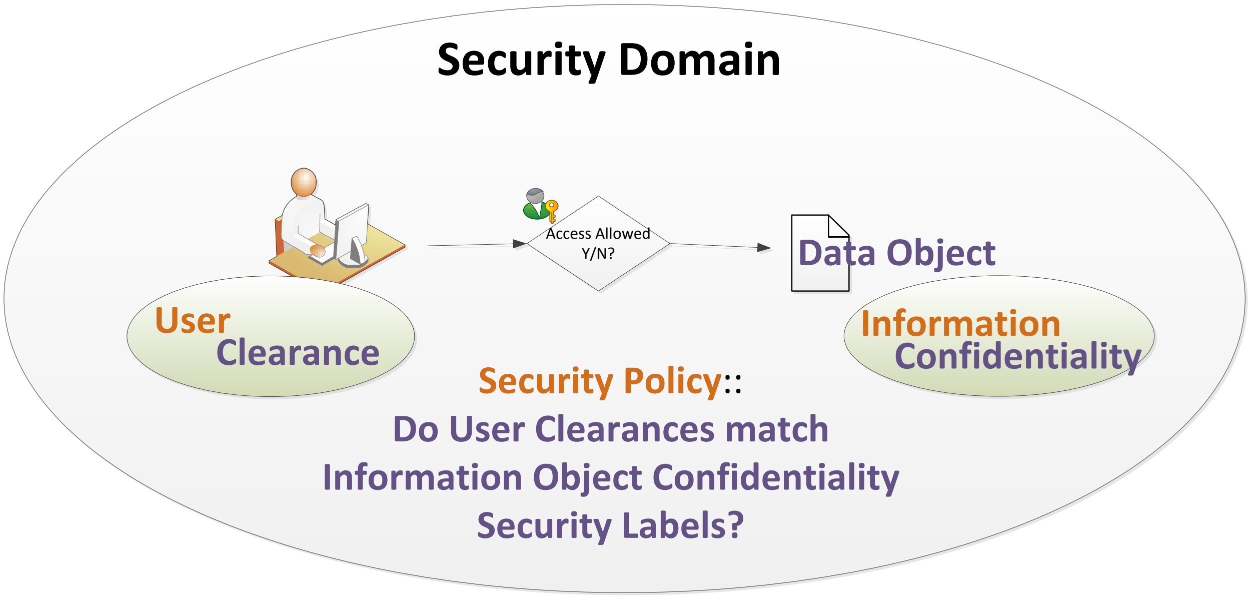

Security Domain
Access Allowed Y/N?
Data Object
User Clearance
Information Confidentiality
Security Policy::
Do User Clearances match Information Object Confidentiality Security Labels?

Figure 1 Access Control Model

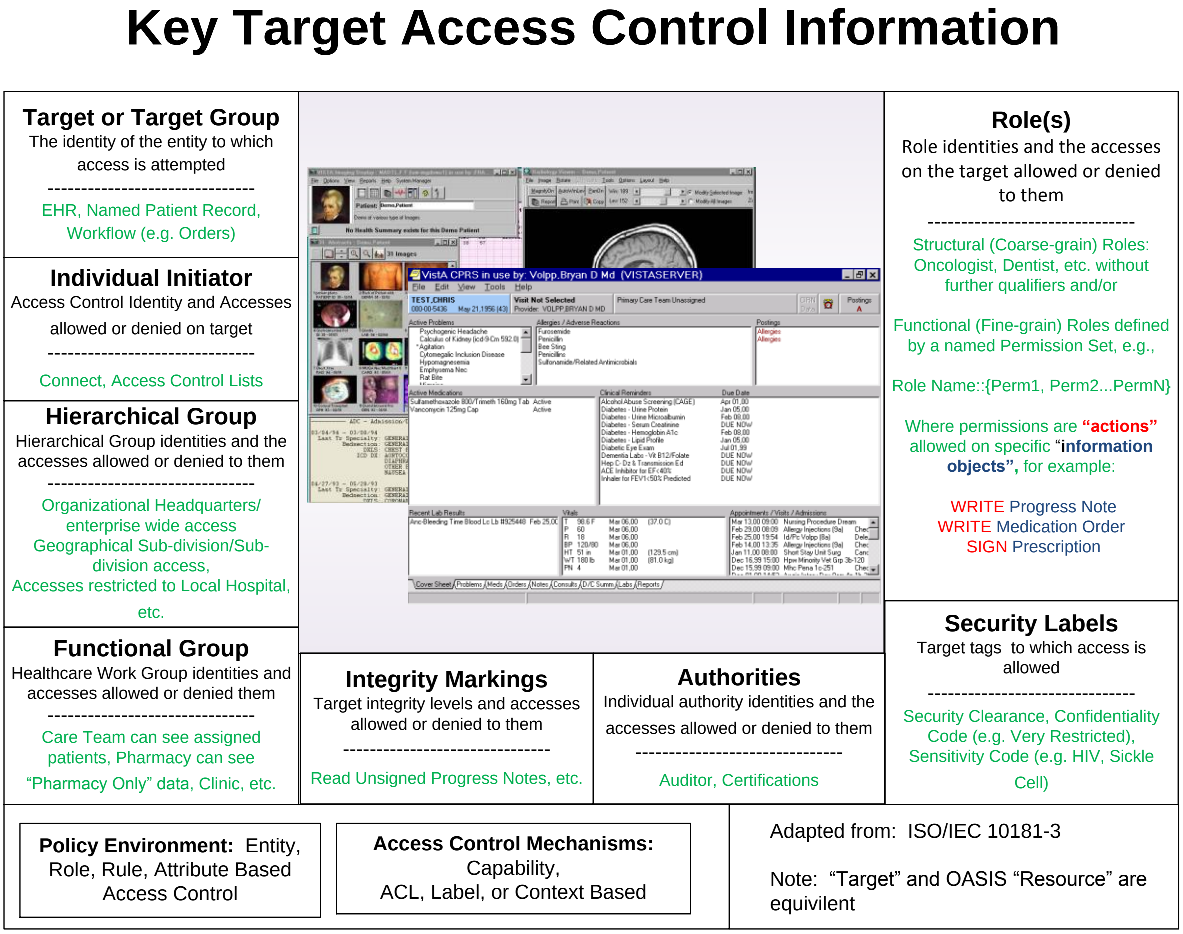
When an initiator is a human user (or an initiator process represents a human user), the label bound to the initiator often is called a clearance. In these cases, the label bound to the target (data object) is called a classification. (ISO 10181-3/ITU X.812)

As described in Figure 1, policy evaluation ensures that a user's security clearance meets or exceeds the security label field values "classifying" a data object (in this context, a "clinical fact"). For example, if the clinical fact is tagged with security label field values for sensitivity = HIV, then access is permitted only if the user possesses a security clearance that includes the corresponding HIV clearance.

Other policy matters may also need to be resolved as well, such as in the case that patient authorization was required as a pre-requisite for such disclosure, evaluation of environmental policies, etc. In security parlance a label is an attribute of security-relevant object. Labels are well-known security mechanisms and as used here are part of a broad category of attribute-based access control systems. See ISO 10181-3/ITU X.812for further information

6.1 Key Target Access Control Information

ISO 10181-3/ITU X.812 specifies key clinical fact (aka resource/target) access control decision information (ACDI) , which are representative of the metadata types that an access control service (ACS) uses to match the clearance of an initiator with the classification of the target. Different access control schemes may use a subset of these metadata types. Figure 2 below represents key types of metadata that particular access control scheme may use as ACDI.



Key Target Access Control Information

Target or Target Group
The identity of the entity to which access is attempted

EHR, Named Patient Record, Workflow (e.g. Orders)

Individual Initiator
Access Control Identity and Accesses allowed or denied on target
----
Connect, Access Control Lists

Hierarchical Group
Hierarchical Group identities and the accesses allowed or denied to them
----
Organizational Headquarters/ enterprise wide access
Geographical Sub-division/Sub-division access,
Accesses restricted to Local Hospital, etc.

Functional Group
Healthcare Work Group identities and accesses allowed or denied them
----
Care Team can see assigned patients, Pharmacy can see "Pharmacy Only" data, Clinic, etc.

Role(s)
Role identities and the accesses on the target allowed or denied to them
----
Structural (Coarse-grain) Roles: Oncologist, Dentist, etc. without further qualifiers and/or

Functional (Fine-grain) Roles defined by a named Permission Set, e.g.,

Role Name::{Perm1, Perm2...PermN}

Where permissions are **"actions"** allowed on specific "**information objects"**, for example:

WRITE Progress Note
WRITE Medication Order
SIGN Prescription

Integrity Markings
Target integrity levels and accesses allowed or denied to them
----
Read Unsigned Progress Notes, etc.

Authorities
Individual authority identities and the accesses allowed or denied to them
----
Auditor, Certifications

Security Labels
Target tags to which access is allowed

Security Clearance, Confidentiality Code (e.g. Very Restricted), Sensitivity Code (e.g. HIV, Sickle Cell)

Policy Environment: Entity, Role, Rule, Attribute Based Access Control

Access Control Mechanisms: Capability, ACL, Label, or Context Based

Adapted from: ISO/IEC 10181-3

Note: "Target" and OASIS "Resource" are equivilent

Figure 2 Types of Resource Access Control Information

A role-based access control system, for example, would be primarily focused on the initiator's roles. A label-based scheme, which is constructed in accordance with a rule-based access control model ((ISO/IEC 9594-2:2008/ITU X.501) would be primarily focused on clearances and target classifications. An attribute-based scheme would be primarily focused on ACDI in which roles, clearances and other access control decision information (e.g. the user's location, organizational affiliation etc.) are viewed collectively as attributes to be evaluated by a rules engine.

6.2 Applying Clinical and Security Labels

The clinical labels and attributes applied to clinical facts are expected to be slow changing and relatively static for an instance of clinical fact retained within the EHR repository. Accordingly, while the rules for applying clinical attributes may change over time, such change is unlikely to have significant impact on the day to day use of clinical information retained within the EHR.

On the other hand, security and privacy rules policy rules are relatively dynamic and depend upon a number of factors external to the clinical facts themselves such as the patient consent directives, purpose of use of the information, environmental constraints, the identity and roles of the requestor, and various policies for use and re-disclosure of the information by the recipient, which cannot be known or predicted in advance.

This variability in general cannot be resolved except in the context of a specific response managed adjudicated under the rules of a security and privacy access control service. Some conclusions of this, represented in this section and the models which follow include:

- Maintaining static tagging of security and privacy labels for individual clinical facts may be problematic, inefficient or impossible as the tags and rules for any particular access present variability that cannot generally be assessed until runtime,
- Security and privacy tagging is best done at runtime when access control variables about to whom, why, where, and what type of information are known and can be resolved,
- Security and privacy tagging is applied to the aggregated EHR response to a query for information based upon rules, policies, and obligations in effect at the time of release,
- The preservation of the tagging, handling caveats (including obligations), and information provenance becomes the responsibility of the recipient if subsequent reuse or disclosure to additional parties is contemplated.

Security labels allow for the management and enforcement of inter-enterprise privacy policies. Enterprises receiving information become, in effect, the equivalent of registered system users of an information owner's access control service. Users of a receiving enterprise desiring to subsequently further re-disclosure this information may be obligated to adhere in the future to policies agreed to when the original request was made. This means that received information, meta-data and provenance must be retained with the information as a whole for its lifetime.

6.3 Categories and Clearances of Security Labels

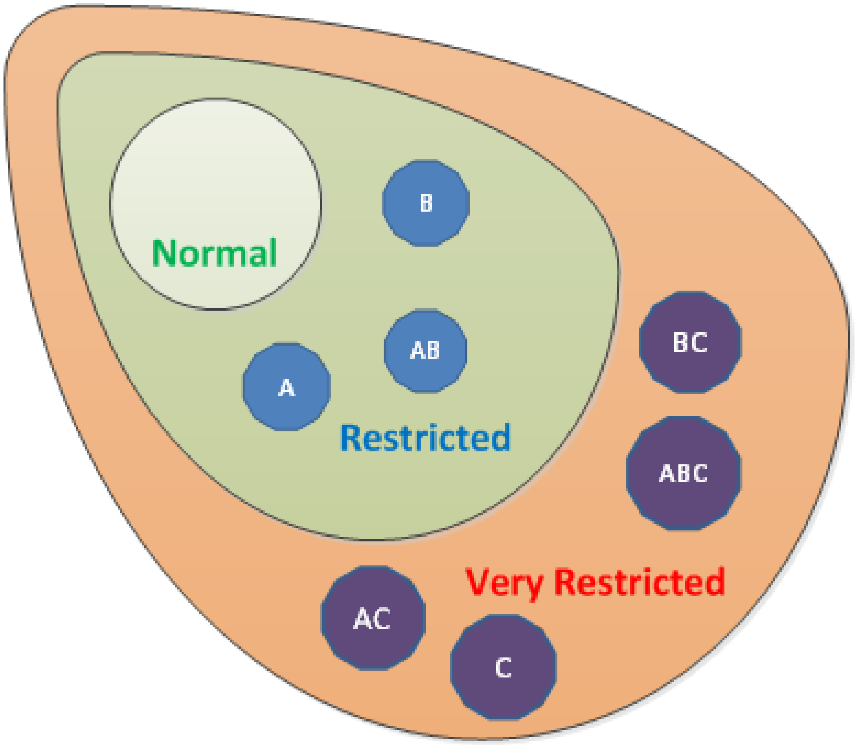


Figure 3 Applied Data Classification Example

Figure 3 represents a model classification system consisting of three major categories of Normal, Restricted and Very Restricted. Restricted contains 3 sub-categories A, B and AB. Very Restricted contains 4 sub categories, C. AC. BC and ABC. This system controls user access to major categories and sub-categories of clinical facts by comparing the security label in a user clearance with the security label on the clinical fact.

Users possessing the Very Restricted clearance can access Very Restricted clinical fact categories with exception of C, AC, BC and ABC. Access to these categories requires both the Very Restricted clearance and individual clearances for the four sub-categories. Users possessing the Very Restricted clearance can also access Restricted clinical facts (contained within the Very Restricted category), but only A, B, and AB as authorized. Users possessing the Very Restricted clearance can access all clinical facts in the Normal category contained within the Very Restricted and Restricted category.

Users possessing the Restricted clearance can access all clinical facts in the Restricted category, but only A, B, and AB as authorized. Users with the Restricted clearance can also access all clinical facts in the Normal category.

Users possessing the Normal clearance can access all clinical facts in the Normal category, but no clinical facts in the Restricted and Very Restricted categories including the special sub-categories.

Note that users cannot possess sub-category clearance without first possessing the clearance for the major categories Restricted and/or Very Restricted. These HCS rules for matching the security labels on clinical facts with a user's clearance ("dominance rules") can be extended to include integrity classifications (e.g., a hierarchy from very reliable to unreliable) and integrity categories (e.g., workflow status of a healthcare record from initial to complete to legally attested).

7. HCS Operational Model

Figure 4 HCS Functional Model, provides a high level view of the components used by a Segmenting EHR to semantically label clinical facts with sufficient metadata to enable the EHR Access control service to apply the security labels required for compliance with privacy policies.

EHR semantic labeling is a function of the clinical domain, which must be capable of disaggregating clinical elements into discrete clinical information objects, which have sufficient meaning to be understood on their own, e.g., observation, medication, procedure, lab results etc. The EHR generates "clinical facts" by applying semantically interoperable clinical attributes to clinical elements in accordance with organizational and jurisdictional clinical guidelines.

A Security Labeling Service is the pivotal capability applying and enforcing the HCS. The following conceptual model illustrates the relationship between the clinical system's generation of clinical facts and the security system's labeling of those facts per policy and consumption of the labels to enforce access control

The Access Control Service invokes a Security Labeling Service to apply security labels to clinical facts in accordance with organizational and jurisdictional privacy policies, including any patient privacy consent directives associated with these clinical facts. It then enforces access controls on requests for EHR data. See Figure 5: Applying Clinical Labels.

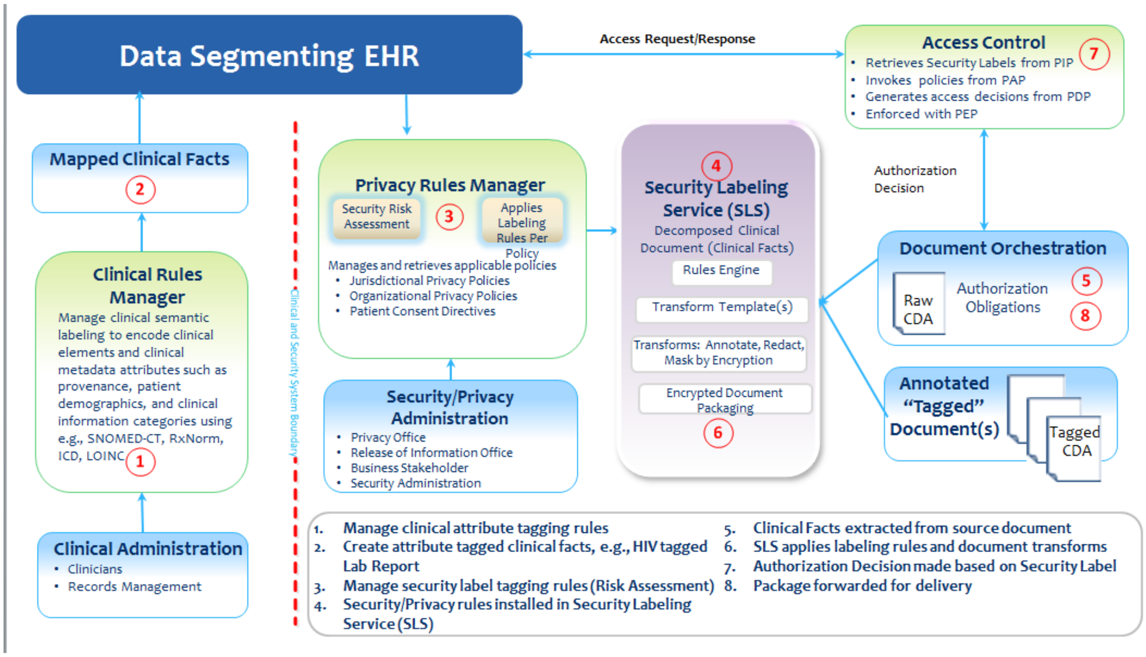

Data Segmenting EHR
Access Request/Response
Access Control
7
Retrieves Security Labels from PIP
Invokes policies from PAP
Generates access decisions from PDP
Enforced with PEP
Mapped Clinical Facts
2
Clinical Rules Manager
Manage clinical semantic labeling to encode clinical elements and clinical metadata attributes such as provenance, patient demographics, and clinical information categories using e.g., SNOMED-CT, RxNorm, ICD, LOINC
1
Clinical Administration
Clinicians
Records Management
Clinical and Security System Boundary
Privacy Rules Manager
Security Risk Assessment
3
Applies Labeling Rules Per Policy
Manages and retrieves applicable policies
Jurisdictional Privacy Policies
Organizational Privacy Policies
Patient Consent Directives
Security/Privacy Administration
Privacy Office
Release of Information Office
Business Stakeholder
Security Administration
4
Security Labeling Service (SLS)
Decomposed Clinical Document (Clinical Facts)
Rules Engine
Transform Template(s)
Transforms: Annotate, Redact, Mask by Encryption
Encrypted Document Packaging
6
Authorization Decision
Document Orchestration
Raw CDA
Authorization Obligations
5
8
Annotated "Tagged" Document(s)
Tagged CDA
1. Manage clinical attribute tagging rules
2. Create attribute tagged clinical facts, e.g., HIV tagged Lab Report
3. Manage security label tagging rules (Risk Assessment)
4. Security/Privacy rules installed in Security Labeling Service (SLS)
5. Clinical Facts extracted from source document
6. SLS applies labeling rules and document transforms
7. Authorization Decision made based on Security Label
8. Package forwarded for delivery

Figure 4 HCS Operational Model

7.1 HCS General Functional Model

Functional requirements for a HCS are typically integrated within the functional model for the health care IT system in which the HCS is implemented. HCS functional requirements may vary depending on the business requirements for the specific health care IT system. Examples of health care IT systems include provider EHRS, patient PHRS, health plan enrollment, claims, and operational IT systems, Health Information Exchanges, Health Information Service Providers, and Clearinghouses.

Data Segmentation Functional Model Capabilities are detailed in Figure 4. These are aligned with the business requirements listed in Appendix B Table of HCS Requirements, which provides the detailed business requirements for a *Segmenting EHR*. [The diagram includes capability descriptions that display when pointer is placed over the capability

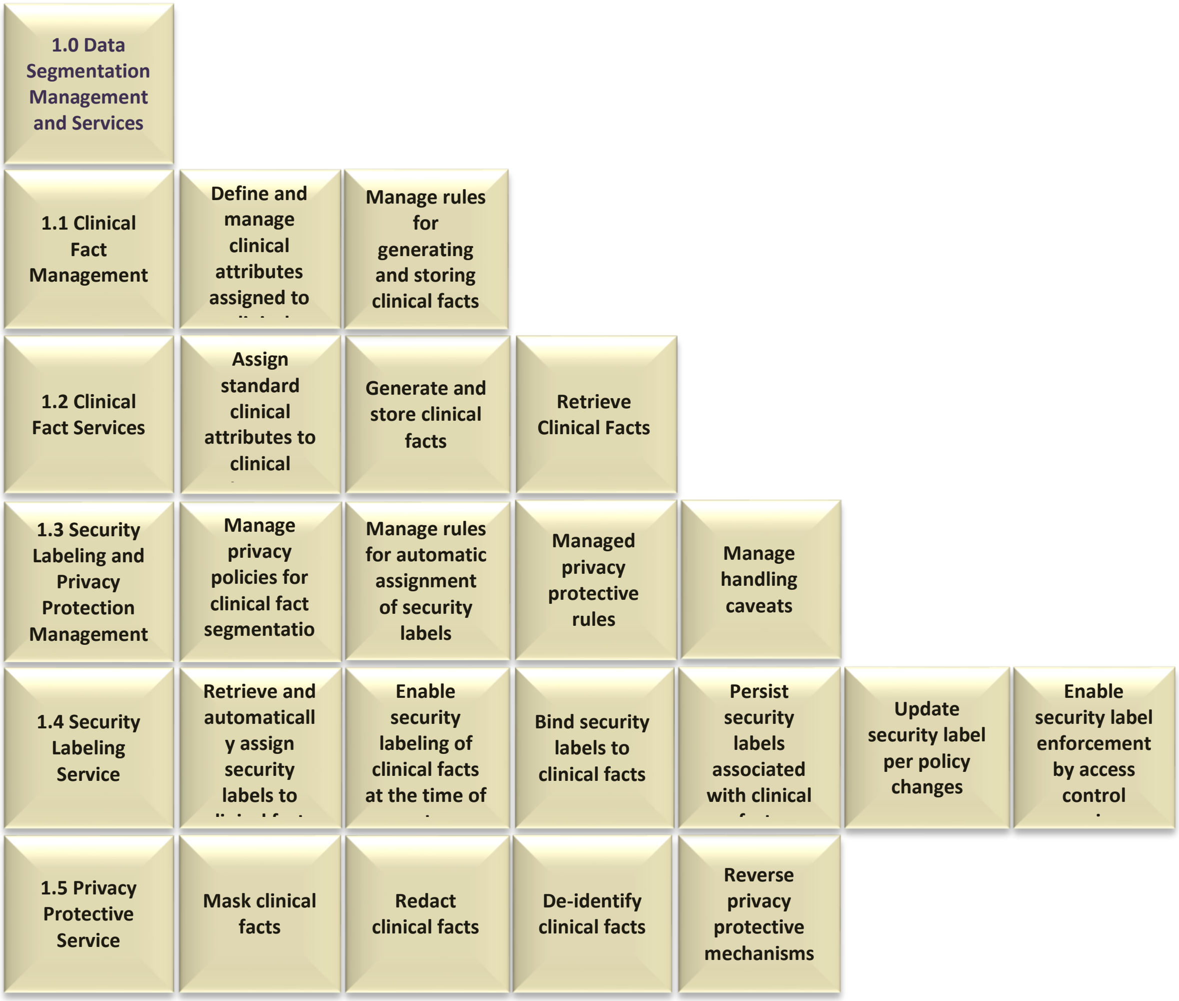

1.0 Data Segmentation Management and Services
1.1 Clinical Fact Management
Define and manage clinical attributes assigned to
Manage rules for generating and storing clinical facts
1.2 Clinical Fact Services
Assign standard clinical attributes to clinical
Generate and store clinical facts
Retrieve Clinical Facts
1.3 Security Labeling and Privacy Protection Management
Manage privacy policies for clinical fact segmentatio
Manage rules for automatic assignment of security labels
Managed privacy protective rules
Manage handling caveats
1.4 Security Labeling Service
Retrieve and automaticall y assign security labels to
Enable security labeling of clinical facts at the time of
Bind security labels to clinical facts
Persist security labels associated with clinical
Update security label per policy changes
Enable security label enforcement by access control
1.5 Privacy Protective Service
Mask clinical facts
Redact clinical facts
De-identify clinical facts
Reverse privacy protective mechanisms

Figure 5 Data Segmentation Functional Model

8. Application of Labels to Healthcare Systems

8.1 Using Labels for Clinical Management

The application and use of clinical labels provides for the creation of structured information for clinical, financial, operational, research and other workflows. Such usages include healthcare specific treatment purposes such as orders, recording an observation, patient history, medication, and immunization data or for providing various types of clinical decision support services.

The purpose of clinical labeling is intended to be primarily clinical support, factual and unclouded by perceived risks of stigmatizing harm resulting from unauthorized disclosure.

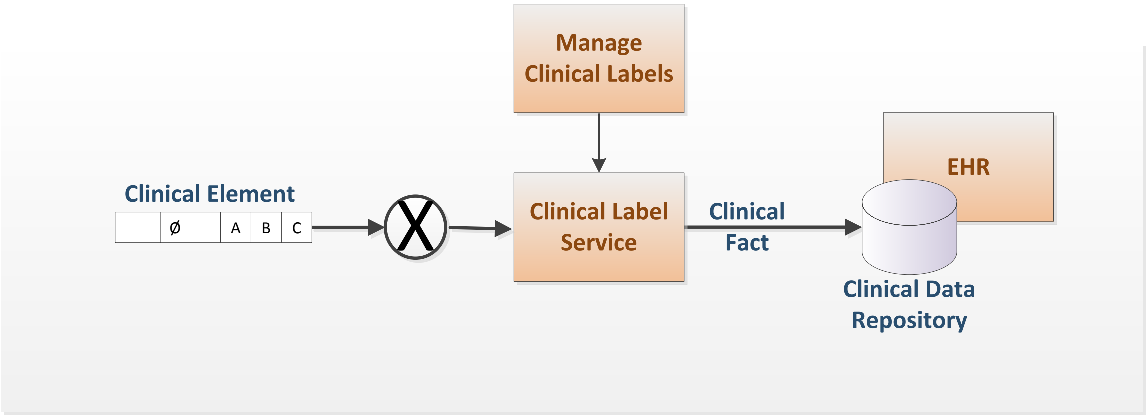


Figure 6 Applying Clinical Labels

Figure 6 illustrates the binding of clinical elements to clinical labels through a Clinical Label Service to create clinical facts stored in the Clinical Data Repository of an Electronic Health Record (EHR).

Manage Clinical Labels provides precursor provisioning of the Clinical Labeling Service-with (standardized) clinical vocabularies and rules for binding labels to clinical elements. This component:

- Establishes clinical vocabularies to be used for tagging and,
- Defines rules for tagging clinical elements,
- Provisions Clinical Label Services.

Clinical Labeling Services apply clinical labels according to the established rules in an operational context. The Clinical Labeling Services component:

- Retrieves clinical elements and their clinical attributes Tags,

- Creates clinical facts by application of clinical attributes (standard metadata) to clinical elements by a clinical rule,
- Stores clinical facts in EHR repository.

8.2 Using Labels for Policy Enforcement

Security labels are applied based on risk assessment of harm resulting from unauthorized disclosure. This assessment may reflect personal perceptions or legal requirements, which may involve inherently emotional characterization of clinical information as prejudicial to a party's "interests" when exposed in unauthorized ways or to those who lack authority and responsibility for its care and use.

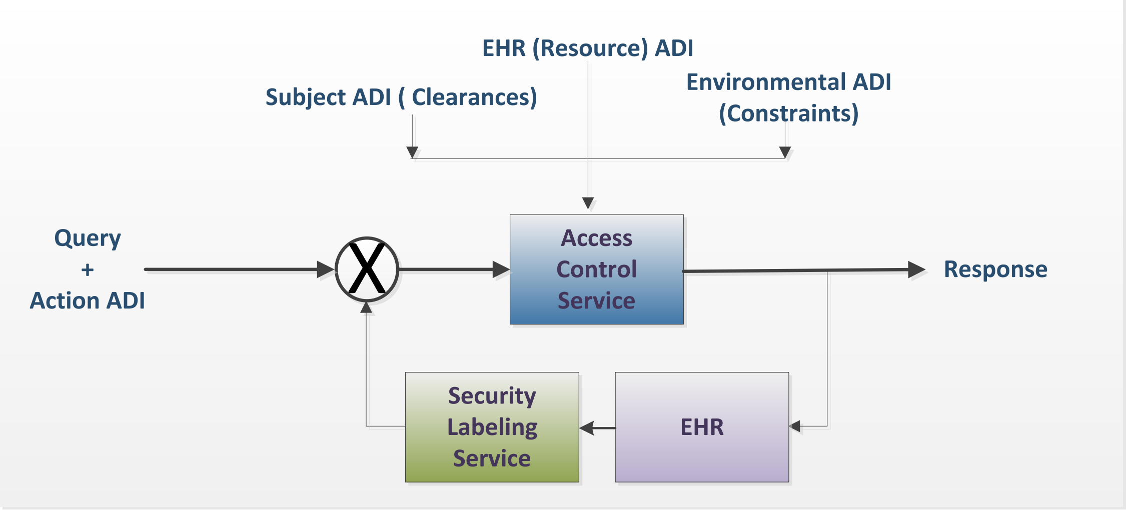

EHR (Resource) ADI
Subject ADI (Clearances)
Environmental ADI (Constraints)
Query + Action ADI
Access Control Service
Response
Security Labeling Service
EHR

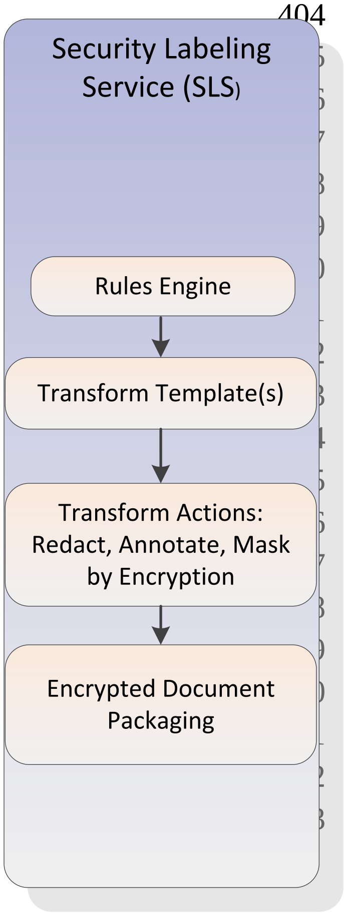
Figure 7 Applying Security Labels and Masking Rules to EHR Query- Response

Access Control Service (ACS)

As illustrated in Figure 7, the Access Control Service accepts and mediates all requests for EHR information. When a request for protected information is received, the ACS must first establish that the request itself and the requestors asserted attributes meets acceptance parameters. If not, the query is rejected and an appropriate negative response returned. Following this first pass, the request is then forwarded to the EHR which returns the initial response to the Security Labeling Service. The Security Labeling Services labels the EHR response content, applies masking/redaction and obligation rules. The ACS then returns the completed response.

In general, the ACS acts as a monitor for policy enforcement including all requests for protected information both internal and external. The access control service is made up of the following general capabilities:

- Policy Administration Point (PAP): Manages the complete jurisdictional, organizational and subject (e.g., patient, employee) privacy policies for a specific target, and translate these into security policy sets for input to the PDP (Policy Decision Point), which are persisted in the PAP database,
- Policy Information Point (PIP): Manages access control decision information (ACI) of different types to identity attributes by subject, resource, action or environment including identifier, data-type and optionally issuer,
- Policy Decision Point (PDP). Access Control Decision Information (ADI) is the subset of ACI needed for a specific authorization instance. To make the decision, the PDP is provided with, or acquires ADI associated with the initiator, the target and the action. Other inputs to the PDP are the access control policy rules from PAP policy sets and contextual information needed to interpret the ADI or the policy,
- Policy Enforcement Point (PEP). The PEP is responsible for ensuring that any actions by the initiator on the target are authorized (by the PDP). When an initiator makes a request to perform an action on the target, the PEP invokes the services of the PDP so that a decision can be made.


Security Labeling Service (SLS)
Rules Engine
Transform Template(s)
Transform Actions: Redact, Annotate, Mask by Encryption
Encrypted Document Packaging

Security Labeling Service

The Security Labeling Service evaluates the clinical tagging and provenance of items in the initial EHR response to determine the security labels to be assigned and how the final response is to be packaged for delivery.

The Security Labeling Service is provisioned by a Security Label Management Sub-System (Not shown) which establishes/provisions security tagging vocabularies and creates security labeling rules to support jurisdictional and organizational privacy policies and patient consent directives including Obligations or rules that must be met prior to release of information.

The Rules Engine is provisioned with policies established by the Security Label Management Service described above. The Rules Engine contains the logic for applying security and privacy tagging to clinical elements of a query response.

Pre-developed Transform Templates provide document/format specific representations of the final response. Transform Templates establish how and where security and privacy tags are to be applied.

Figure 8 Security Labeling Service

Transform Actions apply the tagging to the final form of the response through rules contained in the Rules Engine. This tagging “segments” the response into logical categories for downstream application of a wide variety of access control policies. Annotations include document, portion and entry-level tagging as well as application of handling instructions.

Transform actions also include content masking or redaction. Masking allows authorized recipients access to protected information by decrypting content based upon cryptographic keys corresponding to their authorizations and clearances. Redaction removes content from the response, making it impossible to recover regardless of permissions.

In the final step, the Security Labeling Service encrypts the final result into an inner envelope with high-water mark classification and handling instructions and an encrypted outer envelope for transmission but without any external indicators of the nature of the inner content.

Security labeling, redaction, and masking of unstructured PHI such as a provider’s dictated consult note, require fully encoding of the clinical facts comprising the unstructured PHI and references linking each coded “structured” clinical fact back to the associated unstructured clinical fact. This enables the ACS to restrict access to and disclosure of unstructured clinical facts based on the security labels on the structured clinical facts. The ACS uses the structured clinical fact security labels to assign handling caveats and apply any redaction or masking required for disclosure of the narrative block. [More detailed discussion in Appendix I. ***Rendering CDA with Security Labels***].

9. HCS Security Labels

HCS Security Labels conform to NIST FIPS PUB 188 Standard Security Label structure, which consists of a set of specified fields. Each field comprises a globally unique Tag Set Name and a set of semantically interoperable security tag or field values. The following diagram is a more extensive version than that shown in the HCS and includes all of the Integrity label field types.

Guide to the HL7 Health Care Privacy and Security Classification System

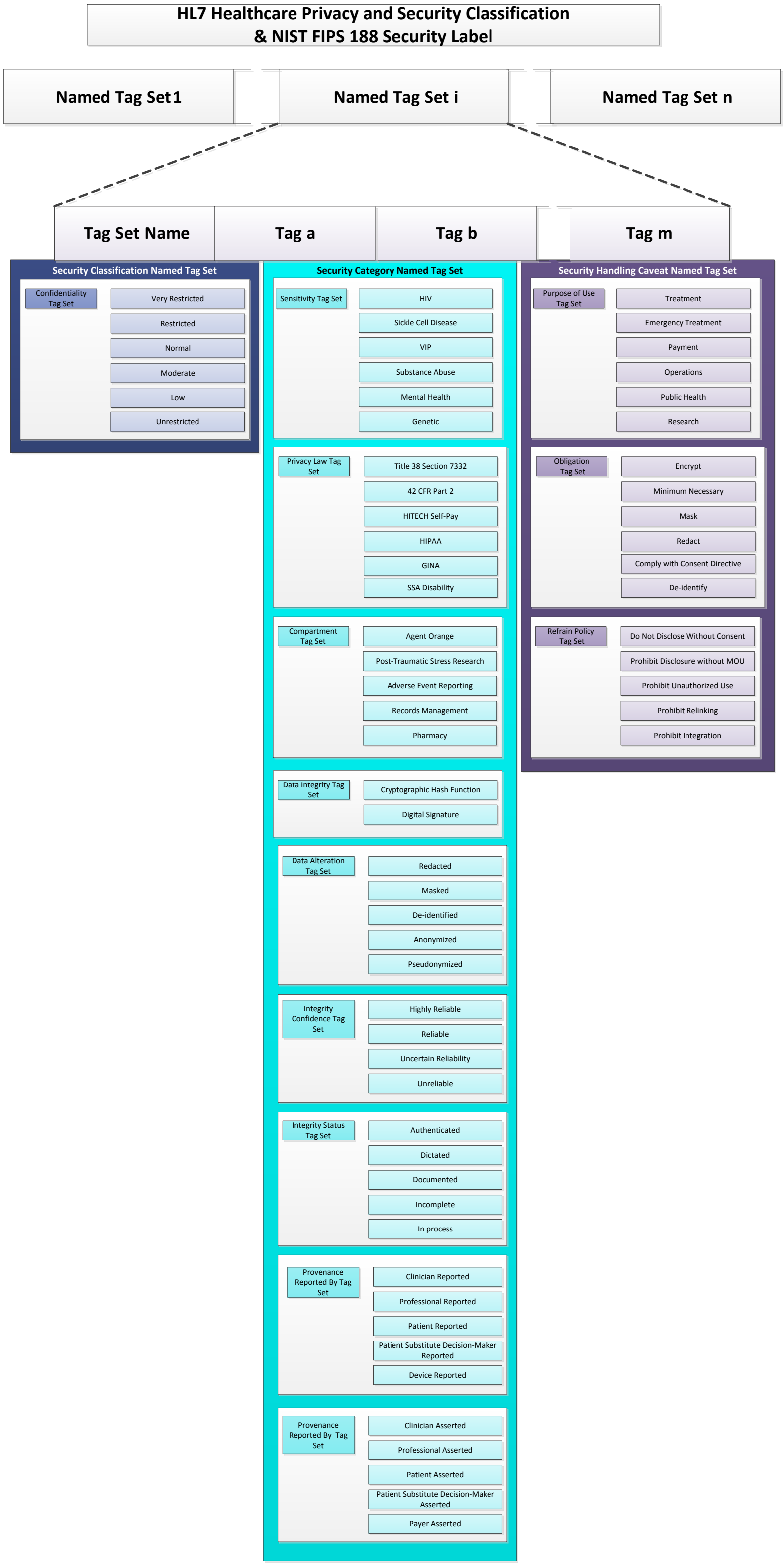


Figure 9 NIST Security Label Field Structure

These labels define the classification of each item and constituent components (inner envelope, cover sheet, body, and section(s) and sub-sections, segments portions and entry elements).

- Objects in the HCS can either be a container (element) for content or content for another container,
- Encoded clinical data goes into clinical element fields,
- Metadata goes into metadata attribute fields,
- Metadata is data about data.

9.2 Security Labels in Practice

Figure 10 below, Aggregating Clinical Facts, illustrates an EHR view of individual clinical facts used to produce a composite result, here a generic prescription. The un-normalized database view illustrates the concept that each clinical fact does not redundantly repeat needed information, that groups of information (Demographics, Diagnosis and Order) receive and provide information by means of key field linkages. For example, Diagnosis "provenance" information, as well as patient demographics, is available to Order via the Diag_Order_Link table (wasDerivedFrom). The EHR table fields represent smallest dis-aggregated pieces of clinically relevant information relative to the Rx.

Without these links, it would be impossible to create composite output without redundantly managing information in each of the linked tables which in itself would become a data management issue to ensure consistency.
Put another way, each EHR table is uniquely "authoritative" for the information it holds.

Figure 11 below illustrates the binding of security and privacy labels by means of a rule. The elements of the EHR (patient Demographics, Diagnosis and Order) and their relationships are established in the EHR as discussed previously.
A privacy rule is applied to composite information extracted from the EHR for creating a report of the patient's medication history. Based upon knowledge of the values for the clinical diagnosis (HIV), the rule is able to associate the fact that the medication is sensitive having been prescribed for the HIV condition and not another, along with provenance information related to the patient's coverage, the provider type, and service delivery location. The security labeling service is then directed to apply the appropriate confidentiality and sensitivity codes based upon this rule.

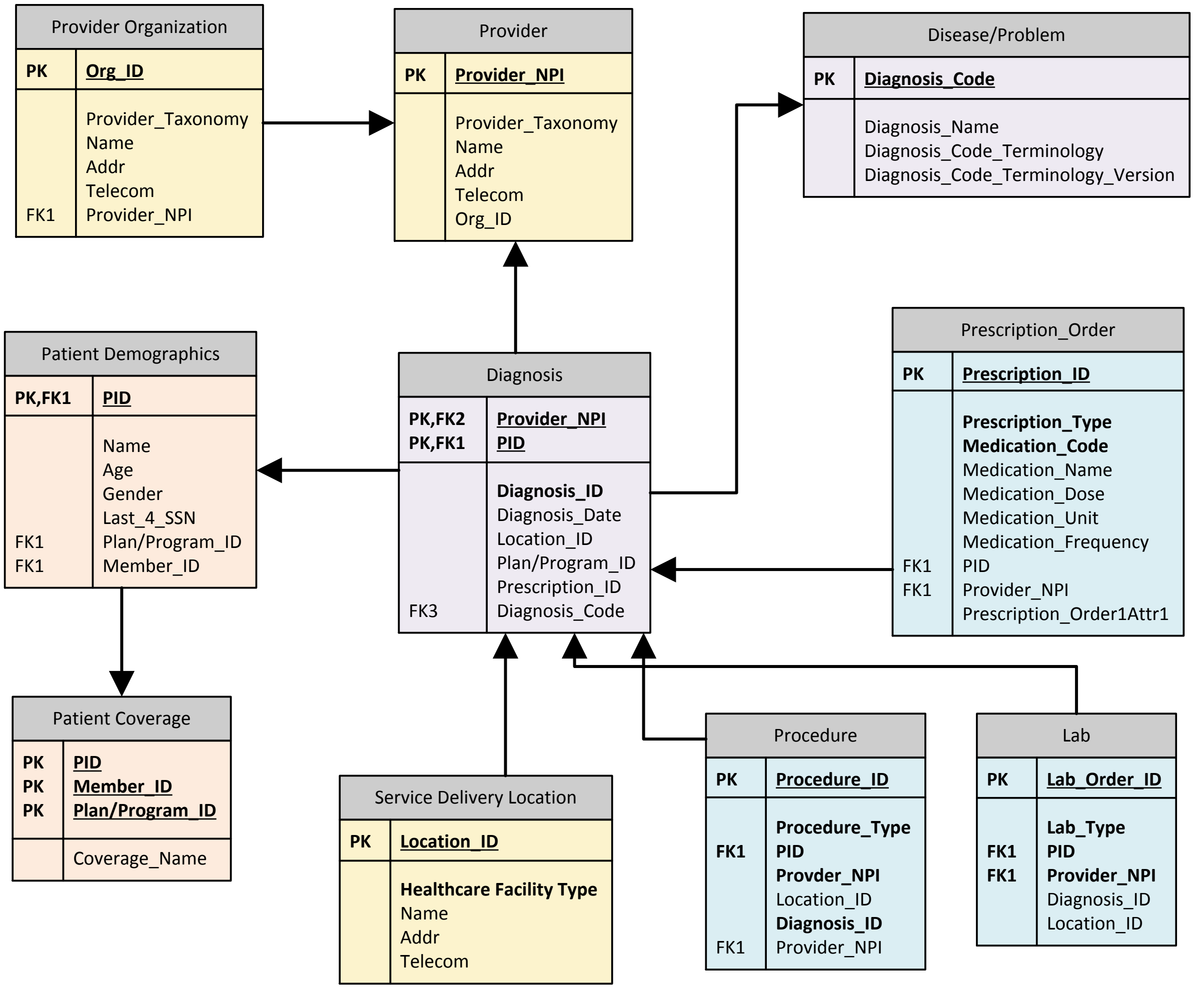
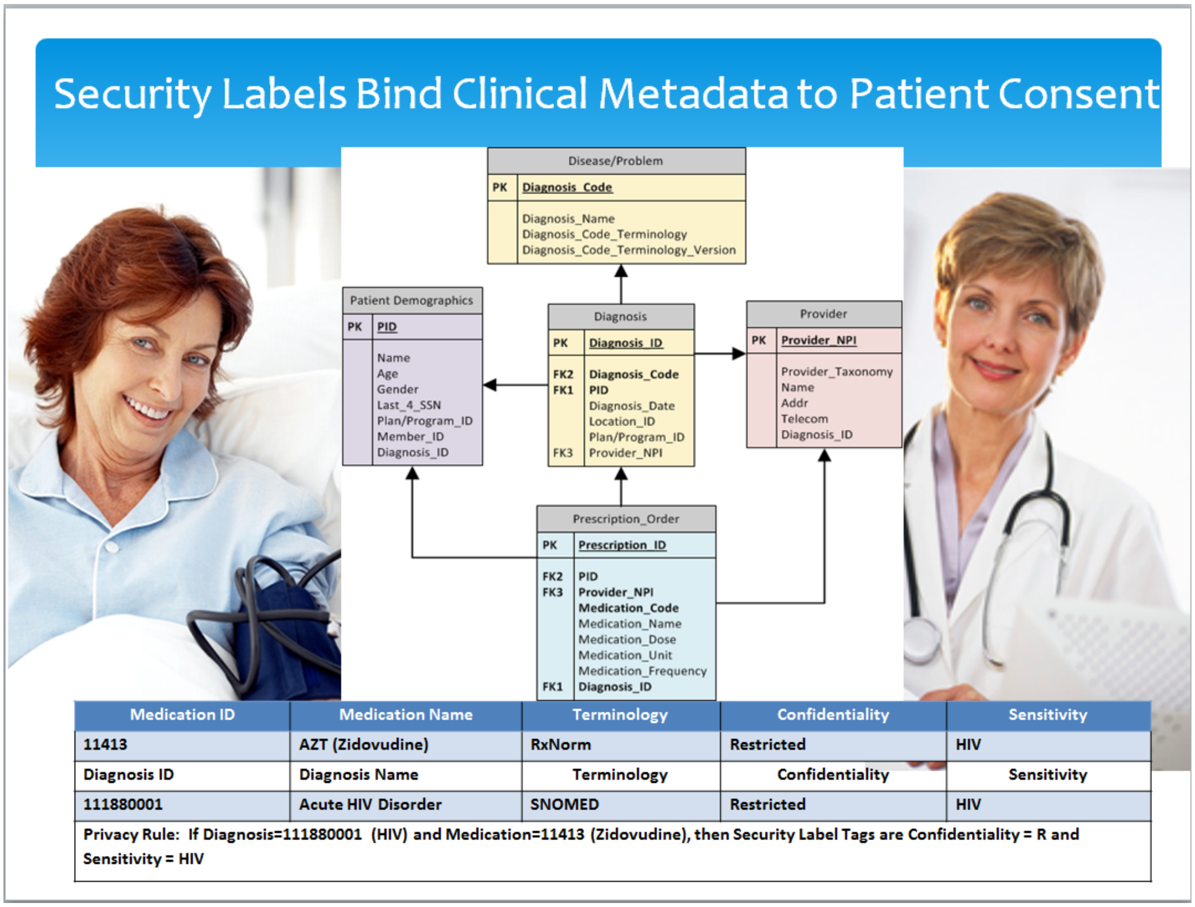


Figure 10 Aggregating Clinical Facts in database tables into more complex Clinical Facts

Final release of the medication history may depend on additional factors, not shown here. For example, without a patient consent, the USC Title 38 Article 7332 HIV data may be masked or redacted by access control services prior to allowing disclosure to an external requesting party.



Security Labels Bind Clinical Metadata to Patient Consent

Disease/Problem
PK Diagnosis_Code
Diagnosis_Name
Diagnosis_Code_Terminology
Diagnosis_Code_Terminology_Version

Patient Demographics
PK PID
Name
Age
Gender
Last_4_SSN
Plan/Program_ID
Member_ID
Diagnosis_ID

Diagnosis
PK Diagnosis_ID
FK2 Diagnosis_Code
FK1 PID
Diagnosis_Date
Location_ID
Plan/Program_ID
FK3 Provider_NPI

Provider
PK Provider_NPI
Provider_Taxonomy
Name
Addr
Telecom
Diagnosis_ID

Prescription_Order
PK Prescription_ID
FK2 PID
FK3 Provider_NPI
Medication_Code
Medication_Name
Medication_Dose
Medication_Unit
Medication_Frequency
FK1 Diagnosis_ID

Medication ID	Medication Name	Terminology	Confidentiality	Sensitivity
11413	AZT (Zidovudine)	RxNorm	Restricted	HIV
Diagnosis ID	Diagnosis Name	Terminology	Confidentiality	Sensitivity
111880001	Acute HIV Disorder	SNOMED	Restricted	HIV

Privacy Rule: If Diagnosis=111880001 (HIV) and Medication=11413 (Zidovudine), then Security Label Tags are Confidentiality = R and Sensitivity = HIV

Figure 11 Applying Security Labels Based on a Rule

9.3 Representative Data Segmentation for Privacy Approach

Table 2, General Approach to Data Segmentation by Attribute (Example) below, is a generalized sample template for specifying the rules and analyzing instances of semantic and security labeling of clinical facts. The table includes Clinical Facts, Clinical Attributes, Provenance Attributes and Security Label Attributes.

Examples of analyzed instances follow in Table 3 HL7 Security Observation Value Codes.

CLINICAL FACT

The tagged clinical element is the de-aggregated smallest health care relevant tagged clinical component. Clinical facts are elemental information objects in a clinical environment. See for example the HL7 Electronic Health Record-or the HL7 RBAC Permission Catalog information objects.

CLINICAL ATTRIBUTE

Clinical attributes are selected values from a code system used to label clinical elements. Representative sample code systems used in health care include:

- SNOMED CT,
- LOINC,
- RxNORM,
- ICD 9/10.

PROVENANCE ATTRIBUTES

Figure 9 illustrates the functionality provided by the foreign keys relating clinical facts to each other for tagging purposes. The linkages and history of clinical facts defines the essential element of their provenance. Provenance provides the context and history of an object. Provenance may provide information about the reliability of a clinical fact and confidence that the fact is accurate and trustworthy. Provenance attributes provide useful information needed by the security labeling system, for example as an integrity tag. Accordingly, this guide adopts the vocabulary and entity relations of the W3C for the description of provenance and entity relations (See Appendix D *PROVENANCE RELATIONS DEFINED BY W3C*).

SECURITY LABEL ATTRIBUTES

These are the attributes and labels previously discussed in section 7.1 Data Segmentation Attribute types above.

Table 1 General Approach to Data Segmentation by Attribute (Example)

Clinical Fact	Clinical Attribute	Provenance Attributes	Security Label Attributes
Clinical Fact Name	Clinical Attribute Name	Clinical attribute provenance including: · wasAttributedTo · wasDerivedFrom · wasGeneratedBy · wasInformedBy · wasInfluencedBy · hadPrimarySource · wasInvalidatedBy · wasQuotedFrom · wasRevisionOf	Security attribute metadata including: · Classification, · Sensitivity, · Integrity, · Category, · Handling Instructions

Table 3 HL7 Security Observation Value Codes illustrates the application of specific code/values sets and provenance labels applied to clinical facts of Diagnosis, Medications, Allergies, Laboratory Report, and Procedure.

Table 2 HL7 Security Observation Value Codes

Clinical Fact	Clinical Attribute	Provenance	Security Label
			(HL7*)
Diagnosis	<Patient Name >		N
	Source=<Organization>		N
	111880001 Acute HIV infection (disorder)	hadPrimarySource: SNOMED Code	Restricted, HIV
		wasAttributedTo: <Attending>	
Medications	<Patient Name >		N
	11413 Zidovudine (AZT)	hadPrimarySource: RxNorm	
		wasDerivedFrom: Diagnosis	Restricted, HIV
Allergies	<Patient Name >	wasDerivedFrom: Encounter	N
	91936005 (Penicillin)	hadPrimarySource: SNOMED CT	N
Laboratory Report	8053 (Lipid Panel)	hadPrimarySource: LOINC	N
	8320 Total Cholesterol		
	8316 Triglyceride		
	8429 HDL		
	7973 LDL		
Procedure	86689.Z7 (HIV-1 Western Blot)	hadPrimarySource: CPT	Restricted, HIV

APPENDIX A: TABLE OF DEFINITIONS

Table A: Table of Definitions

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
Access Control Service	A service that provides the basic operational aspects of access control such as making access control decision information (ADI) available to access decision components and performing access control functions. The service also provides security labeling and privacy and security protection functions. The service, known as an Access Control Service (ACS), requires the following infor-mation: Access policy rules, Contextual information needed to interpret ADI, Initiator, target, and access request ADI, Security labeling rules and vocabulary, Transform rules and services. ACS generates information made available to other elements includes transformed information response to an information request as well as handling caveats.
Access (Security) Level	The combination of a hierarchical security classification and a security category that represents the sensitivity of an object or the security clearance of an individual. [ISO 2382-8/T-REC-X.812-199511-I!!PDF-E] A level associated with an individual who may be accessing information (for example, a clearance level) or with the information which may be accessed (for example, a classification level).[HIPAA Security Glossary]
Break the Glass	"Break the glass" access barriers are application generated warnings at the moment of possible transgression that requires users to assert their need for access. Distinguish break glass from emergency access. In the case of break glass no additional user permissions are required (similar to a fire alarm in a hallway, all users have access to the alarm); however, access may involve alerts to system managers and increased auditing. Examples of break glass include access to one's own records, to records belonging to a spouse, family member or to a VIP. In contrast to emergency access, break glass does not require evaluation of patient consent directives, nor is eminent threat to patient safety a concern. Security Work Group Emergency Access paper
Classification *Child concept: Security Classification*	Confidential protection of data elements by segmentation into restricted and specifically controlled categories set by policies, professional practice, and laws, legislation, and regulations. [Adapted from ASTM E-1986]
Clearance	Initiator-bound access control information (ACI) that can be compared with security labels of targets. [ISO 10181-3/ITU X.812]
	Permission granted to an individual to access data or information at or below a particular security level. [ISO/IEC 2382-8:1998]
Clinical attribute	Any clinical characteristic that binds a health care relevant parameter to a clinical element by a rule. Parameters may include authorship, category of information, terminological characteristics, history of permutations, integrity and provenance, as well as the relationship to and inclusive of associated clinical facts necessary to provide context essential for applying security labels. [PCAST discusses attributes that provide context to clinical data elements such as patient demographics.]

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
Clinical Attribute set	The complete collection of parameters that in total describe the relevant characteristics of a clinical fact. These include, clinical attributes, security labels and provenance: For example, the patient's name and birthdate, diagnosis code, the applicable privacy rules and policies, including any patient's pre-consented privacy choices security label classification and sensitivity codes, and the data source (provider).
Clinical element	A clinical object that has been disaggregated into the smallest possible data element suitable for use in a healthcare context. [PCAST p. 70 description of clinical elements as the smallest clinical data units that make sense to exchange and aggregate.]
Clinical fact	A healthcare data IT resource comprised of a clinical element associated or "tagged" with at least one clinical attribute such as a clinical information category, patient information, and provenance. A clinical fact is a type of "tagged data element." [PCAST p. 89 "Tagged data element: Data accompanied by metadata describing the data."]
Clinical rule	A computational algorithm used for assigning a clinical attribute to a clinical element.
Compartment	A security label tag that "segments" an IT resource by indicating that access and use is restricted to members of a defined community or project. A set of categories in a security label. [Sandhu]
Compartment-based policies	In a compartment-based policy, sets of targets are associated with a named security compartment or category, which isolates them from other targets. Users need to be given a distinct clearance for a compartment to be able to access targets in the compartment. [Ford Chapter 6 p.155]
Compartmentalization	A division of data into isolated blocks with separate security controls for the purpose of reducing risk. [ISO 7498-2] Example: The division of data relative to a major project into blocks corresponding to subprojects, each with its own security protection, in order to limit exposure of the overall project.
Confidentiality	Privacy metadata classifying an IT resource (data, information object, service, or system capability) according to its level of sensitivity, which is based on an analysis of applicable privacy policies and the risk of financial, reputational, or other harm to an individual or entity that could result if made available or disclosed to unauthorized individuals, entities, or processes. Usage Notes: Confidentiality codes are used in security labels and privacy markings to classify IT resources based on sensitivity to indicate the custodian or receiver obligation to ensure that the protected resource is not made available or re-disclosed to individuals, entities, or processes (security principals) per applicable policies. Confidentiality codes are also used in the clearances of initiators requesting access to protected resources. Map: Definition aligns with ISO 7498-2: Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. [HL7 Confidentiality code system 2.16.840.1.113883.5.25 and value set 2.16.840.1.113883.1.11.10228]

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
Data Segmentation	Process of sequestering from capture, access or view certain data elements that are perceived by a legal entity, institution, organization or individual as being undesirable to share. [Goldstein GWU]
End User	Person or organization who utilizes information processing facilities or systems, e.g., employee, contractor or third party user. [ISO 27011]
Healthcare Privacy and Security Classification System (HCS)	A defined scheme for the classification and handling of health care and healthcare related information.
High water mark	Rule that when information is combined from several targets, the result is assigned the highest classification level. [Warwick Ford –Computer Communications Security]
IT Resource	Any data, information object, operation, process, service, or system capability. An IT resource that is assigned a security label is sometimes referred to as a "security object". An IT resource that is represented as a requested security object of an initiator's access request is sometimes referred to as a "target".
	Data, service or system component. [XACML]
	The term resource embraces, e.g., information resources, processing resources, communication resources, and physical resources. [Ford]
	An object that is the target of security controls, including data, information, record, system file, service, or capability). [HL7 RBAC]
Metadata	Data about other data. [ISO 14721]
	Data describing context, content, and structure of records and their management through time. [ISO 15489-1]
	Structured information that describes, explains, locates, and otherwise makes it easier to retrieve and use an information resource. (NISO)
	Information that characterizes data, such as contextual information. [PCAST]
	Security labels are a type of security metadata that is associated with a security object/IT resource and considered a security attribute.
Named Tag Set	Field containing a Tag Set Name and its associated set of security tags. [NIST FIPS PUB 188]
Object	An object is an entity that contains or receives information. The objects can represent information containers (e.g., files or directories in an operating system, and/or columns, rows, tables, and views within a database management system) or objects can represent exhaustible system resources, such as printers, disk space, and central processing unit (CPU) cycles. [HL7 RBAC] Synonymous with IT resource.
Predicate	A statement about attributes whose truth can be evaluated. [XACML]

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
Privacy	The claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. [Westin] This definition is foundational for Privacy Act of 1974 (P.L. 93579; 5 U.S.C. § 552a).
	Freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual. [ISO/IEC 2382-8]
	The right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed. [ISO 7498-2]
	[T]he right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses." June 13, 2002, speech to the Freedom of Information and Protection of Privacy Conference Privacy Commissioner of Canada June 13, 2002]
	Individual's or organization's right to determine whether, when, and to whom, personal or organizational information is released. Also, the right of individuals to control or influence information that is related to them, in terms of who may collect or store it, and to whom that information may be disclosed. [HITSP Glossary]
Privacy Mark	Human readable security labels, which are rendered in the graphic user interface on accessed electronic information, are called "privacy marks." The act of enabling the rendering of a privacy mark is called "privacy marking".
	If present, the privacy-mark is not used for access control. The content of the privacy-mark may be defined by the security policy in force (identified by the security-policy-identifier) which may define a list of values to be used. Alternately, the value may be determined by the originator of the security-label. [ISO 22600-3 Section A.3.4.3]
Provenance	The history of the ownership of an object, especially when documented or authenticated. For example, references to a type of equipment, standard clinical procedure, attestable content author, data source, provider or other clinical facts. [PCAST]
	Information about entities, activities, and people involved in producing a piece of data or thing, which can be used to form assessments about its quality, reliability or trustworthiness. [W3C PROV-Overview]
	Provenance of a resource is a record that describes entities and processes involved in producing and delivering or otherwise influencing that resource. Provenance provides a critical foundation for assessing authenticity, enabling trust, and allowing reproducibility. Provenance assertions are a form of contextual metadata and can themselves become important records with their own provenance. [W3C Provenance XG Final Report]
	Data provenance is information that helps determine the derivation history of a data product, starting from its original sources. Data product or dataset refers to data in any form, such as files, tables, and virtual collections. […] Two important features of the provenance of a data product are the ancestral data products from which this data product evolved, and the process of transformation of these ancestral data product(s), potentially through workflows, that helped derive this data product. [Simmhan]

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
	The information that documents the history of the Content Information. This information tells the origin or source of the Content Information, any changes that may have taken place since it was originated, and who has had custody of it since it was originated. The archive is responsible for creating and preserving Provenance Information from the point of Ingest; however, earlier Provenance Information should be provided by the Producer. Provenance Information adds to the evidence to support Authenticity. [OAIS]
Security Attribute	A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes. NIST FIPS PUB 188
	Characteristic of a subject, resource, action or environment that may be referenced in a predicate or target. [XACML]
Security Classification	The determination of which specific degree of protection against access the data or information requires, together with a designation of that degree of protection. Examples: "Top secret", "secret", "confidential". ISO 2382-8/T-REC-X.812-199511-I!!PDF-E
Security Label *Synonymous with Target Label*	*Note to Readers: In the definitions below, "security label" is defined as both a verb: "means used to associate security attributes" as in "security labeling", and as noun: "the markings bound to a resource". As a noun, the term is sometimes considered synonymous with "security metadata" and "security tag." As a verb, the term is sometimes considered synonymous with "tagging". However, authoritative security standards sometimes use the term "security label" for both the classification given to IT resources and the classification level in an initiator's clearance. In addition, some authoritative standards use the term "marking bound to a resource" to refer to both computable security labels, and the human readable rendering of security label fields better known as "privacy markings".*
	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object [ISO 10181-3/ITU X.812]
	Access control information associated with the attribute values being accessed. [ISO/IEC 9594-2:2008/ITU X.501]
	The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. NOTE - The marking and/or binding may be explicit or implicit. [ISO 7498-2/CCITT Rec. X.800]
	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object. [NIST SP 800-53]
	Security labels may be used to associate security-relevant information with attributes within the Directory. Security labels may be assigned to an attribute value in line with the security policy in force for that attribute. The security policy may also define how security labels are to be used to enforce that security policy. A security label comprises a set of elements optionally including a security policy identifier, a security classification, a privacy mark, and a set of security categories. The security label is bound to the attribute value using a digital signature or other integrity mechanism. [ISO/IEC 9594-2:2008/ITU X.501]
	Sensitivity labels are security labels which support data confidentiality models, like the Bell and LaPadula model. The sensitivity label tells the amount of damage that will result from the disclosure of the data and also indicates which measures the data requires for protection from disclosure. The amount of damage that results from unauthorized disclosure depends on who obtains the data; the sensitivity label should reflect the worst case. [IETF RFC 1457]
	A security label, sometimes referred to as a confidentiality label, is a structured representation of the

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
	sensitivity of a piece of information. A security label is used in conjunction with a clearance, a structured representation of what information sensitivities a person (or other entity) is authorized to access and a security policy to control access to each piece of information. [XMPP Core]
	A security label is a type of PCAST Metadata Tag defined as "information that characterizes data, such as contextual information."
Security (Labeling) Policy	The definition of which classification and category values are used and how security labels are checked against clearances.
Security label rule	A computational algorithm used for assigning a security label to an IT resource such as a clinical fact.
Security Policy Information File (SPIF)	A construct that conveys domain-specific security policy information. [ISO/IEC 15816]
	An XML schema, that provides a high level representation of a security labeling policy in a generic and open fashion. [Open XML SPIF]
Security Tag *A type of Security Metadata*	Information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map). [NIST FIPS PUB 188]
Segmentation	The process of sequestering from capture, access or view certain data elements or "datatypes" (clinical information categories) that are perceived by a legal entity, institution, organization, or individual as being undesirable to share.
Sensitivity	The characteristic of a resource which implies its value or importance and may include its vulnerability. [ISO/IEC 7498-2:1989/CCITT Rec. X.800]
Sensitivity Label	Security labels which support data confidentiality models, like the Bell and LaPadula model. The sensitivity label tells the amount of damage that will result from the disclosure of the data and also indicates which measures the data requires for protection from disclosure. The amount of damage that results from unauthorized disclosure depends on who obtains the data; the sensitivity label should reflect the worst case. [IETF RFC 1457]
Tag Set Name	Numeric identifier associated with a set of security tags. [NIST FIPS PUB 188]
Target	A target is a resource subject to access control. [Ford]
	The set of decision requests, identified by definitions for resource, subject and action that a rule, policy or policy set is intended to evaluate. [XACML]
	A target is an IT resource for which an initiator seeks access.
Target Label *Synonymous with Security Label*	A security label can be used as target ACI to protect a target. Access rules define the access permissions (operations) granted given the security label of the initiator and the security label assigned to a target. If the security policy requires that the ACI held in the security label are used for target ACI, then overall flow of data in and out of that target can be controlled. Hence, the overall flow of data in and out of targets may be analyzed for security domains applying the same security policy. Targets can be created within other targets. The security label of the containing target limits the security labels that may be assigned to the contained target under the rules for the appropriate security policy. Examples of targets to

Term *Note that hyperlinked terms are either links back to text or to related terms.*	**Definitions and Descriptions** *Note that where no source is specified, the terms are defined in the context of HCS. Some entries are authoritative descriptions about the use of the term and may contain the term being defined in this glossary. These descriptions are not considered definitions.*
	which labels may be applied include: OSI n-entities; Directory Service entries; files held in a file store; database entries. [ISO/IEC 10181-3 p. 24]

Appendix B: HCS Business Requirements

The following table details the EHR Data Segmentation business requirements from the preceding Figure 4 Data Segmentation Functional Model, which can also be viewed by holding a pointer over the diagram boxes. In addition, this table includes implementer guidance and policy sources for these requirements.

Table 3 Appendix B: HCS Business Requirements

#	Name	Description
1.00	Data Segmentation Management and Services (Names on the Diagram)	Capability to use standard clinical attribute and security labels, conversion (such as redaction or de-identification), and encryption (such as masking) to segment clinical facts such as individually identifiable health information.
1.10	Clinical Fact Management	Capability to manage rules for assigning standard clinical attributes to structured and unstructured clinical elements that are required for assigning security labels, and for aggregating, disaggregating, persisting, and retrieving clinical facts for security label assignment.
1.1.1	Define and manage clinical attributes assigned to clinical elements	Provide the ability to manage rules for assigning standard clinical attributes to structured and unstructured clinical elements that are required for assigning security labels.
1.1.2	Manage rules for generating and storing clinical facts	Provide the ability to manage rules for aggregating, disaggregating, persisting, and retrieving clinical facts for security label assignment.
1.2.0	Clinical Fact Services	Capability to execute rules for assigning standard clinical attributes to structured and unstructured clinical elements stipulated by Clinical Fact Management.

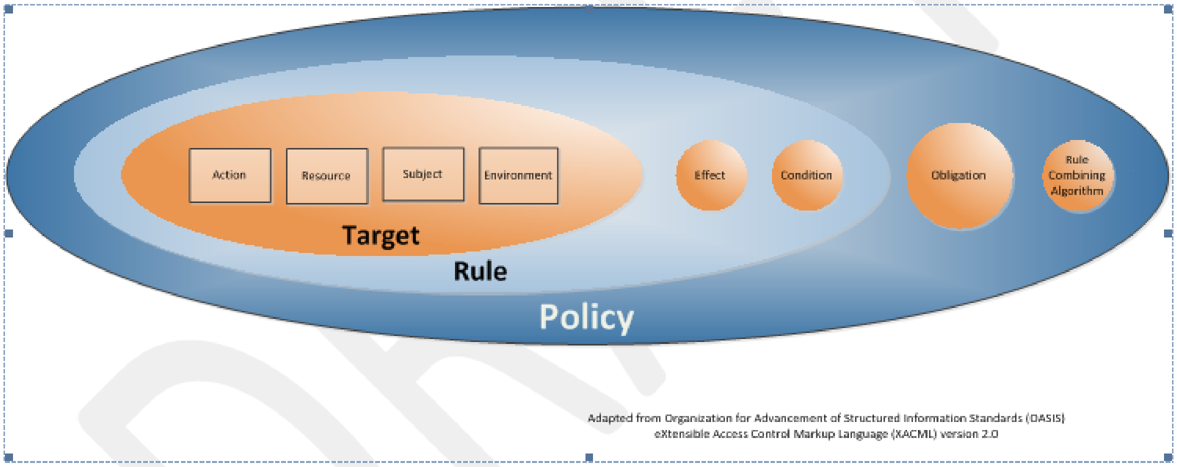
1.2.1	Assign standard clinical attributes to clinical elements	Provide the ability to assign applicable clinical attributes encoded with standard terminologies to standard structured and unstructured clinical elements as required for assigning security labels.
1.2.2	Generate and store clinical facts	Provide the ability to persist clinical elements with assigned standard clinical attributes as clinical facts that are required for security label assignment.
1.2.3	Retrieve Clinical Facts	Provide the ability to retrieve clinical facts as required for security label assignment.
1.3.0	Security Labels & Privacy Protection Management	Capability to manage rules for assigning security labels to clinical facts and providing privacy protections.
1.3.1	Manage privacy policies for clinical fact segmentation	Provide the ability to establish, translate, reconcile, and store privacy policies, including consent directives, as input to security labeling rules.
1.3.2	Manage rules for automatic assignment of security labels	Provide the ability to manage rules for automatic assignment of security labels to clinical facts.
1.3.3	Manage rules for manual assignment of security labels	Provide the ability to manage rules for a user to manually override a security label automatically assigned to a clinical fact, e.g., based on professional judgment, policy, or an approved patient request.
1.3.4	Managed privacy protective rules	Provide the ability to manage rules for automatic masking, redaction, and de-identification of clinical facts.
1.3.5	Manage handling caveats	Provide the ability to manage rules for automatic assignment of handling caveats in security labels assigned to clinical facts.
1.4.0	Security Labeling Services	Capability to execute rules for assigning security labels to clinical facts by applying security classification, sensitivity, integrity, category, and handling instructions markings to healthcare system output (data views, reports and messages) prior to access or disclosure.

1.4.1	Retrieve and automatically assign security labels to clinical facts	Provide the ability to retrieve a clinical fact for automatic assignment of a security label.
1.4.2	Enable security labeling of clinical facts at the time of entry	Provide the ability for a user to manually override a security label automatically assigned to a clinical fact based on professional judgment, policy, or an approved patient request.
1.4.3	Bind security labels to clinical facts	Provide the ability to bind security labels to clinical facts retrieved for automatic or manual labeling to ensure integrity.
1.4.4	Persist security labels associated with clinical facts	Provide the ability to persist security labels associated with clinical facts.
1.4.5	Update security label per policy changes	Provide the ability to update security labels based on changes in policy, such as the revocation of a consent directive.
1.4.6	Enable security label enforcement by access control services	Provide the ability to invoke access control services to enforce security labels.
1.5.0	Privacy Protective Services	Capability to enable and reverse privacy protective services such as redacting, masking, de-identifying, and applying privacy marks to clinical facts in accordance with transform rules. The service accepts obligations resulting from an access control decision and clinical facts as input to generate information response to a query.
1.5.1	Mask clinical fact	Provide the ability to mask and unmask clinical facts.
1.5.2	Redact clinical facts	Provide the ability to redact clinical facts and maintain a link to the original clinical fact.
1.5.3	De-identify clinical facts	Provide the ability to deidentify clinical facts using techniques such as shedding, anonymization, and pseudonymization, and to maintain a link to the original clinical fact per policy.

1.5.4	Reverse privacy protective mechanisms	Provide the ability to unmask a clinical fact with a "shared secret" key based upon user clearance or other trigger, e.g., emergency or other specific situation.
1.5.5	Display Privacy Mark	Provide the ability to render security label fields required by policy to be displayed to end users.

APPENDIX C: GENERAL SECURITY POLICY COMPONENTS

As illustrated in Figure 8 below security label field values equate to the access control information (ACI) defined as attributes used by an Access Control Service to match a user's rights (permissions) to perform certain actions on a particular resource to the attributes of an access control policy. The OASIS eXtensible Access Control Markup Language (XACML) provides a representational model and language for describing these relationships. The OASIS Cross-enterprise Security and Privacy Authorizations (XSPA) profile or XACML provides a health care specific approach to using attributes and clearances for the purpose of making access control decisions.



Adapted from Organization for Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) version 2.0

Figure 12 OASIS Policy Model

Legend

Action - An operation on a ***resource***

Attribute - Characteristic of a ***subject***, ***resource, action*** or ***environment*** that may be referenced in a ***predicate*** or ***target*** (see also – ***named attribute***)

Condition* -** An expression of ***predicates. A function that evaluates to "True", "False" or "Indeterminate"

Effect* -** The intended consequence of a satisfied ***rule (either "Permit" or "Deny")

Environment - The set of ***attributes*** that are relevant to an ***authorization decision*** and are independent of a particular ***subject, resource*** or ***action***

Named Attribute* –** A specific instance of an ***attribute, determined by the ***attribute*** name and type, the identity of the ***attribute*** holder (which may be of type:

subject, ***resource***, ***action*** or ***environment***) and (optionally) the identity of the issuing authority.

Obligation - An operation specified in a ***policy*** or ***policy set*** performed in conjunction with the enforcement of an ***authorization decision***

Predicate* -** A statement about ***attributes whose truth can be evaluated

Policy* -** A set of ***rules, an identifier for the ***rule-combining algorithm*** and (optionally) a set of ***obligations.*** May be a component of a ***policy set***

Rule* -** A ***target, an ***effect*** and a ***condition.*** A component of a ***policy***

Resource - Data, service or system component

Rule-combining algorithm* -** The procedure for combining ***decisions from multiple ***rules***

Subject* -** An actor whose ***attributes may be referenced by a ***predicate***

Target* -** The set of ***decision requests, identified by definitions for ***resource***, ***subject*** and ***action*** that a ***rule***, ***policy*** or ***policy set*** is intended to evaluate

APPENDIX D: COMPONENTS OF THE HEALTHCARE PRIVACY AND SECURITY CLASSIFICATION SYSTEM

A number of choices exist for describing HCS components. The section describes these and options in a general sense not intended as prescriptive, believing that the specific approach is best left to the domain in which it is deployed.

The basic features of the health care security label based system are described as:

- Clearances applied to initiators,
- Security (Label) Policy Information File defining which security labels are valid and how the check them against security clearances,
- HCS Security Labels applied to resources and data passed between systems.

Confidentiality Label

Figure D.1provides the basic class structure for resource security label information.

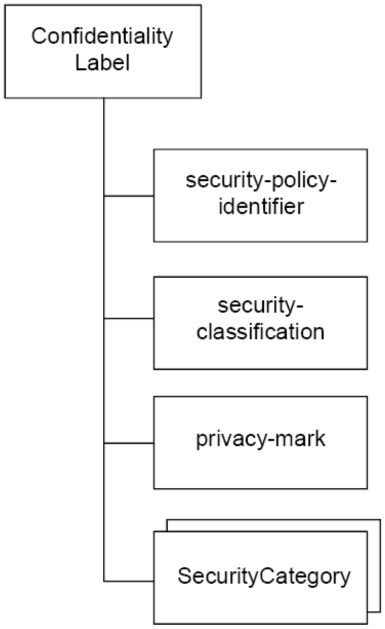


Figure D.1 Confidentiality Label Classes (ISO/IEC 15816/ITU-T X.841)

The following example shows encoding of a SPIF using the OpenXML approach:

```
<?xml version="1.0" encoding="UTF-8"?>
<ww:SecurityLabel xmlns:spif="http://www.xmlspif.org/spif"
 xmlns:ns2="urn:hl7-org:v3:datatypes-base"
 xmlns:ww="http://www.va.gov"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.va.gov file:/C:/Users/Duane%20DeCouteau/Downloads/xmlspifsecuritylabel.xsd">
    <ww:labelName>Confidentiality</ww:labelName>
    <spif:securityPolicyId name="42CFRPart2" id="2.3.4.5.6.7"/>
    <spif:securityClassification name="RESTRICTED" lacv="5" hierarchy="5"/>
    <ww:labelValue>R</ww:labelValue>
    <spif:privacyMarks>
      <spif:privacyMark name="Confidentiality">
        <spif:markingData phrase="RESTRICTED">
          <spif:code>noNameDisplay</spif:code>
        </spif:markingData>
        <spif:markingQualifier markingCode="pageTop">
          <spif:qualifier markingQualifier="Confidentiality" qualifierCode="prefix"/>
          <spif:qualifier markingQualifier=" " qualifierCode="separator"/>
        </spif:markingQualifier>
      </spif:privacyMark>
    </spif:privacyMarks>
  </ww:SecurityLabel>
```

The applicable ASN.1 syntax for a confidentiality label can be found at ITU-T X.841 page 4

```
   id-ConfidentialityLabel OBJECT IDENTIFIER ::= {
   joint-iso-itu-t sios(24) specification(0) securityLabels(1) confidentiality(0)}
   ConfidentialityLabel ::= SET {
   security-policy-identifier SecurityPolicyIdentifier OPTIONAL,
   security-classification INTEGER(0..MAX) OPTIONAL,
   privacy-mark PrivacyMark OPTIONAL,
   security-categories SecurityCategories OPTIONAL }
   (ALL EXCEPT({-- none; at least one component shall be present --}))
   SecurityPolicyIdentifier ::= OBJECT IDENTIFIER
   PrivacyMark ::= CHOICE {
   pString PrintableString (SIZE(1..ub-privacy-mark-length)),
   utf8String UTF8String (SIZE(1..ub-privacy-mark-length))
   }
   ub-privacy-mark-length INTEGER ::= 128 -- as defined in ITU-T Rec. X.411 | ISO/IEC 10021-4
   SecurityCategories ::= SET SIZE (1..MAX) OF SecurityCategory
   SecurityCategory ::= SEQUENCE {
   type [0] SECURITY-CATEGORY.&id ({SecurityCategoriesTable}),
   value [1] SECURITY-CATEGORY.&Type ({SecurityCategoriesTable} {@type})
   }
   SECURITY-CATEGORY ::= TYPE-IDENTIFIER
  SecurityCategoriesTable SECURITY-CATEGORY ::= {…}
```

Methods for Binding Security Labels to IT Resources

Although the HCS considers binding assurance of a security label to an IT Resource as a mandatory precondition of conformance with the HCS specified security label structure and semantics, the HCS is agnostic to mechanism by which a security label is bound to an IT Resource. There are multiple means for binding that depend on the binding target type to which the label is assigned and the context in which these are accessed and used (e.g., internal database or external federated environment), which result in different levels of binding assurance.

ISO/IEC 15816/ITU-T X.841 Section 6.1.3 describes three such methods:

- Storing representations of protected information with the security label as a record within a secure environment where overall system access control ensures the label binding integrity.

- Use of a digital signature or encrypting with a message authentication code to bind protected information with the label such that the label and digital signature can be stored outside of a secure system

Clearance

Figure D.2 provides the basic class structure for initiators clearance information.

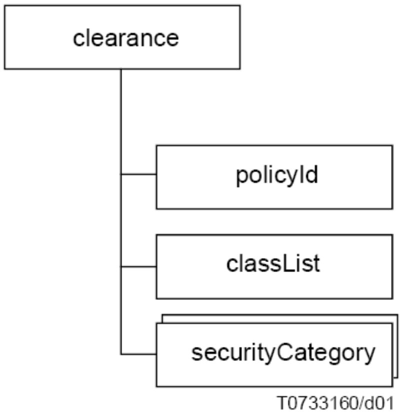


Figure D.2 Security Clearance Classes (ISO/IEC 15816/ITU-T X.841)

The **policyId** OID identifies which optional components must be present. The **classList** component defines the user's granted and hierarchical clearances as indicated by **ClassList**, which is defined by ITU-T Rec. X.501 | ISO/IEC 9594-2.
The **securityCategory** component identifies any number of restrictive and permissive bit mapped security categories as well as restrictive and permissive enumerated security categories assigned to the user. (ISO/IEC 15816:2001 (E). This structure is illustrated in Figure 1.

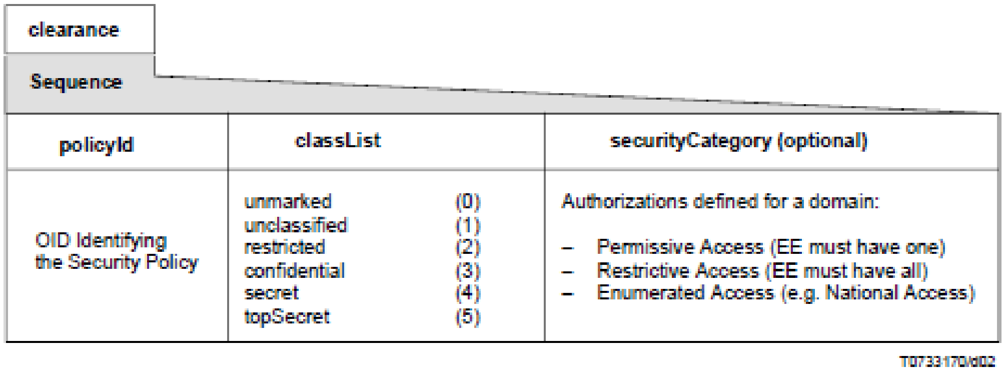
The following example illustrates clearance encoding using the OpenXML approach:

```
<?xml version="1.0" encoding="UTF-8"?>
<ww:Clearance xmlns:spif="http://www.xmlspif.org/spif" xmlns:ns2="urn:hl7-org:v3:datatypes-base"
   xmlns:ww="http://www.va.gov" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.va.gov
file:/C:/Users/Duane%20DeCouteau/Downloads/xmlspifsecuritylabel.xsd">
   <spif:securityPolicyId name="42CFRPart2" id="2.3.4.5.6.7"/>
   <classList>
      <ww:className>UNRESTRICTED</ww:className>
      <ww:className>NORMAL</ww:className>
      <ww:className>LOW</ww:className>
      <ww:className>MODERATE</ww:className>
      <ww:className>RESTRICTED</ww:className>
      <ww:className>VERY RESTRICTED</ww:className>
   </classList>
   <ww:securityCategory id="1.2.3.4.5">
```

```
      <ww:Privileges>
        <!-- Allowed Purpose Of Use Treatment -->
        <ww:namedTagSetPrivilege id="2.3.4.5.6.8">
          <ww:securityTagPrivilege tagType="enumerated">
            <ww:attributeFlags>TREAT</ww:attributeFlags>
          </ww:securityTagPrivilege>
        </ww:namedTagSetPrivilege>
        <!-- member of Pharmacy Team -->
        <ww:namedTagSetPrivilege id="2.3.4.5.6.9">
          <ww:securityTagPrivilege tagType="enumerated">
            <ww:attributeFlags>Pharmacy</ww:attributeFlags>
          </ww:securityTagPrivilege>
        </ww:namedTagSetPrivilege>
        <!-- Access to Mental Health and Substance Abuse Information -->
        <ww:namedTagSetPrivilege id="2.3.4.5.6.10">
          <ww:securityTagPrivilege tagType="enumerated">
            <ww:attributeFlags>ETH</ww:attributeFlags>
            <ww:attributeFlags>PSY</ww:attributeFlags>
          </ww:securityTagPrivilege>
        </ww:namedTagSetPrivilege>
        <!-- Workflow requires access to only highly reliable information -->
        <ww:namedTagSetPrivilege id="2.3.4.5.6.11">
          <ww:securityTagPrivilege tagType="enumerated">
            <ww:attributeFlags>HRELIABLE</ww:attributeFlags>
          </ww:securityTagPrivilege>
        </ww:namedTagSetPrivilege>
      </ww:Privileges>
  </ww:securityCategory>
</ww:Clearance>
```

The applicable ASN.1 syntax reference for security clearance classes and clearance diagram can be found at ISO/IEC 15816/ITU-T X.841.

```
clearance ATTRIBUTE ::= { WITH SYNTAX Clearance
ID id-at-clearance }
id-at-clearance OBJECT IDENTIFIER ::= {
joint-iso-itu-t (2) ds (5) attributeType (4) clearance (55) }
Clearance ::= SEQUENCE {
policyId OBJECT IDENTIFIER,
classList ClassList DEFAULT {unclassified},
securityCategories SecurityCategories OPTIONAL}
ClassList ::= BIT STRING {
unmarked (0),
unclassified (1),
restricted (2),
confidential (3),
secret (4),
topSecret (5) }
SecurityCategories ::= SET SIZE(1..MAX) OF SecurityCategory
```



clearance

Sequence

policyId	classList	securityCategory (optional)
OID Identifying the Security Policy	unmarked (0) unclassified (1) restricted (2) confidential (3) secret (4) topSecret (5)	Authorizations defined for a domain: – Permissive Access (EE must have one) – Restrictive Access (EE must have all) – Enumerated Access (e.g. National Access)

Figure 2 – Clearance Attribute Fields

Section 6.3.1 of ISO/IEC 15816/ITU-T X.841 explains how an initiator's clearance is matched with security labels on requested IT Resources. These rules apply to the HCS as well. The policyID on the clearance and the security label must match. The classification field must be populated with a confidentiality code at a level that meets or exceeds the confidentiality code in the security label. Security categories on the clearance have the following rules:

- Security Category components of HCS Security Labels are designated as either restrictive or permissive tags according to whether a clearance must meet all the category tags in a clinical fact label (restrictive) or whether a clearance must only meet one category tags in order to gain access.

Restrictive Tag	Specifies a hierarchical security parameter used to restrict access to a clinical fact such that only a clinical fact with a restrictive tag equal to or less restrictive than the corresponding tag in the user's clearance may be accessed or disclosed. Restrictions may be extended to not accepting clinical facts with labels lower than the lowest level for the receiving end, and so on. Examples include confidentiality and integrity reliability classification.
Permissive Tag	Specifies a non-hierarchical security parameter (aka "release marking") used to permit access to a clinical fact such that only a clinical fact with at least one permissive tag equal to the corresponding tag in the user's clearance may be accessed or disclosed. Examples include purpose of use and compartment where the user's clearance for one of the clinical fact purpose of use or compartment is sufficient to permit access or disclosure.
Tag type adjudication	Rule: Restrictive tag fields are adjudicated first. If the end user's clearance matches or exceeds all of the restrictive tags in a label, then the permissive tags are processed.

Security Policy Information File

A security policy is the basis for the decisions made by the access control mechanisms. Domain-specific security policy information is conveyed via the Security Policy Information File (ISO/IEC 15816/ITU-T X.841)
Aspects of security policy as stated in ISO/IEC 15816 include the following and may be extended as required by context:

- The level of protection to be given to data stored on a system;
- Who is authorized to access data, processes or resources;
- Security markings required to be shown on any display or print of the material;
- Routing and enciphering requirements for data transmitted between systems;
- Requirements for protection against unauthorized copying and re-disclosure;
- Methods for storage of data;
- Enciphering algorithms to be used;
- Methods of authenticating entities;
- Whether operations on the object are to be audited;
- Whether preventing repudiation of receipt of an object by recipients is required;
- Whether, and whose, digital signatures are required to authenticate the data.

The HL7 HCS allows for the selection of a variety of security policy information file (SPIF) formats. Selection of a format is left to the discretion of security domain authorities. There are several non-compatible formats in general use including:

U.S. Department of Defense Specification SDN.801c

- ISO/IEC 15816/ITU-T X.841 Information technology – Security techniques – Security information objects for access control
- Open XML XMLSPIF Version 2

A security policy in its simplest form is a set of criteria for the provision of security services. With regard to access control, security policy is a subset of a higher system-level security policy that defines the means for enforcing access control policies between initiators and targets. The access control mechanisms must:

Allow communication where a specific policy permits; and

- Deny communication where a specific policy does not explicitly permit.

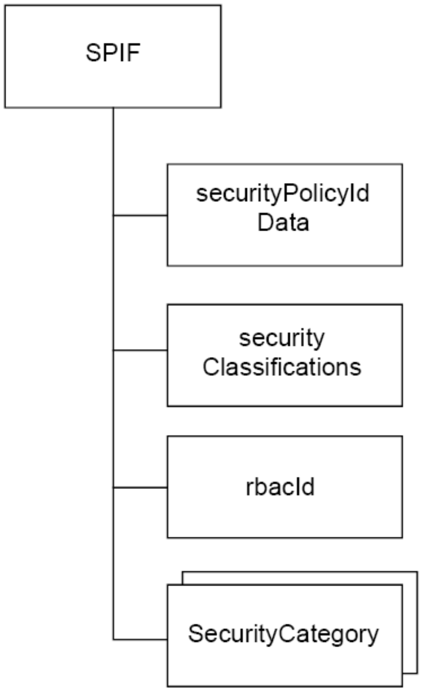


Figure D.3 Security Policy Information File (SPIF) (ISO/IEC 15816/ITU-T X.841)

The following example shows encoding of a SPIF using the OpenXML approach:

```
<?xml version="1.0" encoding="UTF-8"?>
<SPIF xmlns="http://www.xmlspif.org/spif"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://www.xmlspif.org/spif
file:/C:/Users/Duane%20DeCouteau/Downloads/xmlspif.xsd"
 schemaVersion="2.0"
 creationDate="201303182307010800"
 originatorDN="CN=sadmin, OU=VHA, O=Dept. of Veterans Affairs, C=U.S.A"
 keyIdentifier="ABCDEF==="
 privilegeId="1.2.3.4.5.1"
 rbacId="1.2.3.4.5">
    <securityPolicyId name="42CFRPart2" id="2.3.4.5.6.7"/>
    <securityClassifications>
        <securityClassification name="UNRESTRICTED" lacv="1" hierarchy="1"/>
        <securityClassification name="NORMAL" lacv="2" hierarchy="2"/>
        <securityClassification name="LOW" lacv="3" hierarchy="3"/>
        <securityClassification name="MODERATE" lacv="4" hierarchy="4"/>
        <securityClassification name="RESTRICTED" lacv="5" hierarchy="5"/>
        <securityClassification name="VERY RESTRICTED" lacv="6" hierarchy="6"/>
    </securityClassifications>
    <!-- NOTE:  SecurityCategory equiv in XML SPIF v2.0 schema follows -->
    <securityCategoryTagSets>
        <securityCategoryTagSet name="Release Reason" id="2.3.4.5.6.8">
            <securityCategoryTag name="Purpose of Use" tagType="enumerated" enumType="permissive"
singleSelection="true">
                <tagCategory name="TREAT" lacv="0">
```

```
          <markingData phrase="TREATMENT">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="ETREAT" lacv="1">
          <markingData phrase="EMERGENCY TREATMENT">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="HOPERAT" lacv="2">
          <markingData phrase="OPERATIONS">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="HPAYMT" lacv="3">
          <markingData phrase="PAYMENT">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="HRESCH" lacv="4">
          <markingData phrase="RESEARCH">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="PATRQT" lacv="5">
          <markingData phrase="PATIENT REQUEST">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="COVERAGE" lacv="6">
          <markingData phrase="INSURANCE COVERAGE">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <tagCategory name="PUBHLTH" lacv="7">
          <markingData phrase="PUBLIC HEALTH">
            <code>noNameDisplay</code>
          </markingData>
        </tagCategory>
        <markingQualifier markingCode="pageBottom">
          <qualifier markingQualifier="Document has been released for Purposes of"
qualifierCode="prefix"/>
          <qualifier markingQualifier=" " qualifierCode="separator"/>
        </markingQualifier>
      </securityCategoryTag>
    </securityCategoryTagSet>
    <securityCategoryTagSet name="Groups Allowed Access" id="2.3.4.5.6.9">
      <securityCategoryTag tagType="enumerated" enumType="permissive" singleSelection="true"
name="Compartment">
        <tagCategory name="Care Team" lacv="0"></tagCategory>
        <tagCategory name="Laboratory" lacv="1"></tagCategory>
        <tagCategory name="Pharmacy" lacv="2"></tagCategory>
        <!-- and other compartments -->
      </securityCategoryTag>
    </securityCategoryTagSet>
    <securityCategoryTagSet name="Applicable Sensitivity Groups" id="2.3.4.5.6.10">
      <securityCategoryTag tagType="enumerated" enumType="restrictive" singleSelection="false"
name="Sensitivity">
        <tagCategory name="ETH" lacv="0"></tagCategory>
        <tagCategory name="PSY" lacv="1"></tagCategory>
        <!-- and other sensitivity codes if applicable -->
      </securityCategoryTag>
    </securityCategoryTagSet>
    <securityCategoryTagSet name="Data Integrity" id="2.3.4.5.6.11">
      <securityCategoryTag singleSelection="true" tagType="enumerated" enumType="permissive"
name="Integrity" >
        <tagCategory name="LRELIABLE" lacv="0"></tagCategory>
        <tagCategory name="MRELIABLE" lacv="1"></tagCategory>
        <tagCategory name="HRELIABLE" lacv="2"></tagCategory>
        <!-- and other integrity values -->
      </securityCategoryTag>
    </securityCategoryTagSet>
  </securityCategoryTagSets>
  <!-- end Security Category -->
  <privacyMarks>
    <privacyMark name="42CFRPart2">
      <markingData phrase="Recipient must comply with 42CFRPart2 provisions (42CFRPart2)">
        <code>noNameDisplay</code>
      </markingData>
      <markingQualifier markingCode="pageBottom">
        <qualifier markingQualifier=" " qualifierCode="separator"/>
      </markingQualifier>
    </privacyMark>
    <privacyMark name="NORDSLCD">
      <markingData phrase="No redislosure without patients consent (NORDSLCD)">
        <code>noNameDisplay</code>
      </markingData>
      <markingQualifier markingCode="pageBottom">
        <qualifier markingQualifier=" " qualifierCode="separator"/>
      </markingQualifier>
    </privacyMark>
    <privacyMark name="ENCRYPT">
      <markingData phrase="Requires encryption during transmission and at rest (ENCRYPT)">
        <code>noNameDisplay</code>
      </markingData>
    </privacyMark>
  </privacyMarks>
</SPIF>
```

The applicable Security Policy Information File defined by ASN.1 syntax can be found at ISO/IEC 15816/ITU-T X.841.

```
        SecurityPolicyInformationFile ::= SIGNED {EncodedSPIF}
        EncodedSPIF ::= TYPE-IDENTIFIER.&Type( SPIF )
```

```
SPIF ::= SEQUENCE {
versionInformation VersionInformationData DEFAULT v1,
updateInformation UpdateInformationData,
securityPolicyIdData ObjectIdData,
privilegeId OBJECT IDENTIFIER,
rbacId OBJECT IDENTIFIER,
securityClassifications [0] SEQUENCE OF SecurityClassification OPTIONAL,
securityCategories [1] SEQUENCE OF SecurityCategory OPTIONAL,
equivalentPolicies [2] SEQUENCE OF EquivalentPolicy OPTIONAL,
defaultSecurityPolicyIdData [3] ObjectIdData OPTIONAL,
extensions [4] Extensions OPTIONAL }
```

Assigning HCS Security Labels to Clinical Facts and Clearances

A clinical fact is classified by assigning a security label in accordance with a security policy information file (SPIF), which specifies label components. The clinical fact security label (*security label*) is comprised of the security label fields, tag sets, and tags using the syntax and semantics specified by an identifiable SPIF.

An initiator's clearance (*clearance)* must be conveyed with a similarly structured security label comprised of the security label fields, tag sets, and tags using the syntax and semantics specified by the clinical fact SPIF or mappable to that SPIF.

The HCS specifies the security label field, tag sets, and tags types required for a healthcare security label and the vocabulary required for semantic interoperability. The syntax used for the SPIF and the labels are out of scope at this juncture, although several approaches to documenting the label components and vocabulary are recommended including Open XML SPIF and NISTIR Computer Security Object Registry request form. An example of a SPIF for CDA encoded with Open XML is provided above. The HCS Guide included in this ballot package also describes the use of security label in CDA.

Binding of Security Fact to Clinical Fact

A clinical fact classification is a security label that is specific to the security policy in force in the context in which it is assigned. A clinical fact has only one label in that context.

For example, the security label assigned to a clinical fact by Organization X in Jurisdiction A in accordance with Security Policy 1 will likely be different than the security label assigned to the same clinical fact by Organization Y in Jurisdiction B in accordance to security policy 2.

If Organization X wants Organization Y to comply with Security Policy 1, then Organization X must negotiate with Organization Y to uphold Security Policy 1. Using Security Policy 1 security labels along with sharing the Security Policy Information File (SPIF), which specifies the semantics of Security Policy 1 security labels, Organization X is able to communicate this requirement to Organization Y.

If Organization Y agrees by asserting the access control information required by Security Policy 1 in its clearance, then the same clinical fact, when received by Organization Y from Organization X will have a different security label than the label assigned by Organization Y under its own Security Policy.

Level of Granularity

Assigning security labels to clinical facts in accordance with the governing security policy necessitates considering the degree of granularity at which information requiring protection is conveyed and the level of protection required, i.e., the classification level. In addition, two or more clinical facts may be aggregated, and may thereby conveying information with more semantic context and therefore, requiring a higher level of protection.

Determining the level of granularity at which a clinical fact should be assigned a security label is comparable to the concept of “portions” in intelligence community. A portion, in accordance with is classified by determining the risk of harm resulting from unauthorized disclosure (ISO/IEC 7498-2:1989/CCITT Rec. X.800).   This implies that the information must have enough contextual detail to be understood as a whole on its own, and may take on a different meaning when combined with other portions. For example, two unclassified portions may become confidential when combined because together they contribute additional information that increases the potential for unauthorized disclosure to result in harm. When portions classified at different levels are aggregated, the resulting portion is classified with the overall most restrictive label tags or “high water mark”. DoD Guide to Marking Classified Documents

APPENDIX E: PRIVACY CAPABILITIES (DATA MASKING AND DE-IDENTIFICATION)

Masking is additional encryption that permits run-time ability to provide authorized users full access to the clinical fact for "Break the Glass" during and emergency and Clinical Decision Support Systems to determine appropriate protocols and Drug-Drug Interaction for patient safety without unnecessarily providing access to clinicians.

Data De-identification: Unlike Masking, Data De-identification requires a transform of the clinical fact content that does not easily reversed at run-time. De-identified clinical facts would less likely need to be additionally encrypted.

Data Masking: Encrypts segments of protected health information so that they are inaccessible without access to decryption keys.

Anonymization:. Removes the association between protected health information and personal identification to ensure that there is no reasonable basis to believe that the remaining information can be used to identify an individual.

Data Aggregation: Restricts the aggregation of personal health information to that permitted by law.

Data Minimalism: Ensures that the use or disclosure of protected health information is limited to the minimum necessary to accomplish the intended purpose of the use or disclosure.

Data Shredding: Disaggregates protected health information segments so that they cannot be re-aggregated without authorization.

Media Sanitization/Redaction: Removes information from media such that data recovery is not possible. This component also ensures that no one deletes clinical information until the appropriate time has expired.

APPENDIX F: PROVENANCE RELATIONS DEFINED BY W3C

- **wasAttributedTo**: Attribution is the ascribing of an entity to an agent.
- **wasDerivedFrom**: A derivation is a transformation of an entity into another, a construction of an entity into another or an update of an entity, resulting in a new one.
- **wasGeneratedBy**: Generation is the completion of production of a new entity by an activity. This entity did not exist before generation and becomes available for usage after this generation.
- **wasInformedBy**: Communication is the exchange of an entity by two activities, one activity using the entity generated by the other.
- **wasInfluencedBy**: Influence is the capacity of an entity, activity, or agent to have an effect on the character, development, or behavior of another by means of usage, start, end, generation, invalidation, communication, derivation, attribution, association, or delegation.
- **hadPrimarySource**: A primary source for a topic refers to something produced by some agent with direct experience and knowledge about the topic, at the time of the topic's study, without benefit from hindsight. Because of the directness of primary sources, they 'speak for themselves' in ways that cannot be captured through the filter of secondary sources. As such, it is important for secondary sources to reference those primary sources from which they were derived, so that their reliability can be investigated. A primary source relation is a particular case of derivation of secondary materials from their primary sources. It is recognized that the determination of primary sources can be up to interpretation, and should be done according to conventions accepted within the application's domain.
- **wasInvalidatedBy**: Invalidation is the start of the destruction, cessation, or expiry of an existing entity by an activity. The entity is no longer available for use (or further invalidation) after invalidation. Any generation or usage of an entity precedes its invalidation.
- **wasQuotedFrom**: quotation is the repeat of (some or all of) an entity, such as text or image, by someone who may or may not be its original author. Quotation is a particular case of derivation.

- **wasRevisionOf**: A revision is a derivation for which the resulting entity is a revised version of some original. The implication here is that the resulting entity contains substantial content from the original. Revision is a particular case of derivation.

APPENDIX G: HCS PRIVACY AND SECURITY ARCHITECTURE

A typical Privacy and Security Architecture (such as diagrammed in Figure F1 below) includes capabilities and services required to implement a HCS. The relevant services are listed below.

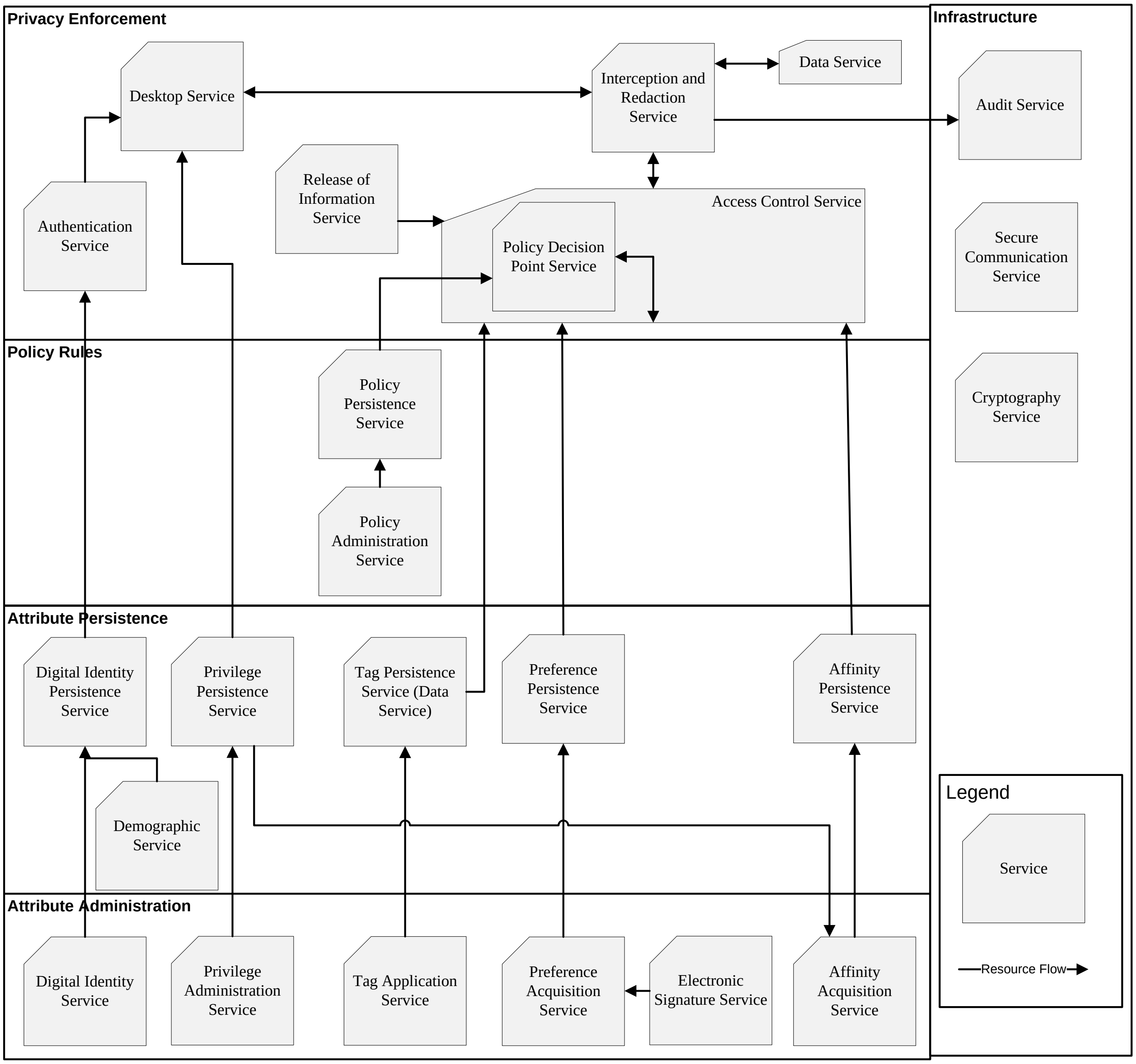

Privacy Enforcement
Desktop Service
Interception and Redaction Service
Data Service
Infrastructure
Audit Service
Release of Information Service
Authentication Service
Access Control Service
Policy Decision Point Service
Secure Communication Service
Cryptography Service
Policy Rules
Policy Persistence Service
Policy Administration Service
Attribute Persistence
Digital Identity Persistence Service
Privilege Persistence Service
Tag Persistence Service (Data Service)
Preference Persistence Service
Affinity Persistence Service
Demographic Service
Legend
Service
Resource Flow
Attribute Administration
Digital Identity Service
Privilege Administration Service
Tag Application Service
Preference Acquisition Service
Electronic Signature Service
Affinity Acquisition Service

Figure F1: General Security and Privacy Model

Services

A mechanism to enable access to a set of one or more capabilities , where the access is provided using a prescribed interface and is exercised consistent with constraints and policies as specified by the service description. The mechanism is a Performer. The "capabilities" accessed are Resources -- Information, Data, Materiel, Performers, and Geopolitical Extents.

Service - Access Control Service

The Access Control Service includes the Policy Decision Point and a consumer requests authorization for an action. The service provides a Yes/No decision or a Yes with Obligation return

Service - Data Service

This is a proxy service for any supplying data service.

Service - Demographic Service

The Demographic Service provides access to Record Subject Traits and is used for matching records and validating identities used for access to records.

Service - Desktop Service

The Desktop service provides the user interface for the user. It allows the user access after calling the authentication service. The Desktop Service is responsible for allocating the appropriate assertions to requests made to the Data Services via the Interception and Redaction Service. Specifically the desktop must validate authorized roles and purpose of use to be used in a session.

Service - Interception and Redaction Service

The Interception and Redaction Service intercepts requests made by a consumer to a data service and requests authorization from the Access Control Service to continue. If the response is Yes with Obligations then the service redacts information in accordance with the obligation.

Service - Policy Administration Service

The Policy Administration Service provides user editing capability to Policies and stores them in the Policy Persistence Service.

Service - Policy Decision Point Service

The Policy Decision Point Service is part of the Access Control Service and makes an authorization decision based on provided policies, assertions and attributes.

Service - Policy Persistence Service

The Policy Persistence Service stores the policies in executable format and enables the Policy Decision Point Service to access them when needed.

Service - Preference Acquisition Service

The Preference Acquisition Service provides the User interface for setting preferences and it passes these to the Preference Persistence Service.

Service - Preference Persistence Service

The Preference Persistence Service stores preferences and supplies them to the Access Control Service when needed.

Service - Privilege Administration Service

The Privilege Administration Service provisions identified users with credentials which may include roles, allowed purposes of use and access to specific applications.

Service - Privilege Persistence Service

The Privilege Persistence Service retains credentials associated with an identified user and can include Role, Organization, Affinity. The service may store these credentials by assigning the user to be a member of a functional group.

APPENDIX H: HOW HCS PRIVACY AND SECURITY SERVICES APPLY AND USE SECURITY LABELS

Clinical facts are consumed by the Security Labeling Service, which invokes security attribute values from the Access Control Service Policy Information Point (PIP). The Security Labeling Service also invokes the governing privacy policies and patient consent directive from the Policy Administration Point (PAP) to control enterprise user access and to construct a CCDA (such as a CCD or C32) for disclosure, which either redacts, masks, or tags a clinical fact (at the CDA header, section, and entry level) with security labels that tell the receiver how to comply with policies that govern the disclosure.

Figure G1 Rhode Island Security, Privacy and Governance below shows a generic model of this service collaboration. Security label fields are "decision factors" that are retrieved by the PIP in response to the PDP request for decision information. The PDP compares the security label field values for e.g., confidentiality levels required for user clearance to access a requested clinical fact based on the policy inputs.

Figure G2 shows an instance of the HCS Services model implemented by the Rhode Island Health Information Exchange.

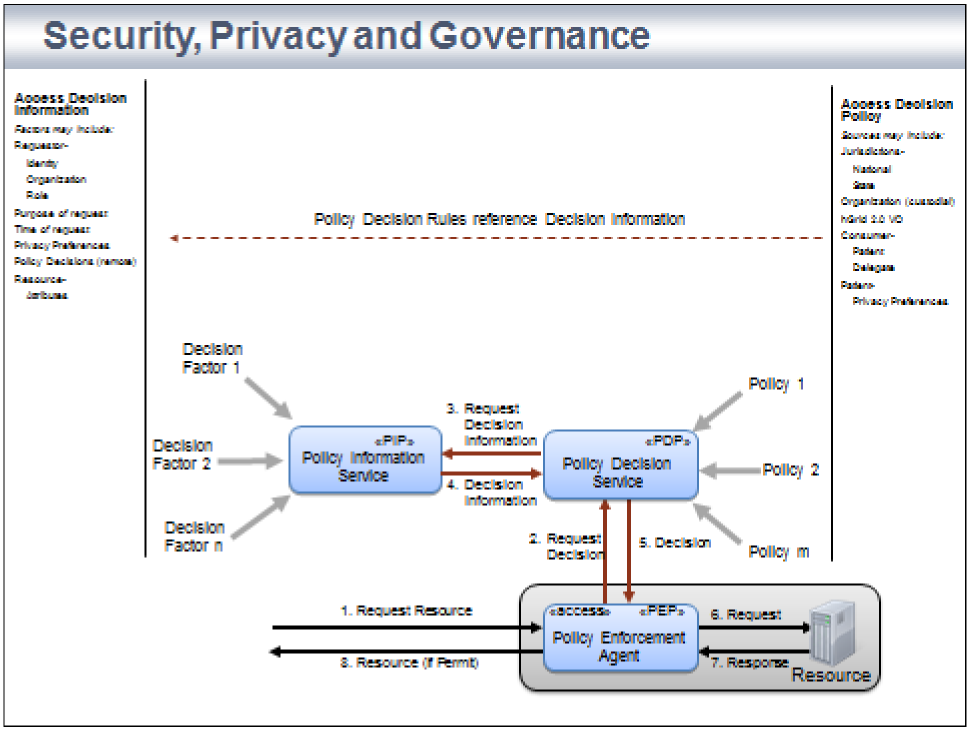


Figure G1: Rhode Island Security, Privacy and Governance

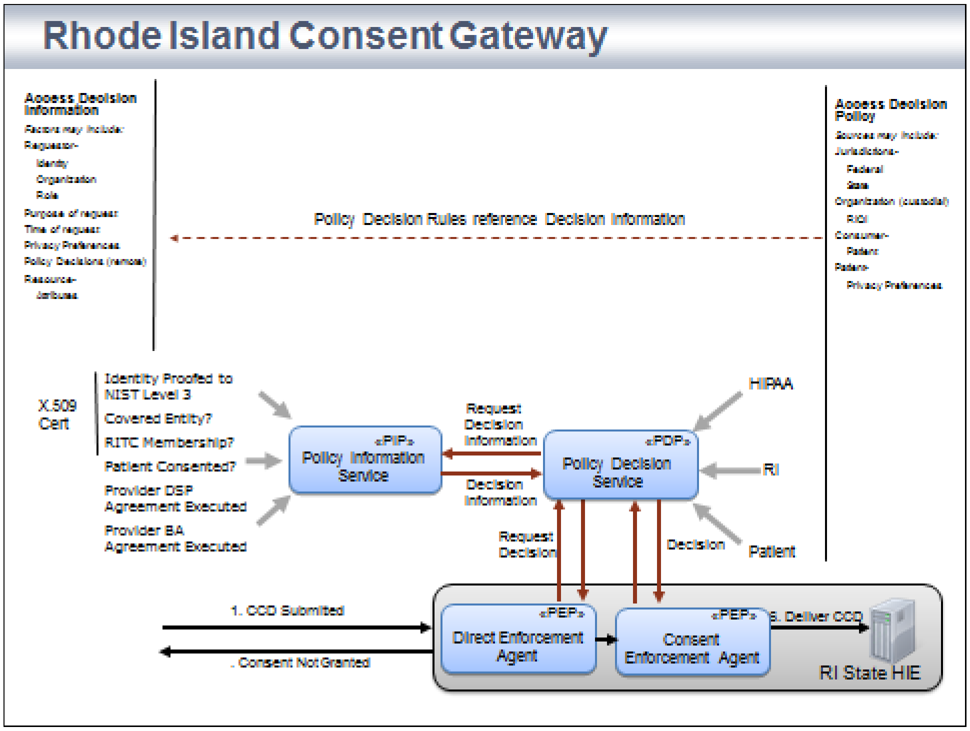


Figure G2: Rhode Island HIE HCS Service Model

APPENDIX I: EXAMPLE DATA SEGMENTATION PROCESS

In response to a request for patient information or in creating a document for submission to a searchable repository, the sender's system evaluates the provenance of each clinical fact relevant to the outbound document or message payload against privacy policies and patient consent directive criteria to determine the security labels to be assigned. The U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC), Data Segmentation for Privacy initiative modeled the system requirements for applying security labels to clinical facts prior to disclosure based on privacy policies and patient consent directives.

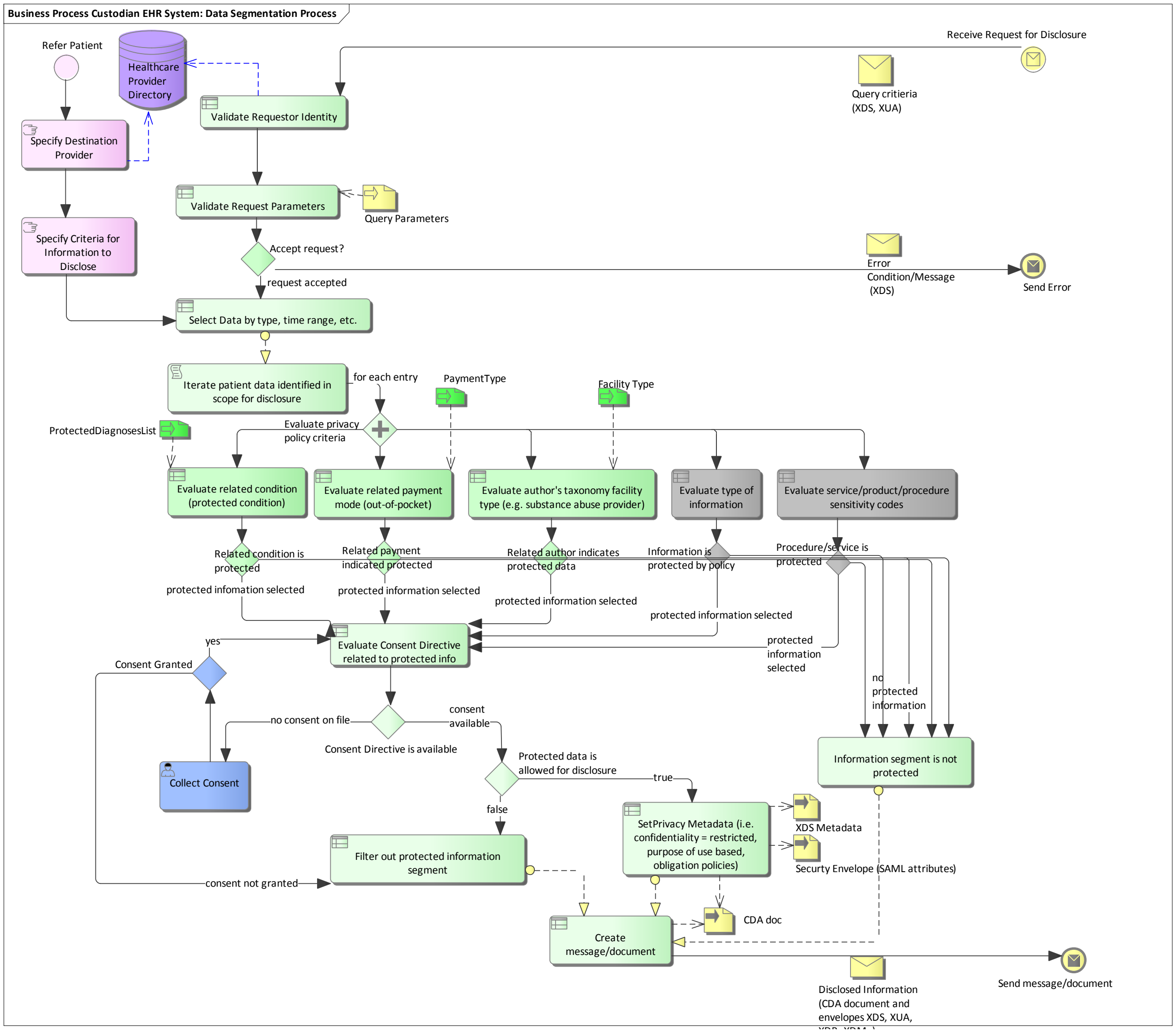

Business Process Custodian EHR System: Data Segmentation Process
Refer Patient
Healthcare Provider Directory
Specify Destination Provider
Specify Criteria for Information to Disclose
Validate Requestor Identity
Receive Request for Disclosure
Query critieria (XDS, XUA)
Validate Request Parameters
Query Parameters
Accept request?
Error Condition/Message (XDS)
Send Error
request accepted
Select Data by type, time range, etc.
Iterate patient data identified in scope for disclosure
for each entry
PaymentType
Facility Type
ProtectedDiagnosesList
Evaluate privacy policy criteria
Evaluate related condition (protected condition)
Evaluate related payment mode (out-of-pocket)
Evaluate author's taxonomy facility type (e.g. substance abuse provider)
Evaluate type of information
Evaluate service/product/procedure sensitivity codes
Related condition is protected
Related payment indicated protected
Related author indicates protected data
Information is protected by policy
Procedure/service is protected
protected infomation selected
protected information selected
protected information selected
protected information selected
protected information selected
no protected information
yes
Consent Granted
Evaluate Consent Directive related to protected info
no consent on file
consent available
Consent Directive is available
Collect Consent
Protected data is allowed for disclosure
true
false
Information segment is not protected
SetPrivacy Metadata (i.e. confidentiality = restricted, purpose of use based, obligation policies)
XDS Metadata
Securty Envelope (SAML attributes)
Filter out protected information segment
consent not granted
CDA doc
Create message/document
Disclosed Information (CDA document and envelopes XDS, XUA,
Send message/document

Figure I.1: Data Segmentation Process -

Figure H1 Data Segmentation Process illustrates the retrieval and evaluation of clinical fact provenance to determine the security labels required by policy. This includes functions to retrieve provenance metadata for required for tagging each clinical fact with security labels (standard attributes) such as:

- Sensitive conditions that are the indication for orders or reason for an encounter, e.g., Sickle Cell Anemia,
- Authoring or performing provider's specialty and role in patient care, e.g., HIV specialist,
- Identifying service delivery location and healthcare facility type, e.g., behavioral health clinic,
- Calling out health policy or program coverage or payment type. e.g., 42 CFR Part 2 or Veteran's Health Benefits programs, and HITECH provisions for self-pay under HIPAA covered health plans ,
- Specifying clinical information category (substance abuse treatment protocol) and type of clinical report (e.g., behavioral health assessment) associated with the clinical fact,
- Tagging each clinical fact being aggregated for the disclosure with security labels by evaluating privacy policies and patient consent directive criteria that match the clinical fact provenance metadata,
- Redacting clinical facts that are not permitted to be disclosed,
- Applying applicable handling caveats to aggregated clinical facts that will be disclosed such as purpose of use, obligations, and refrain policies as well privacy marks that must be displayed to end users (see Privacy Capabilities below),
- Masking tagged clinical facts that are to be disclosed only to authorized users with clearance,
- Reformatting tagged and/or masked clinical facts into the artifact to be disclosed and determine required enveloping structure,
- Re-assigning security labels to the reformatted artifact's top level portion, sub-portions, and the envelope structure according to dominance rules.

For example, to disclose a tagged and masked CDA, security labels may be added to the SOAP body XDS Document Entry Metadata and to the payload at the header, section, and entry level with additional masking encryption where required by policy. Following security labeling service actions, the Access Control Service is responsible for release of the final tagged, and if required, masked disclosure as required by privacy policy and consent directive

Appendix J: Rendering a CDA with SECURITY LABELS

This appendix describes the HCS rules for assigning and rendering security labels in CDA document entry, document header, sections, and entries. These rules are the technical means for implementing the following HCS functional model business requirement included in Appendix B 1.2.2 Generate and store clinical facts**:**

> Provide the ability to persist structured and unstructured clinical elements and assigned clinical metadata encoded with standard terminologies as required for assignment of security labels.

Guidance: The system is able to accurately and completely encode unstructured data, including CDA narrative blocks, as reference-able from structured data. Any narrative content, which if encoded would require a security label, must be encoded as one or more structured clinical facts.

- This ensures that unstructured data such as text from a clinician's dictated note can be assigned security labels at the clinical fact level.

- This enables the access control system (ACS) to restrict access to and disclosure of unstructured clinical facts based on the security labels on the structured clinical facts. Authorized users will be able to view only the tagged unstructured clinical facts for which they have clearance.

- This enables the EHR to render the security labels on unstructured clinical facts that are assigned to the associated structured data. Rendering the security labels assigned to unstructured clinical facts ensures that the user is aware of the patient's privacy concerns and alerts the user to the level of confidentiality.

Assigning Security Labels to CDA Narrative Content Rules

1. **Unique Narrative Content Element Identifier Rule:** Narrative content associated with a CDA entry tagged with a security label ("tagged entry") must have a unique content element identifier.

   The requirement that a narrative content element have a unique identifier, which is otherwise optional in the CDA, is therefore, a further constraint on the CDA narrative block.

2. **Tagged Entry Reference to Narrative Content Element Identifier Rule:** A tagged entry must reference the identifier of the narrative content elements from which the entry was derived or from which the entry was composed in the originalText property of the entry Act.classCode. That is, all sensitive narrative content must be accurately and completely encoded.

   a. **Tagged Entry Reference to Derived Content Element Identifier:** When the narrative content is derived from CDA entries, the reference identifier in an entry originalText provides a link from the entry's security label to the referenced narrative content element.

      This linkage enables the rendering of the security label assigned to the tagged entry as a tag on the associated narrative content so that it is viewable by authorized users, including any prescribed privacy markings such as "do not disclose without consent". Rendering the security labels assigned to narrative content alerts the user about the patient's privacy concerns and the content's confidentiality.
      The ACS is able to restrict access to and disclosure of narrative content based on the entry's security labels. The ACS applies any redaction or masking required for disclosure of a tagged entry to the associated narrative content.

   b. **Component Tagged Entry Reference to Original Narrative Content Element Identifier:** When the narrative content is the source of component CDA entries, there is no guarantee that all of the sensitive narrative content is encoded.

      Unless all sensitive narrative content is encoded, the Security Labeling Service will not be able to assign required security labels to an associated entry. Without associated security labels, the ACS will be unable to restrict access and disclosure of sensitive narrative content.

      Authorized users will not be aware of the confidentiality, sensitivity, and handling caveats pertaining to narrative content or the patient's privacy concerns.

3. **Tagged Entry *Attribute* Reference to Original or Derived Narrative Content Element Identifier Rule:** In order to persist security labels with the sensitive coded attributes of a tagged entry, the attribute originalText must reference the associated narrative content element. A "sensitive" coded attribute would trigger assignment of the same security label with which the entry is tagged if it were not associated with the entry.

For example, the Observation.code, Observation.value, and Observation.text attributes of a HIV related Observation entry would trigger the same security label that is assigned to the entry.

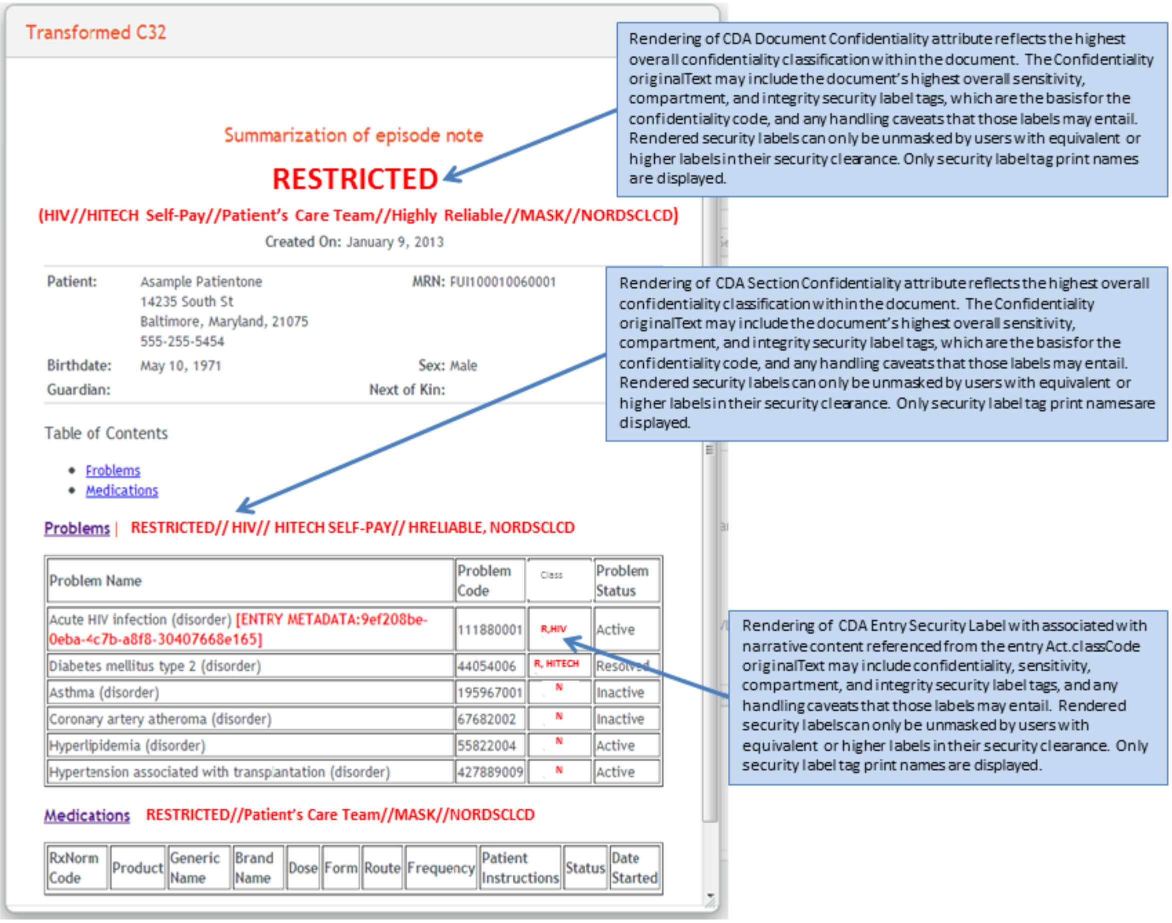
This ensures that the ACS access control decisions are the same for narrative content associated with the entry and the subset of that content that is associated with the entry’s sensitive attributes.

Narrative Content Referenced by a Tagged Entry Rule: Narrative content referenced by a tagged entry Act.classCode originalText must include all content elements associated with non-sensitive attributes of the tagged entry, including non-coded attributes such as effectiveTime, which do not have an originalText property from which to reference narrative content element identifiers.

Non-sensitive coded attributes are not required to reference associated narrative content element identifiers, and the narrative consent is not required to have content element identifiers for content representing non-sensitive attributes. However, the entry Act.classCode originalText must reference a content element identifier for the composite of content elements associated with all of the entry’s sensitive and non-sensitive attributes. For example, Observation attributes such as targetSiteCode, methodCode, and effectiveTime would not trigger security label assignment independently of their association with a sensitive entry.

This ensures that access control, redaction, and masking does not leave the remainder of the unstructured entry content “in the clear” for those not permitted to access restricted unstructured content, thereby flagging the narrative as having hidden or removed information.

Assigning and Rendering Security Labels on CDA Header, Sections, and Entries



Transformed C32

Summarization of episode note

RESTRICTED

(HIV//HITECH Self-Pay//Patient's Care Team//Highly Reliable//MASK//NORDSCLCD)

Created On: January 9, 2013

Patient: Asample Patientone
14235 South St
Baltimore, Maryland, 21075
555-255-5454 MRN: FUI100010060001

Birthdate: May 10, 1971 Sex: Male

Guardian: Next of Kin:

Table of Contents

- Problems
- Medications

Problems | RESTRICTED// HIV// HITECH SELF-PAY// HRELIABLE, NORDSCLCD

Problem Name	Problem Code	Class	Problem Status
Acute HIV infection (disorder) [ENTRY METADATA:9ef208be-0eba-4c7b-a8f8-30407668e165]	111880001	R,HIV	Active
Diabetes mellitus type 2 (disorder)	44054006	R, HITECH	Resolved
Asthma (disorder)	195967001	N	Inactive
Coronary artery atheroma (disorder)	67682002	N	Inactive
Hyperlipidemia (disorder)	55822004	N	Active
Hypertension associated with transplantation (disorder)	427889009	N	Active

Medications RESTRICTED//Patient's Care Team//MASK//NORDSCLCD

RxNorm Code	Product	Generic Name	Brand Name	Dose	Form	Route	Frequency	Patient Instructions	Status	Date Started

Rendering of CDA Document Confidentiality attribute reflects the highest overall confidentiality classification within the document. The Confidentiality originalText may include the document's highest overall sensitivity, compartment, and integrity security label tags, which are the basis for the confidentiality code, and any handling caveats that those labels may entail. Rendered security labels can only be unmasked by users with equivalent or higher labels in their security clearance. Only security label tag print names are displayed.

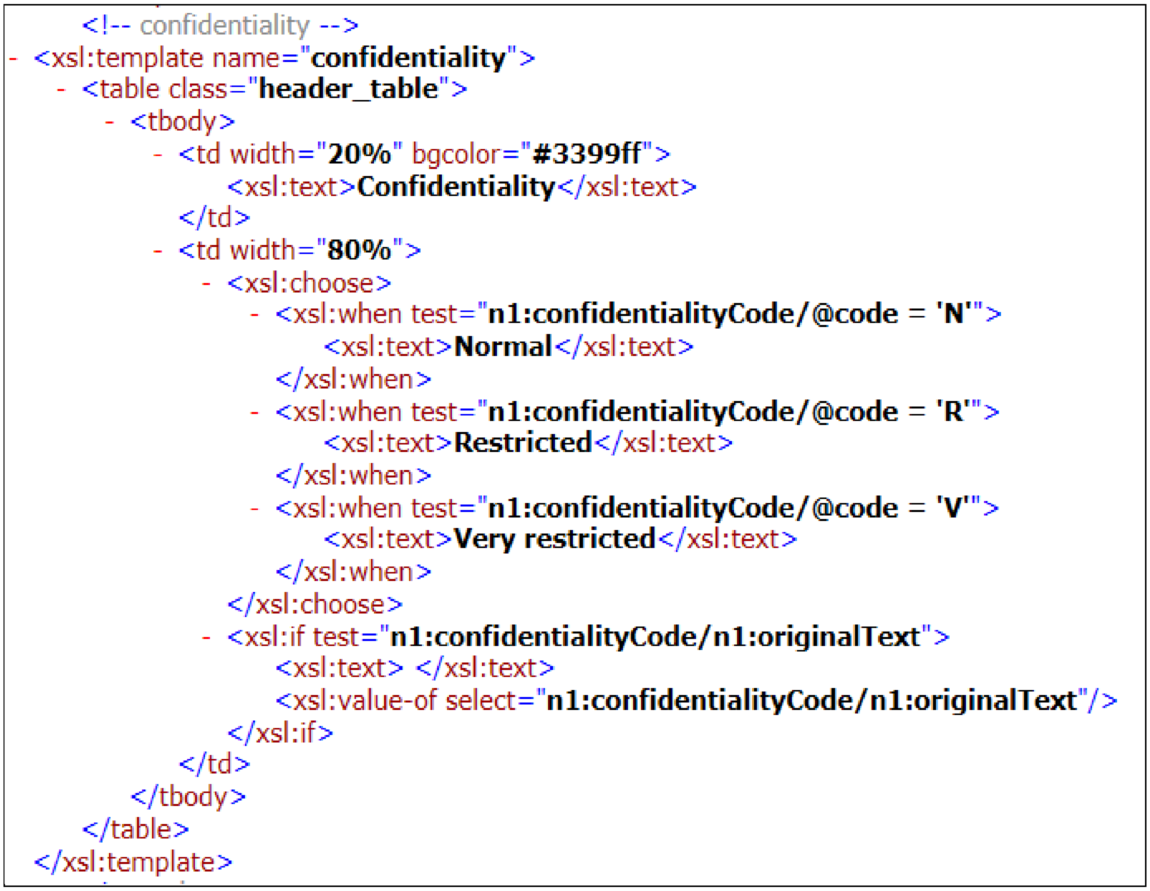
Rendering of CDA Section Confidentiality attribute reflects the highest overall confidentiality classification within the document. The Confidentiality originalText may include the document's highest overall sensitivity, compartment, and integrity security label tags, which are the basis for the confidentiality code, and any handling caveats that those labels may entail. Rendered security labels can only be unmasked by users with equivalent or higher labels in their security clearance. Only security label tag print names are displayed.

Rendering of CDA Entry Security Label with associated with narrative content referenced from the entry Act.classCode originalText may include confidentiality, sensitivity, compartment, and integrity security label tags, and any handling caveats that those labels may entail. Rendered security labels can only be unmasked by users with equivalent or higher labels in their security clearance. Only security label tag print names are displayed.

Document Header Rendering of Overall Highest Security Label Rule: The Confidentiality attribute on a CDA ClinicalDocument Header Class must be populated with the most restrictive confidentiality codes populating the Confidentiality attribute on all included Sections, i.e., the Confidentiality "high water mark".

A CDA high water Confidentiality attribute should be rendered using only the confidentiality code print name, e.g., "Restricted", and should not include the security label field name "Confidentiality".
The other security label field tags such as sensitivity, compartment, and integrity, which are the basis for assigned confidentiality code, may be rendered as print names from the Confidentiality originalText if and only if these can only be unmasked by users with equivalent or higher labels in their security clearance. Handling caveats, which are also related to the assigned confidentiality code, may also be rendered as print names if each

is viewable only by authorized users. Below is a CDA style sheet excerpt for rendering confidentialityCode and its originalText.



```
      <!-- confidentiality -->
- <xsl:template name="confidentiality">
   - <table class="header_table">
      - <tbody>
         - <td width="20%" bgcolor="#3399ff">
              <xsl:text>Confidentiality</xsl:text>
           </td>
         - <td width="80%">
            - <xsl:choose>
               - <xsl:when test="n1:confidentialityCode/@code = 'N'">
                    <xsl:text>Normal</xsl:text>
                 </xsl:when>
               - <xsl:when test="n1:confidentialityCode/@code = 'R'">
                    <xsl:text>Restricted</xsl:text>
                 </xsl:when>
               - <xsl:when test="n1:confidentialityCode/@code = 'V'">
                    <xsl:text>Very restricted</xsl:text>
                 </xsl:when>
              </xsl:choose>
            - <xsl:if test="n1:confidentialityCode/n1:originalText">
                 <xsl:text> </xsl:text>
                 <xsl:value-of select="n1:confidentialityCode/n1:originalText"/>
              </xsl:if>
           </td>
        </tbody>
     </table>
  </xsl:template>
```

Figure I1: CDA XSL Style Sheet

Narrative Block Rendering of Overall Highest Security Label Rule: The Confidentiality attribute on a CDA section must be populated with the most restrictive of the confidentiality codes populating the Confidentiality attribute on all included entries' security classification observations and all included sections, which in turn, have a high water mark confidentiality code based on the confidentiality codes from all included entry security classification observations.

The other entry security label field tags such as sensitivity, compartment, and integrity, which are the basis for their assigned confidentiality codes, may be rendered as print names from the Confidentiality originalText if and only if these can only be unmasked by users with equivalent or higher labels in their security clearance. Handling caveats, which are also related to the assigned confidentiality code, may also be rendered as print names if each is viewable only by authorized users.

CDA Document Entry and Security Label Rule: The XD* metadata in the CDA Document Entry must include a Confidentiality Code that is the overall highest confidentiality classification within the payload. Other security labels must not be included. Handling caveats relevant to intermediaries must be included. As shown in the diagram below, the Transport Envelope must contain only routing information, while the encrypted Inner Envelope must contain only the confidentiality and handling caveats required by intermediaries. All privacy compromising metadata such as healthcare facility types and practice settings associated the treatment for sensitive conditions must not be populated. Only handling caveats germane to the Intermediary must be included. Those that are not germane must not be included as these may indirectly compromise privacy by indicating the nature of the payload.

CDA Security Labeling and Meaningful Use

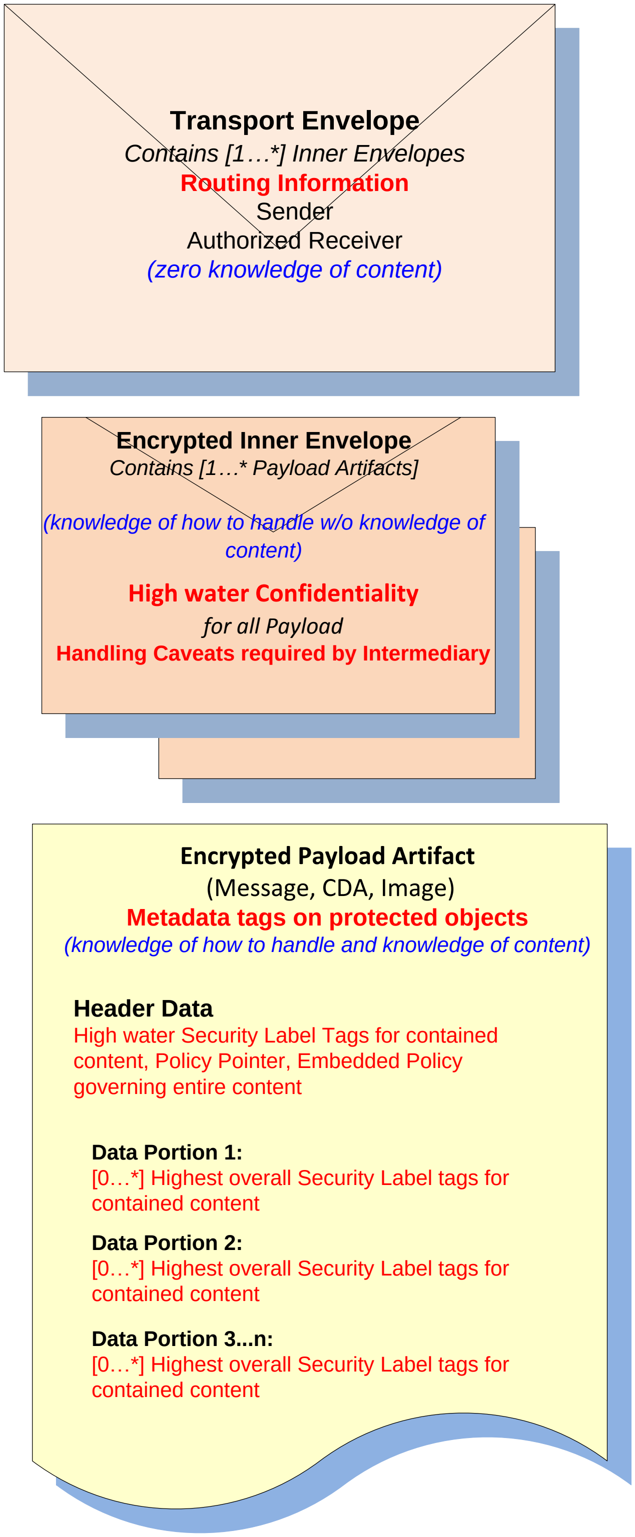
In the U.S., progress toward Meaningful Use adoption and migration to ubiquitous use of structured standards-based data is a key consideration when assessing the feasibility of requiring that all sensitive narrative content be linked to the security labels on associated CDA entries, and for requiring the rendering of security labels to authorized users at the header, section, and entry levels.

The following data points indicate the high percentage of acute hospital providers who are entering, viewing, and using structured data to meet Meaningful Use. While this data may have been encoded based on unstructured data, e.g., dictation notes, which would be inefficient and would likely not scale sufficiently to generate the structured data required to meet capabilities such as CDS, medication lists, and DDI checks. Arguably, most acute hospital EHRS meeting Meaningful Use requirements are less likely to be generating the structured data from unstructured charts and dictation. Note that Advanced Directives are unstructured.

These data points, which indicate the level of structured data use, may be evidence that Meaningful Use certified EHRS should be capable of meeting the HCS requirements for tagging narrative content and rendering security labels to authorized users in order to meet privacy mandates under 42 CFR Part 2, Title 38 Section 7332, and HIPAA self-pay provisions.

Assigning HCS Security Labels to Clinical Facts

Assigning security labels to clinical facts requires consideration of the degree of granularity that conveys information that requires protection and the level of protection required, i.e., the classification level. In addition, two or more clinical facts may be aggregated, and may thereby convey information requiring a higher level of protection by providing increased context. Determining the level of granularity at which a clinical fact should be assigned a security label is comparable to the concept of “portions” in intelligence community. A portion, in accordance with is classified by determining the risk of harm resulting from unauthorized disclosure (ISO/IEC 7498-2:1989/CCITT Rec. X.800). This implies that the information must have enough context to be understood as a whole on its own, and may take on a different meaning when combined with other portions. For example, two unclassified portions may become confidential when combined because together they contribute additional information that increases the potential for unauthorized disclosure to result in harm. When portions classified at different levels are aggregated, the resulting portion is classified with the overall most restrictive label tags or "high water mark". DoD Guide to Marking Classified Documents



Transport Envelope
Contains [1…] Inner Envelopes*
Routing Information
Sender
Authorized Receiver
(zero knowledge of content)

Encrypted Inner Envelope
Contains [1… Payload Artifacts]*

(knowledge of how to handle w/o knowledge of content)

High water Confidentiality
for all Payload
Handling Caveats required by Intermediary

Encrypted Payload Artifact
(Message, CDA, Image)
Metadata tags on protected objects
(knowledge of how to handle and knowledge of content)

Header Data
High water Security Label Tags for contained content, Policy Pointer, Embedded Policy governing entire content

Data Portion 1:
[0…*] Highest overall Security Label tags for contained content

Data Portion 2:
[0…*] Highest overall Security Label tags for contained content

Data Portion 3...n:
[0…*] Highest overall Security Label tags for contained content

APPENDIX K: SECURITY LABEL REGISTRATION FORM (NISTIR 5308)

C.1.2 General Tag Set Information

Tag Set Name Format:

[ ] Object Identifier (Layer 7 label syntax)

[ ] Unsigned Integer (Layer 3 label encoding)

Requested Alpha-Numeric Name:

Maximum number of security tags:

Minimum number of security tags:

Tag combination and ordering rules:

C.1.3 Tag-Specific Information

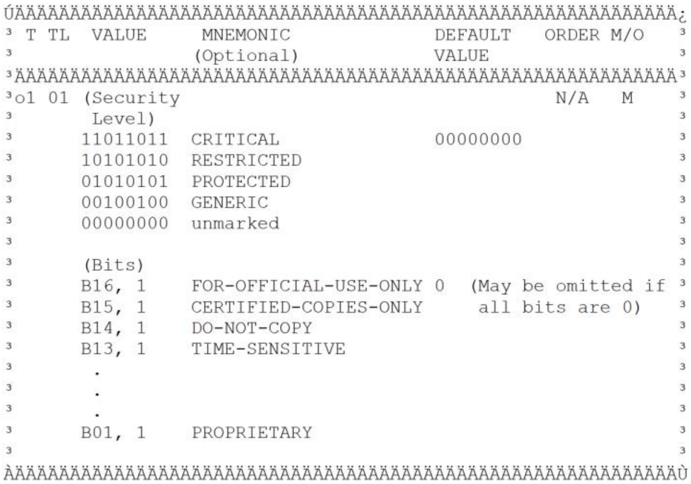
For each tag indicate:

Tag number: Is order significant? (Yes/No)

Tag Type: Is tag Optional or Mandatory?

List of valid attribute values:

The table format in the following example may be used to describe each tag. TT stands for tag type and TL is the tag length. The types are given in the SSL document. Only the tag values indicated will be accepted by an implementation of the Tag Set. An optional mnemonic may be associated to the each attribute value, bit, or field on the tag. A default value for each tag may be given, if appropriate. An optional tag order indication within the set also may be given. The presence of the tag in the set may be marked mandatory or optional. A Tag Set that does not match the format associated with the Tag Set Name preceding it is in error and shall be treated as such by the implementation.



```
ÚÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ¿
³ T TL  VALUE      MNEMONIC                DEFAULT   ORDER M/O   ³
³                 (Optional)               VALUE                 ³
³ÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄ³
³o1 01 (Security                                   N/A    M      ³
³       Level)                                                   ³
³      11011011  CRITICAL                  00000000              ³
³      10101010  RESTRICTED                                      ³
³      01010101  PROTECTED                                       ³
³      00100100  GENERIC                                         ³
³      00000000  unmarked                                        ³
³                                                                ³
³      (Bits)                                                    ³
³      B16, 1    FOR-OFFICIAL-USE-ONLY 0  (May be omitted if     ³
³      B15, 1    CERTIFIED-COPIES-ONLY     all bits are 0)       ³
³      B14, 1    DO-NOT-COPY                                     ³
³      B13, 1    TIME-SENSITIVE                                  ³
³        .                                                       ³
³        .                                                       ³
³        .                                                       ³
³      B01, 1    PROPRIETARY                                     ³
³                                                                ³
ÀÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÄÙ
```

C.1.4 Security Object Usage Rules and Handling Instructions

This section shall cover object usage rules, handling instructions, and implementation details or restrictions beyond those imposed by the base standard. The text in this section may be used to clarify security tag information appearing in the Format Table. Examples are error conditions and their required system response such as return of an error response and local event auditing. The processing rules in Appendix B of the Standard Security Label FIPS may be referenced in this section. Explicit omissions, additions, or refinements to the processing rules in the SSL document also must appear in this section.

10. REFERENCES

ACM, Yogesh, L. Simmhan, et al, A survey of data provenance in e-science, Newsletter ACM SIGMOD Record, Volume 34 Issue 3, Pages 31 - 36, ACM New York, NY, USA, September 2005

ASTM E1986 - 09 (2013) Standard Guide for Information Access Privileges to Health Information

(GWU) Mellissa M. Goldstein, JD et al, Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis, George Washington University Medical Center, September 29, 2010

(HITECH) 45 CFR Parts 160 and 164 Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules

HL7 Version 3 Standard: Role-based Access Control Healthcare Permission Catalog, Release 2 (revision of ANSI/HL7 V3 RBAC, R1-2008), 2/26/2010

IETF, IETF RFC 1457, Security Label Framework for the Internet (Informational), May 1993

IETF, IEFT RFC 6120, Extensible Messaging and Presence Protocol (XMPP): Core (Proposed Standard), March 2011

IETF, IETF RFC 6121, Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence (Proposed Standard), March 2011

ISO, ISO/IEC 2382-8 Information technology -- Vocabulary -- Part 8: Security, 1998 Equivalent: T-REC-X.812-199511-I!!PDF-E

ISO/IEC, ISO 7498-2, Information processing systems-Open systems interconnection-Basic reference model-Part 2: Security Architecture, 1989

ISO/IEC, ITU-T Recommendation X.812 (1995), ISO/IEC 10181-3-00, Information Technology - Open Systems Interconnection - Security Frameworks in Open Systems - Access Control, March 2000

ISO, ISO 15489-1:2001, Information and documentation -- Records management -- Part 1: General, 2001

(ISO 14721) ISO 14721:2003 Space data and information transfer systems -- Open archival information system -- Reference model (OAIS). This reference model is defined by recommendation CCSDS 650.0-B-1 of the Consultative Committee for Space Data Systems

(OASIS XACML) Organization for the Advancement of Structured Information Standards (OASIS) eXtensible Access Control Markup Language (XACML) Version 3.0 August 10, 2010

(NISO) National Information Standards Organization Understanding Metadata

(NIST) FIPS 188 - Standard Security Label for Information Transfer

NIST, Special Publication 800-53, Recommended Security Controls for Federal Information Systems, February 2005

(PCAST) President's Council of Advisors on Science and Technology, "Realizing the Full Potential of Health Information Technology to Improve Healthcare for Americans: The Path Forward", December 2010

(Simmhan) Yogesh, L. Simmhan, et al, A survey of data provenance in e-science, Newsletter ACM SIGMOD Record, Volume 34 Issue 3, Pages 31 - 36, ACM New York, NY, USA, September 2005

(W3C) W3C, PROV-O: The PROV Ontology, W3C Candidate Recommendation, 11 December 2012

Warwick Ford, Computer Communications Security, Prentice Hall, ISBN 0-13-799453-2, 1994

(XMPP) Extensible Messaging and Presence Protocol

[i] Targets represent computer-based or communications entities to which access is attempted or that are accessed by Initiators. A target may be, for example, an OSI layer entity, a file, or a real system.