Healthcare Privacy and Security Classification System (HCS)

HL7 Workgroup Meeting

September, 2013

Mike Davis

Agenda

- Introduction to Data Segmentation
- Definition and Purpose
- Healthcare Classification System
- Examples
- Conclusion

Wife of a Wounded Warrior

(AFP OUT) U.S. President Barack Obama greets Sarah Wade, wife of Ted Wade after signing the Caregivers and Veterans Omnibus Health Services Act in the State Dining Room of the White House May 5, 2010 in Washington, DC. The act will improve health care services for veterans and expand caregiver benefits and training.
(May 4, 2010 - Photo by Pool/Getty Images North America)

- Courageous personal fight to prevent sharing of husbands healthcare information beyond that actually needed for treatment.

Testimony:
http://veterans.house.gov/hearings/Testimony.aspx?TID=59828&Newsid=567&Name=%20Sarah%20%20Wade

Sarah Wade Video:
http://www.youtube.com/watch?v=LUiSPkmX09g

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" *

*Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis
Melissa M. Goldstein, JD; and Alison L. Rein, MS, Director Academy Health.
Acknowledgements: Melissa M. Heesters, JD; Penelope P. Hughes, JD; Benjamin Williams; Scott A. Weinstein, JD

Security Labels

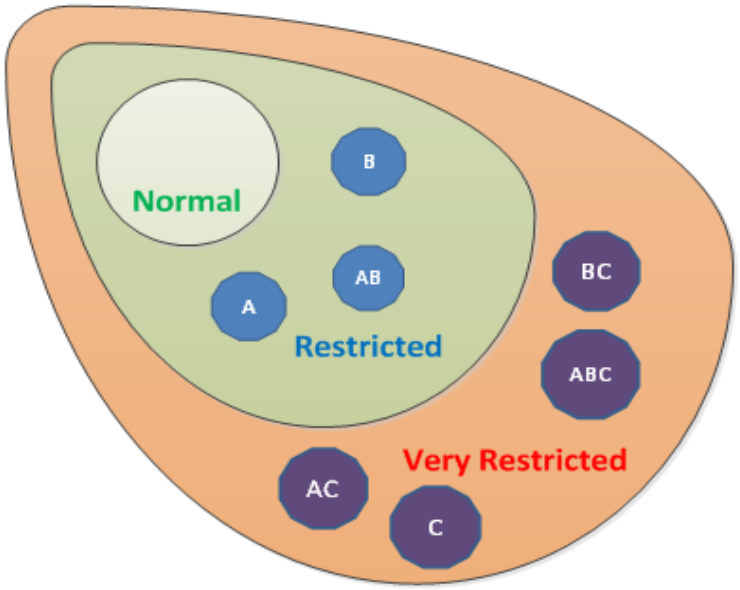
"Security labels convey information used by protocol entities to determine how to handle data communicated between open systems. Information on a security label can be used to control access, specify protective measures, and determine additional handling restrictions required by a communications security policy. "

NIST FIPS PUB 188

Segmenting with Labels (1)

- **Security Labels are placed on to documents and other information for two reasons: (ISODE Security Label)**

  1. **To clearly label information in an unambiguous manner, in order to facilitate human and computer handling of the information,**



The HL7 Healthcare Privacy and Security Classification System (HCS) provides a structured security label for data segmentation purposes.

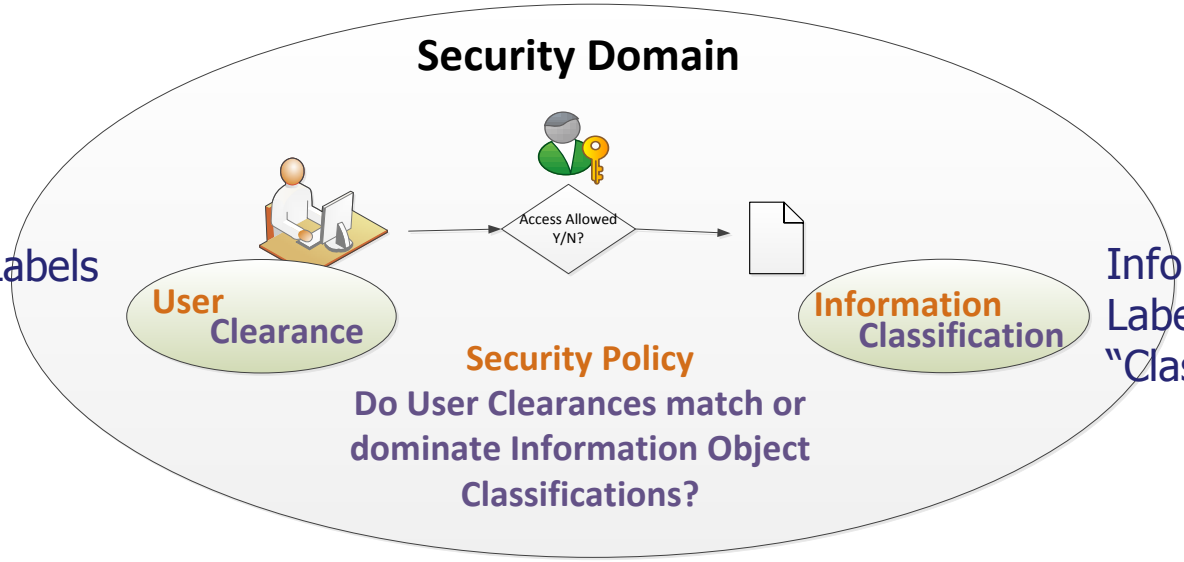
Helps ensure that only a valid security label is used and may also facilitate label mapping into a different security domain.

Segmenting with Labels (2)

2. **To enable a computer to perform Access Control operations on the information, so that the information is accessed only by appropriately cleared people in appropriate locations.**

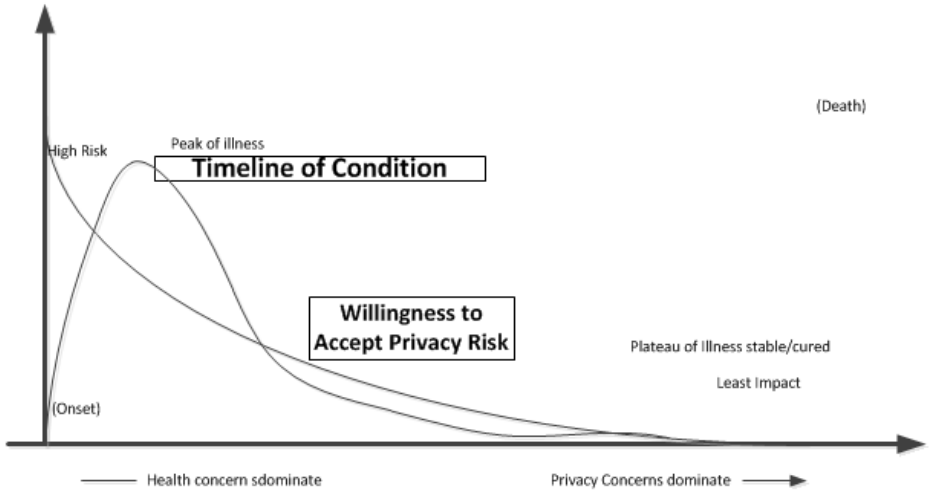
Access Control is performed by checking the data Security Label against the user's Security Clearance in the context of a Security Policy, leading to a yes/no answer for the access control and optionally with handling instructions and/or obligations on the part of the recipient

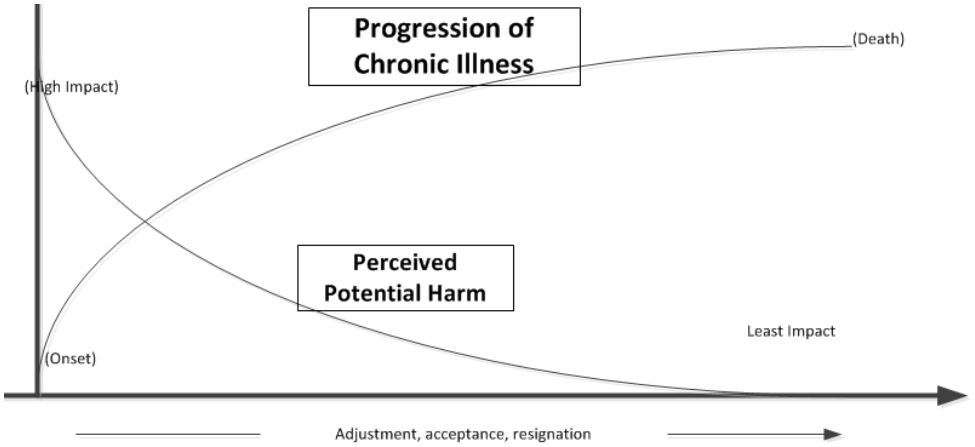
User Security Labels are called "Clearances"



Information Security Labels are called "Classifications"

Timeline of Perceived Harm





Why Segment Data?

- **Some healthcare information requires special handling that goes beyond the protections already provided through common security and privacy practice.**
- **Additional protection through the use of data segmentation addresses social hostility and stigma associated with certain medical conditions.***
- **Data Segmentation for Privacy provides a means for electronically implementing choices made under applicable privacy laws.**

* e.g., *The confidentiality of alcohol and drug abuse Patient records regulation and the US realm HIPAA privacy rule: Implications for alcohol and substance abuse programs*; June 2004, Substance Abuse and Mental Health Services Administration.

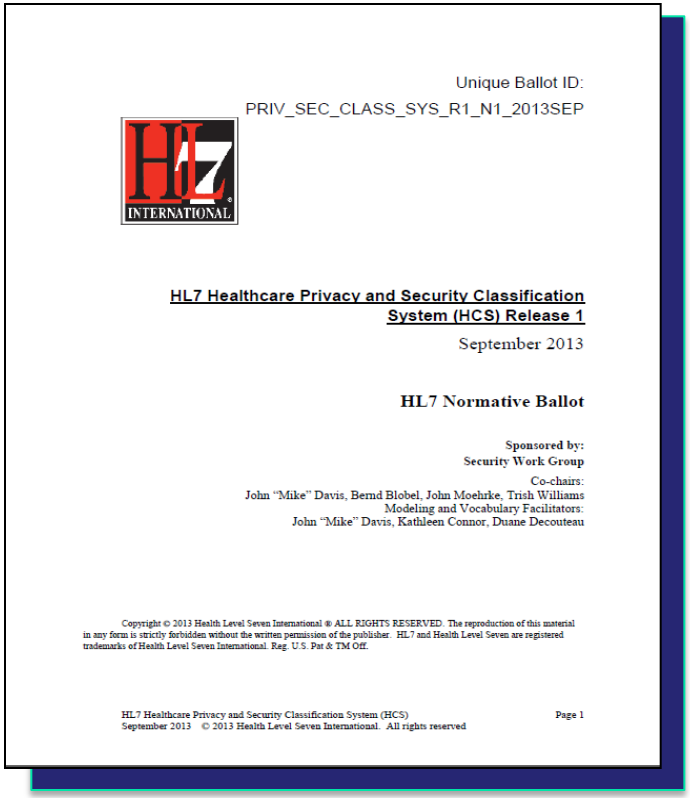
Significance: Patient

- One day you, or someone you care about, is going to get really sick or mentally ill and when you do you may want to control who sees sensitive, intimate or personal information about you. In other words to protect your privacy, dignity and to prevent hostile, annoying or prejudicial actions being taken against you.

Significance: Clinician

- **You are a doctor who swore an oath to "do no harm" which includes honoring your patients choices about exposure of sensitive health information that could cause real or perceived harm, preventing damage to your professional reputation and avoiding fines and lawsuits for violation of security and privacy laws.**

HL7 Healthcare Privacy & Security Classification System (HCS) Sept 2013 Ballot



Unique Ballot ID:
PRIV_SEC_CLASS_SYS_R1_N1_2013SEP

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

September 2013

HL7 Normative Ballot

Sponsored by:
Security Work Group

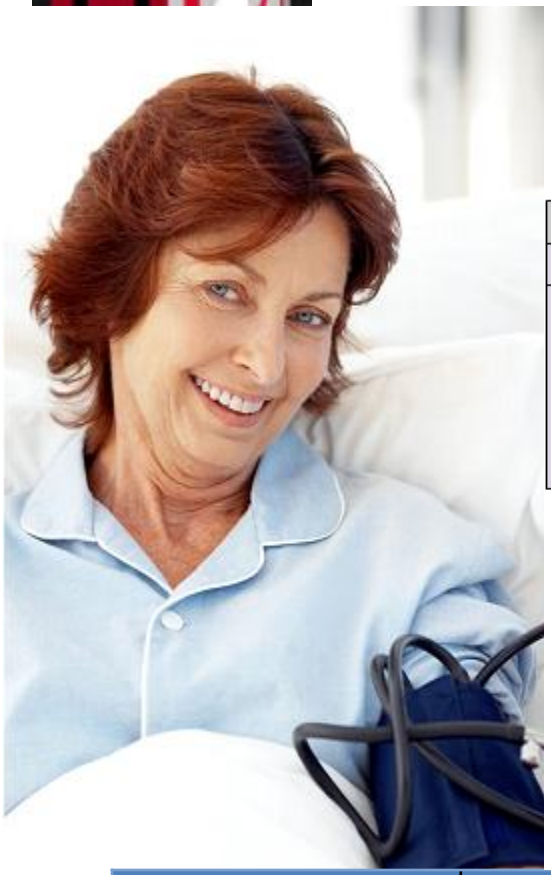
Co-chairs:
John "Mike" Davis, Bernd Blobel, John Moehrke, Trish Williams
Modeling and Vocabulary Facilitators:
John "Mike" Davis, Kathleen Connor, Duane Decouteau

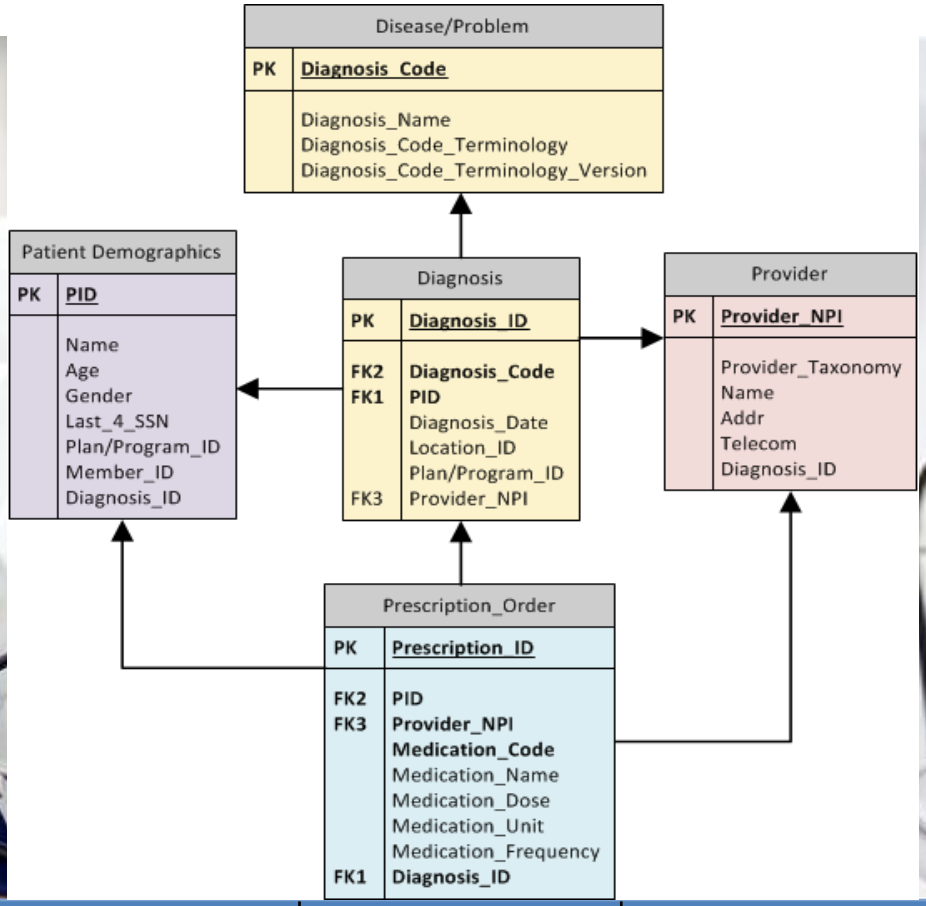
HL7's approach to data segmentation through labels.

Layered Approach for Privacy Metadata

- "Russian doll" concept of applying metadata with decreasing specificity as layers are added to the clinical data.
  - Document Level (High Water Mark)
    - Portion Level
      - Entry Level

Security Labels Bind Clinical Metadata to Patient Consent

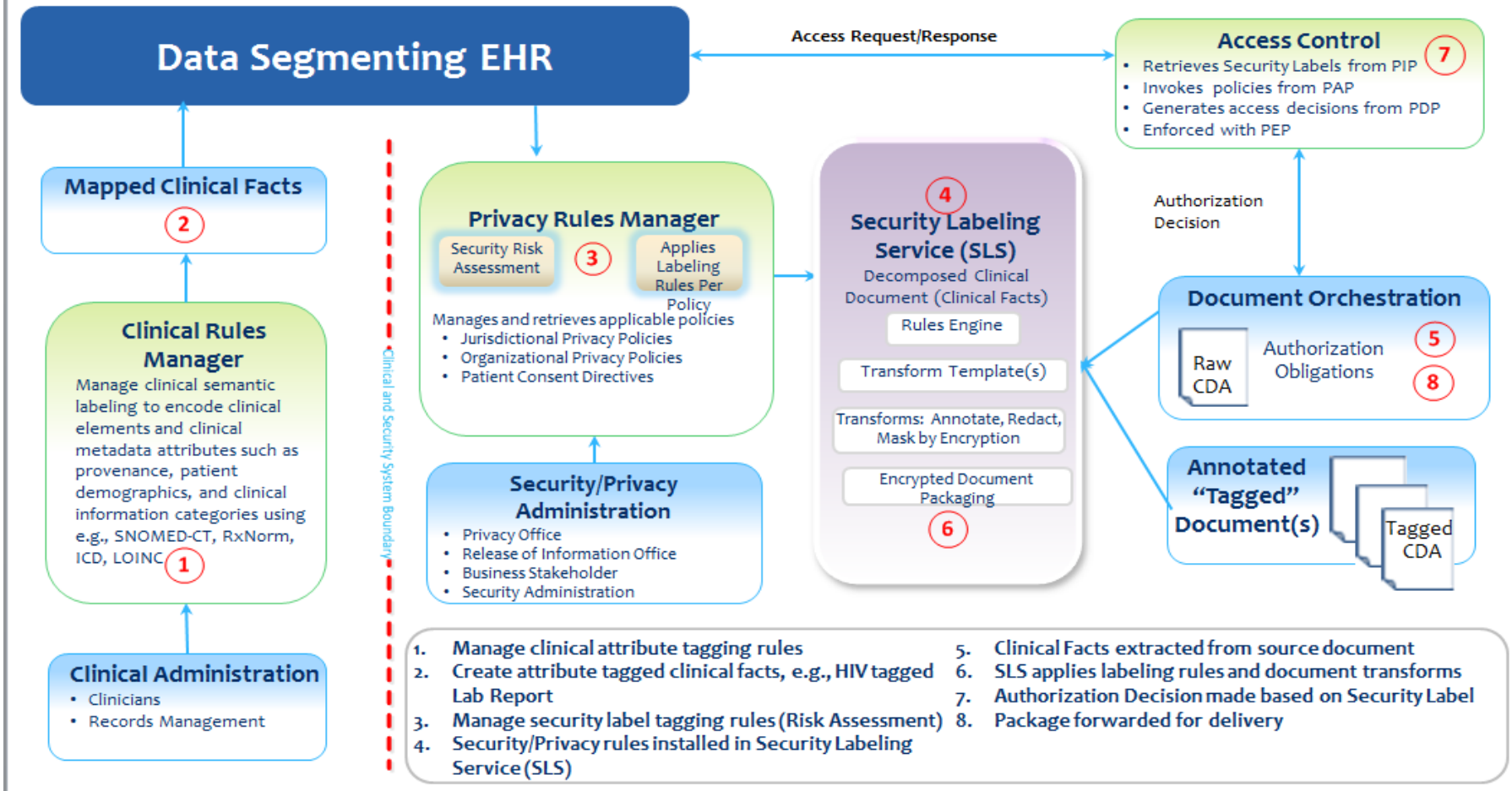




Medication ID	Medication Name	Terminology	Confidentiality	Sensitivity
11413	AZT (Zidovudine)	RxNorm	Restricted	HIV
Diagnosis ID	Diagnosis Name	Terminology	Confidentiality	Sensitivity
111880001	Acute HIV Disorder	SNOMED	Restricted	HIV
Privacy Rule: If Diagnosis=111880001 (HIV) and Medication=11413 (Zidovudine), then Security Label Tags are Confidentiality = R and Sensitivity = HIV				

Data Segmentation Using Healthcare Privacy and Security Labels

Data Segmentation, using a standards-based approach for privacy metadata to achieve interoperability and appropriate sharing of protected information, ensuring those who receive it handle it correctly.



Healthcare Classification System (HCS)

- To support privacy metadata, the HCS defines a quadruplet (4-tuple) of resource label fields, which are ***security attributes*** about clinical facts
  - [1…1] Confidentiality Security Classification Label Field
  - [0…*] Sensitivity Security Category Label Field
  - [0…*] Integrity Security Category Label Field
  - [0…*] Compartment Security Category Label Field
- HCS Security Label includes a security policy-based label (privacy mark) for ***handling caveat*** label field to convey Purpose of Use, Obligations, and Refrain and other policies to which custodians and recipients of clinical facts must comply.
  - [0…*] Handling Caveat Security Category Field
- These labels define the classification of each item and constituent components (inner envelope, cover sheet, body, and section(s) and sub-sections, segments or portions)

Security Label Field	Label Definition	Notes
Confidentiality	Security label 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 that could result from unauthorized disclosure.	Only one classification value is permitted on the header of an IT resource. It must be high water mark (most restrictive). In order to access a classified (tagged) IT resource, the user must possess rights greater than or equal to the IT resource classification. [ISO/TS 22600-3:2009(E) A.3.2]

Security Label Field	Label Definition	Notes
Sensitivity	Security label metadata categorizing the value, importance, and vulnerability of an IT resource perceived as undesirable to share.	In order to access sensitivity tagged IT resource, the user must possess rights corresponding to the sensitivity tag(s).

Security Label Field	Label Definition	Notes
Integrity	Security label metadata conveying the completeness, veracity, reliability, trustworthiness, and provenance of an IT resource.	Distinguish from assurance that information has not been modified in unauthorized way (subset)

Security Label Field	Label Definition	Notes
Compartment	Security label metadata that "segments" an IT resource by indicating that access and use is restricted to members of a defined community or project.	

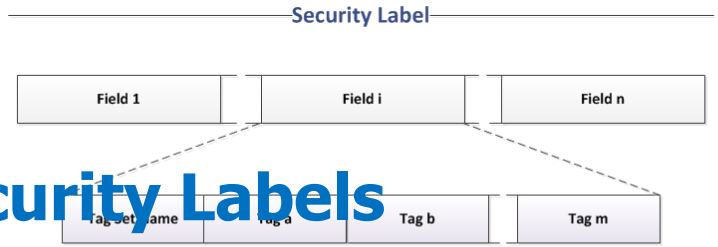
Security Label Field	Label Definition	Notes
Handling Caveat	Security label metadata conveying dissemination controls, information handling caveats, purpose of use, refrain policies, and obligations to which an IT resource custodian or receiver must comply.	Applies to all information within scope of the caveat

NIST FIPS PUB 188 Standard Security Label

Security Label

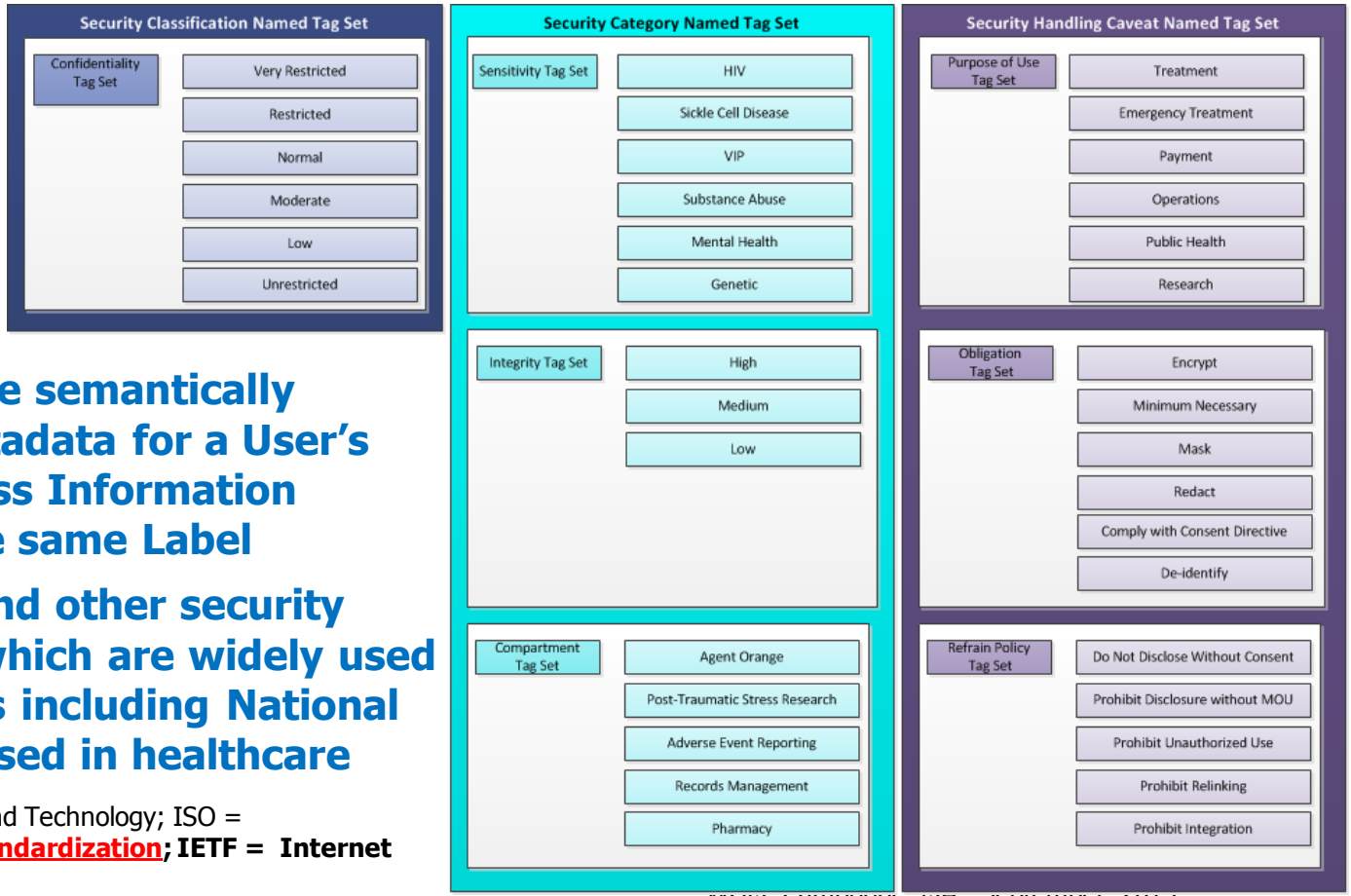
- **General structure of the NIST label structure consists of a set of fields**
- **Each field comprises a globally unique Tag Set Name, plus a set of security tags**

Healthcare Security Labels



NIST FIPS PUB 188 Security Labels

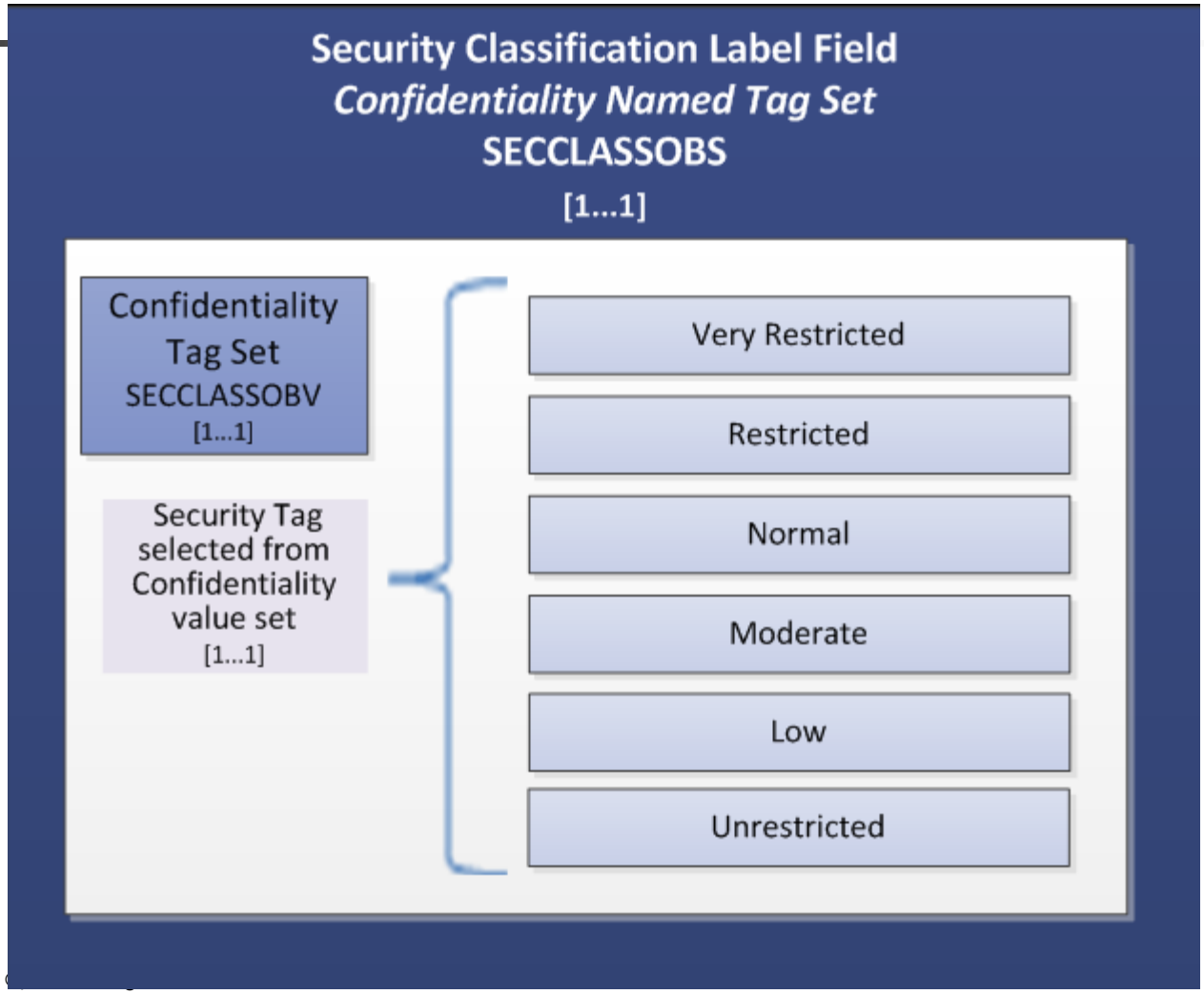
HL7 Privacy and Security Classification System



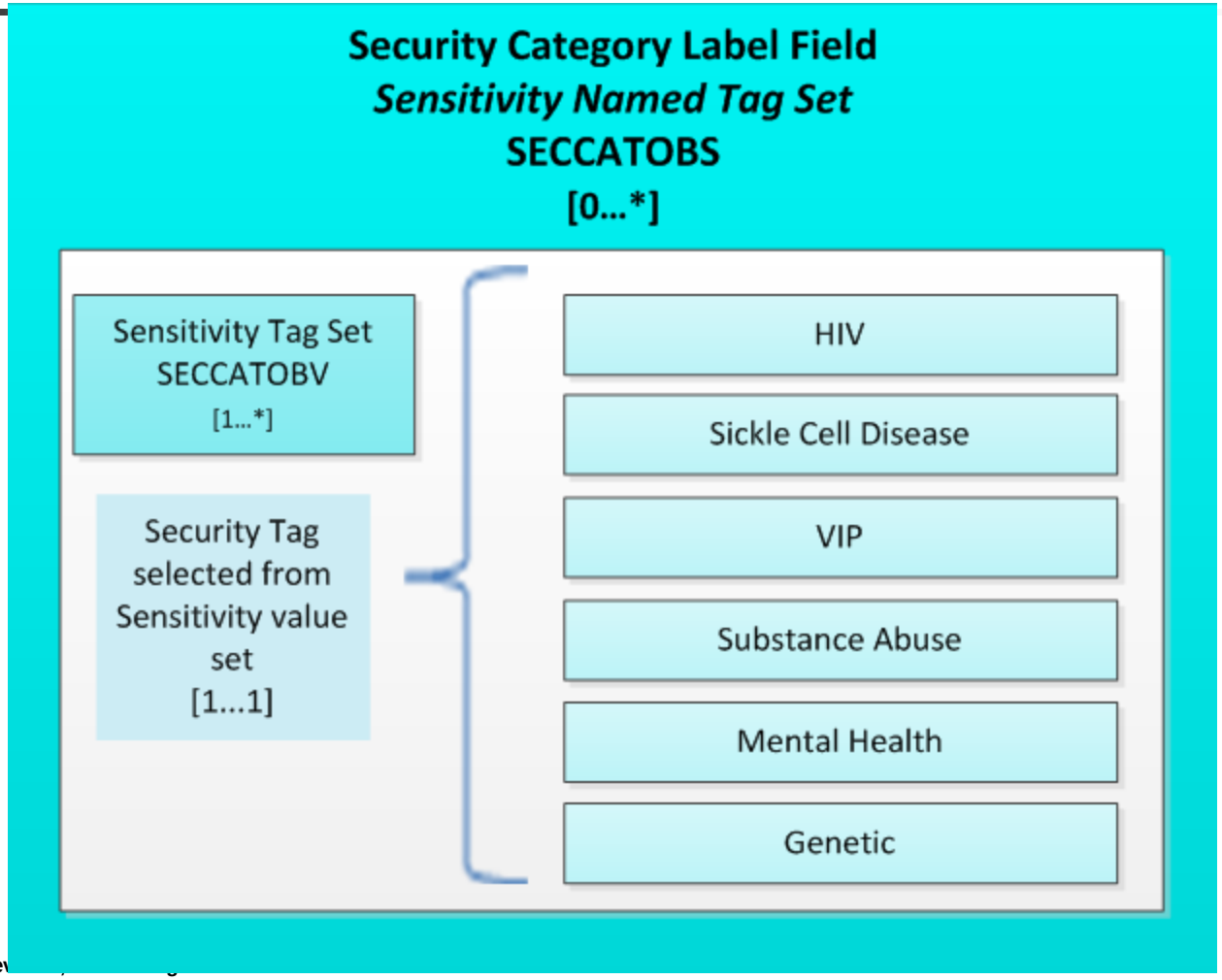
- **Security Labels are semantically interoperable metadata for a User's Clearance to access Information classified with the same Label**
- **NIST, ISO, IETF and other security label standards, which are widely used in other industries including National Defense, can be used in healthcare**

NIST = National Institute of Science and Technology; ISO = International Organization for Standardization; **IETF = Internet Engineering Taskforce**

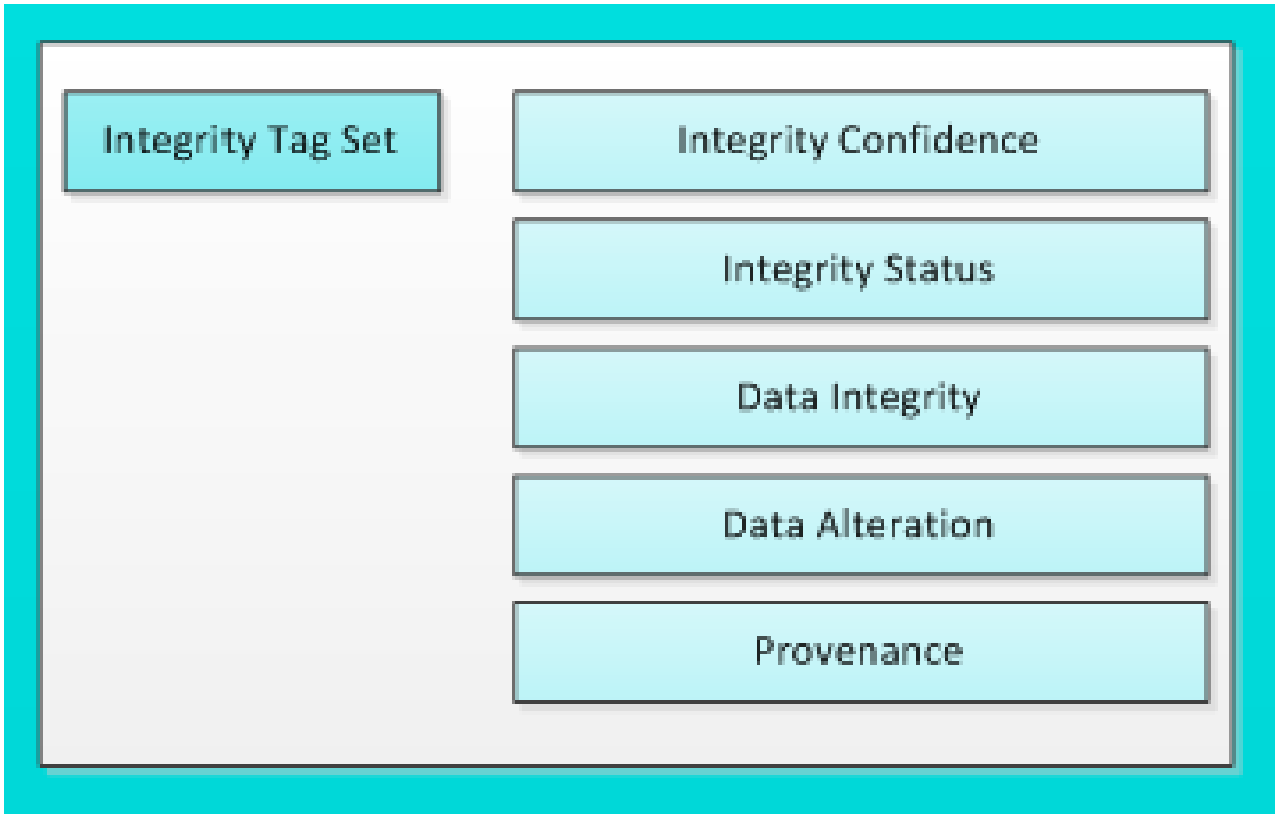
HCS Security Label Field Usage Notes
Field 1: Confidentiality



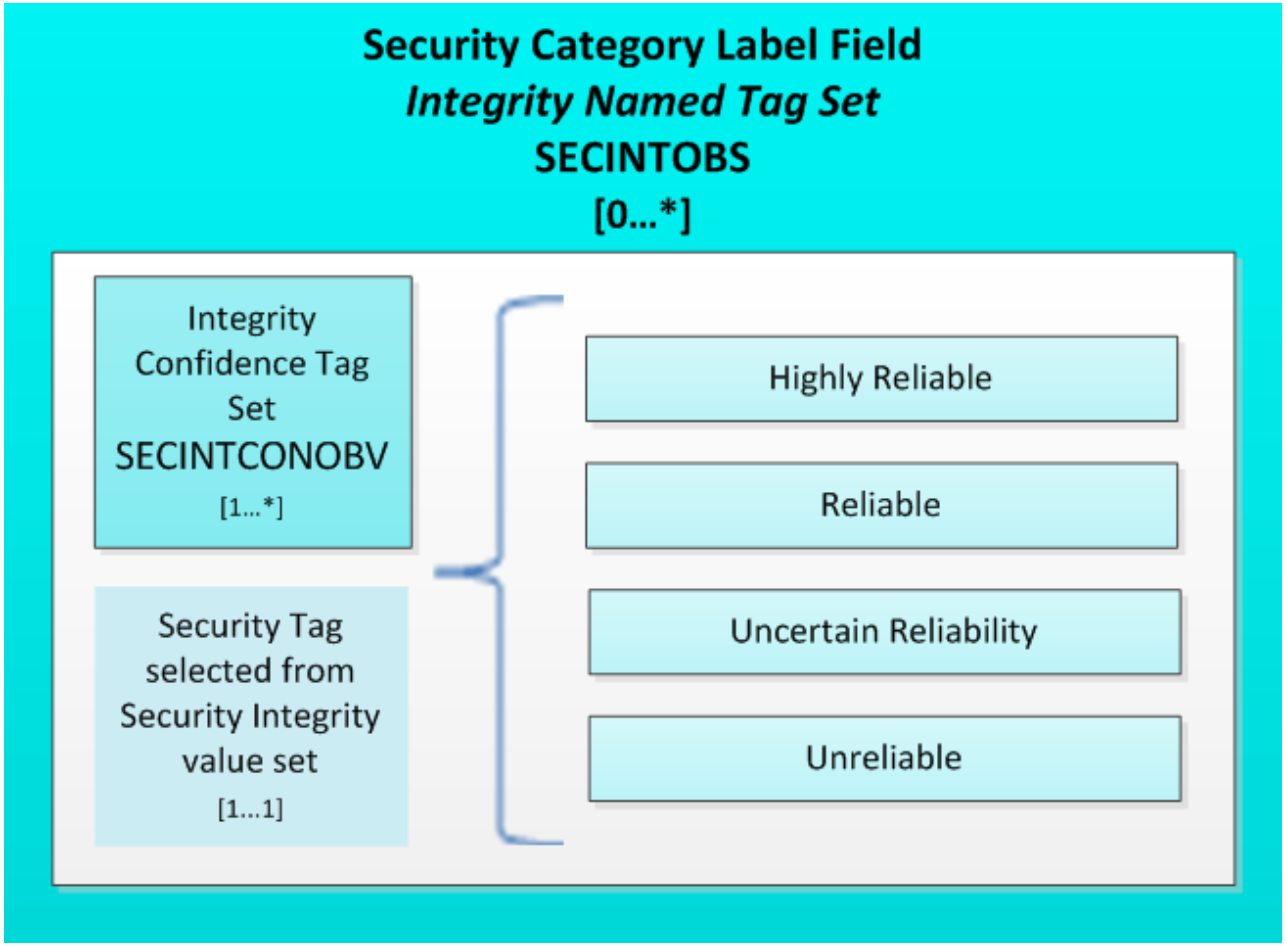
HCS Security Label Field Usage Notes
Field 2: Sensitivity



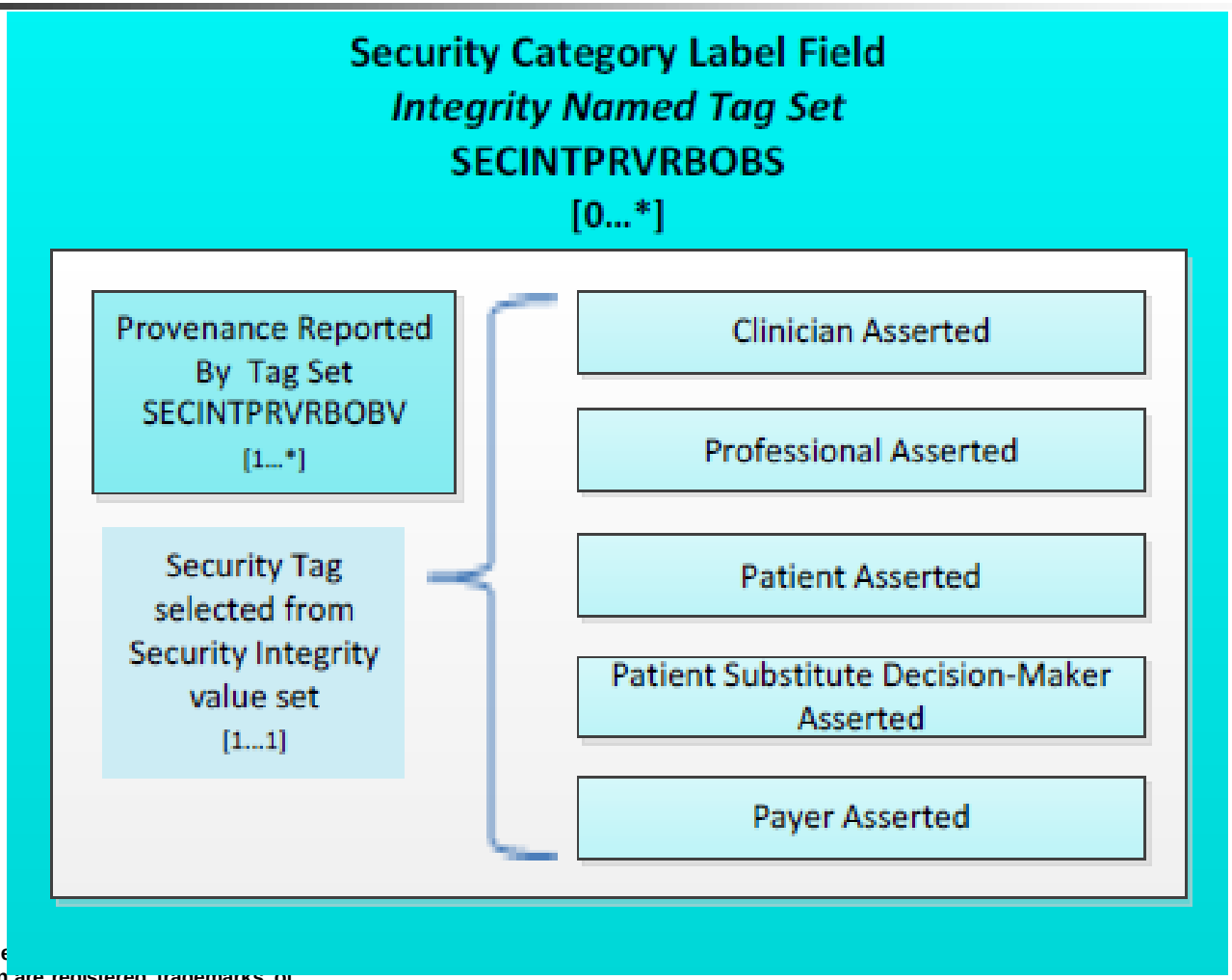
HCS Security Label Field Usage Notes
Field 3: Integrity



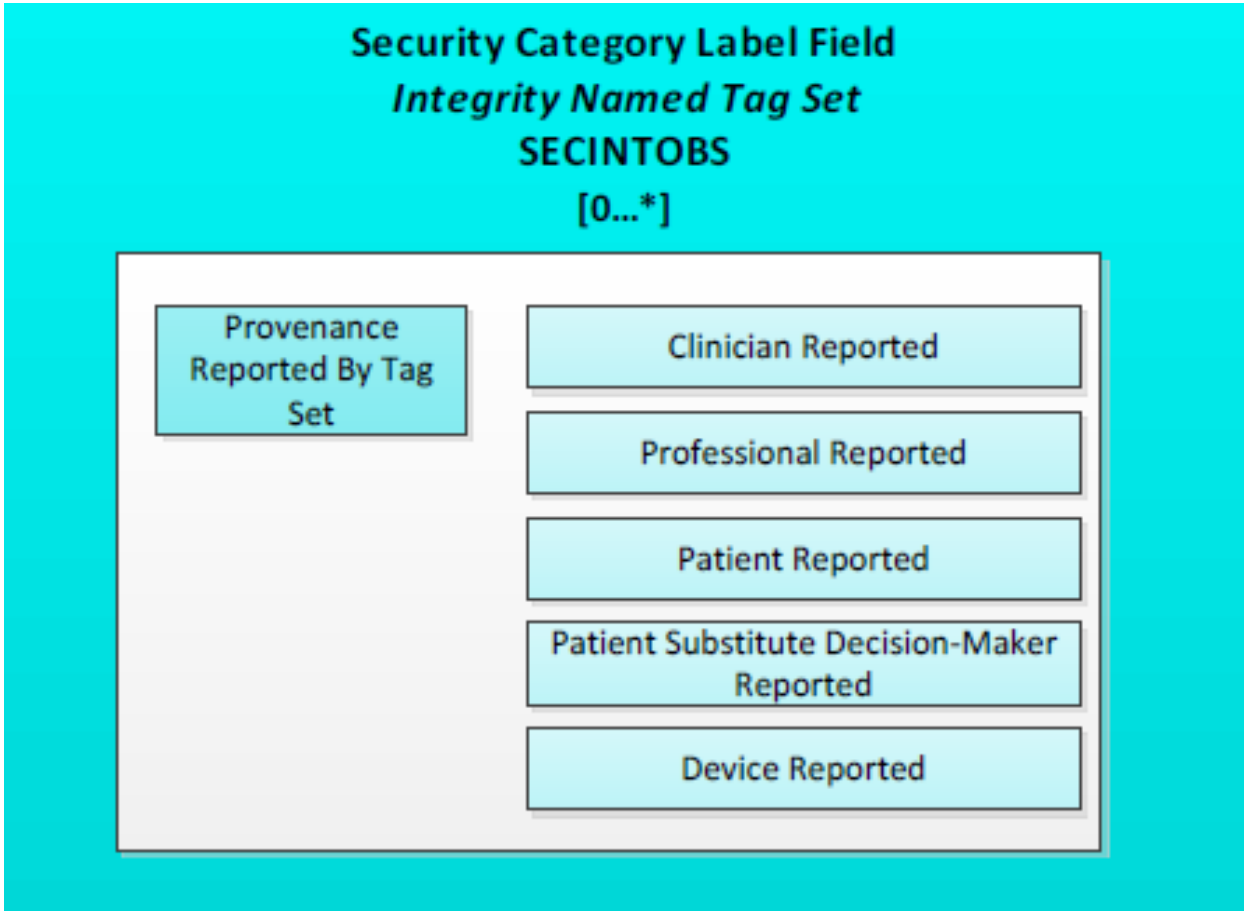
HCS Security Label Field Usage Notes
Field 3: Integrity



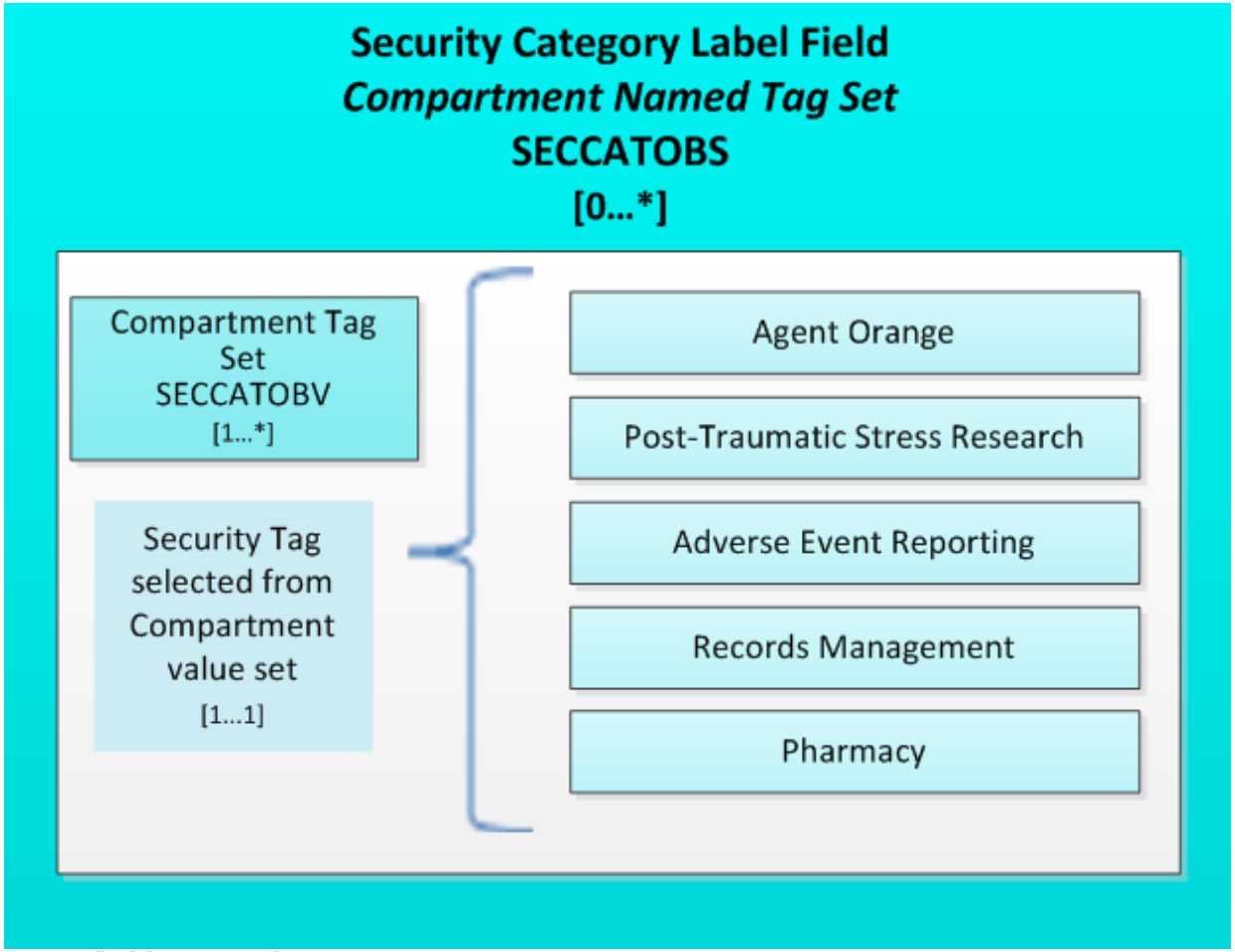
HCS Security Label Field Usage Notes Field 3: Integrity



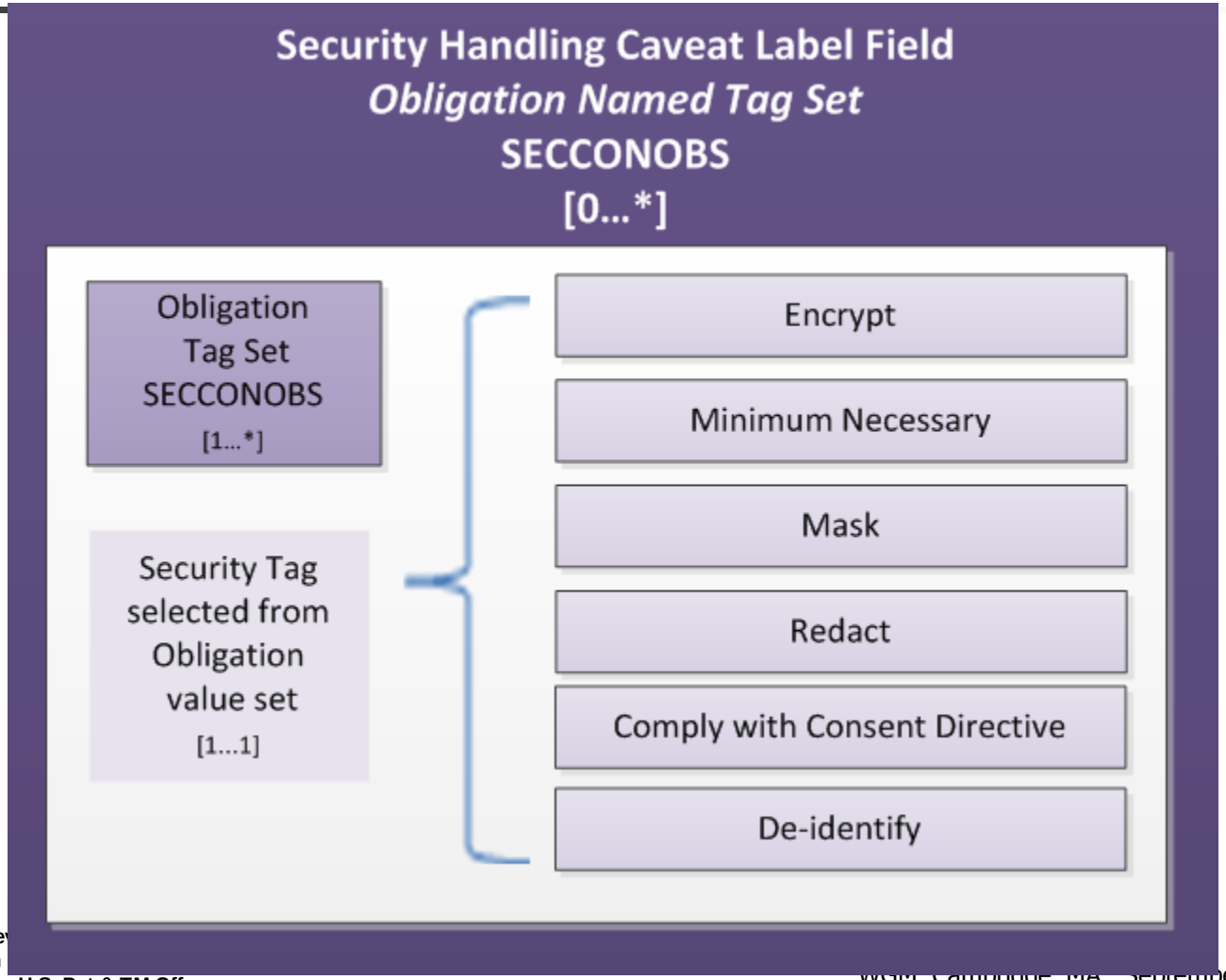
HCS Security Label Field Usage Notes
Field 3: Integrity



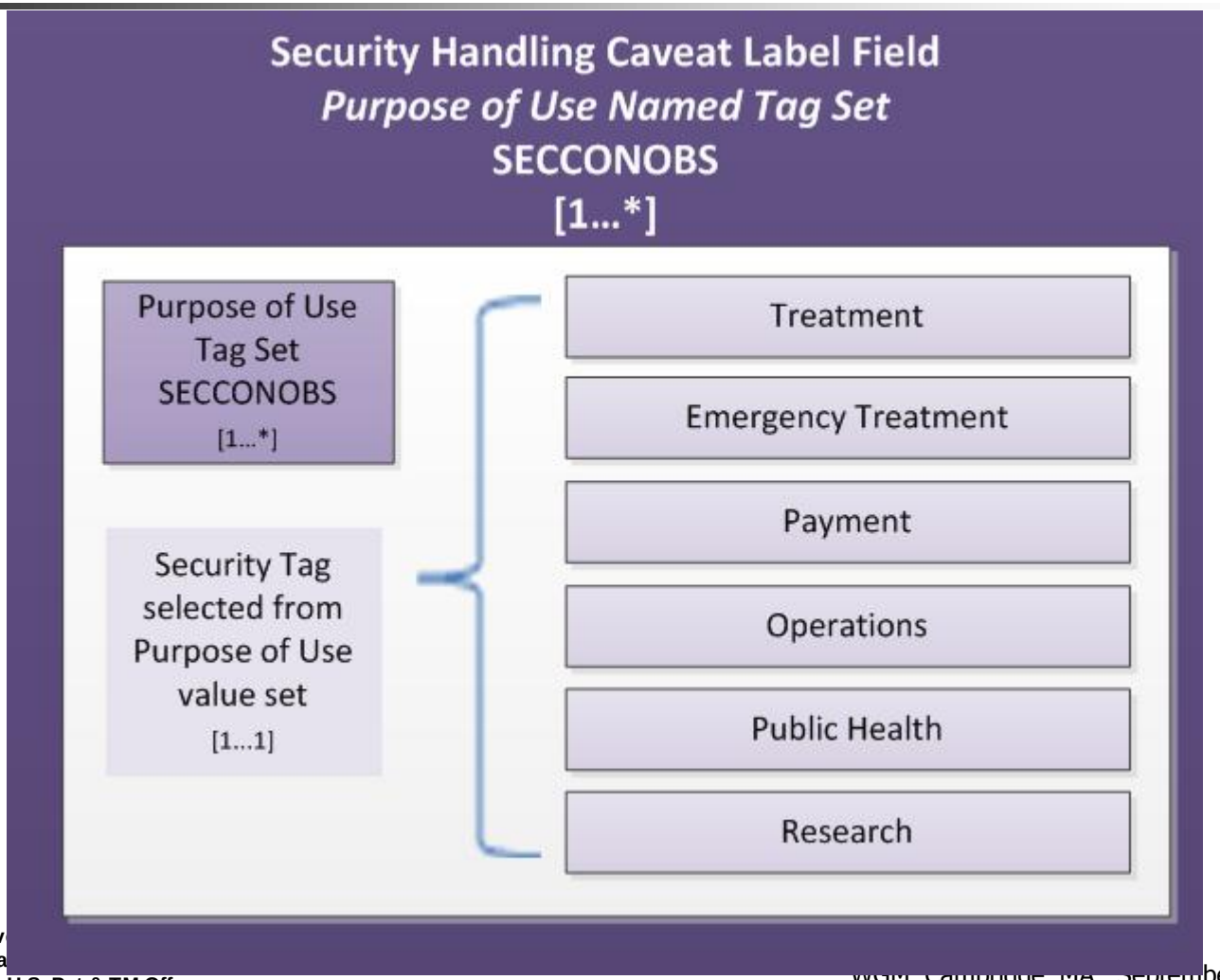
HCS Security Label Field Usage Notes
Field 4: Compartment



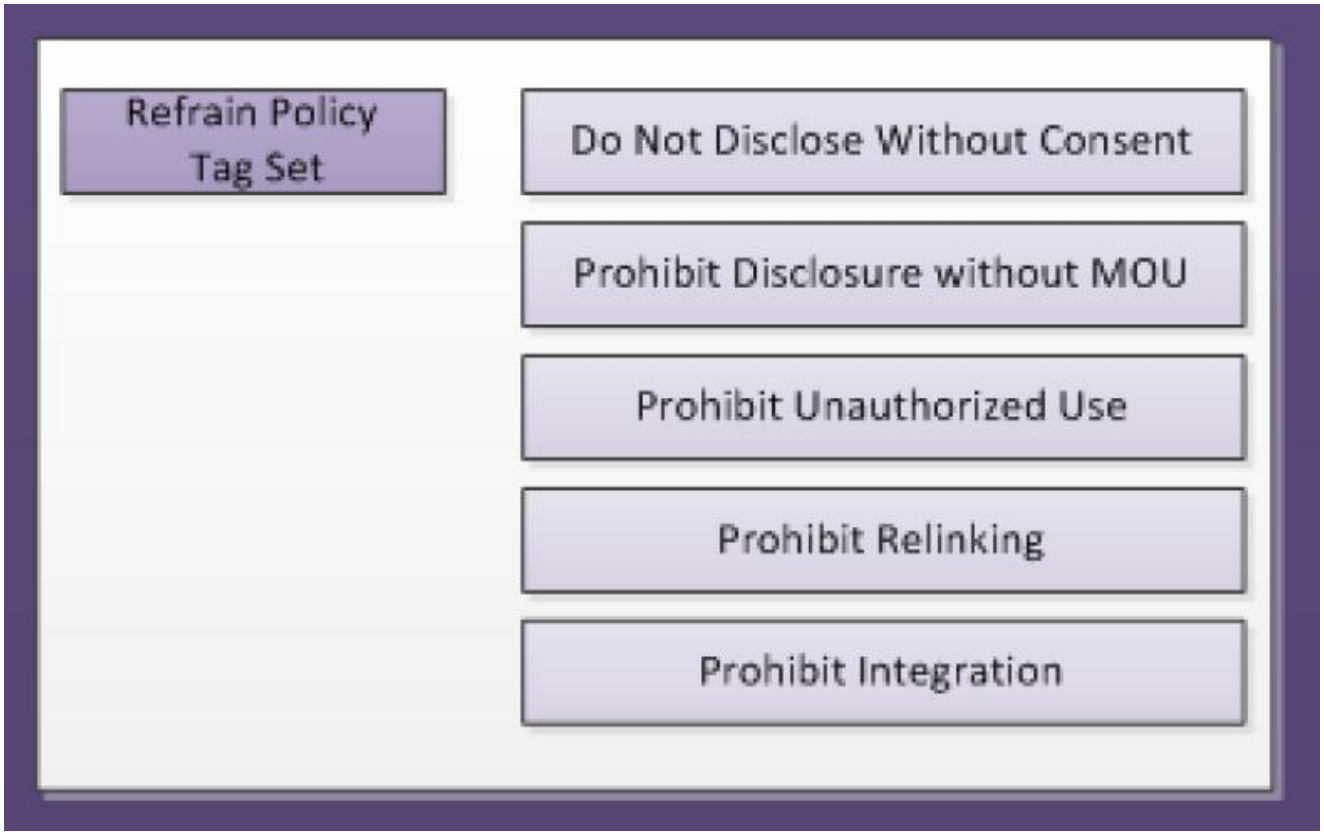
HCS Security Label Field Usage Notes
Field 5: Handling Caveats – Obligation



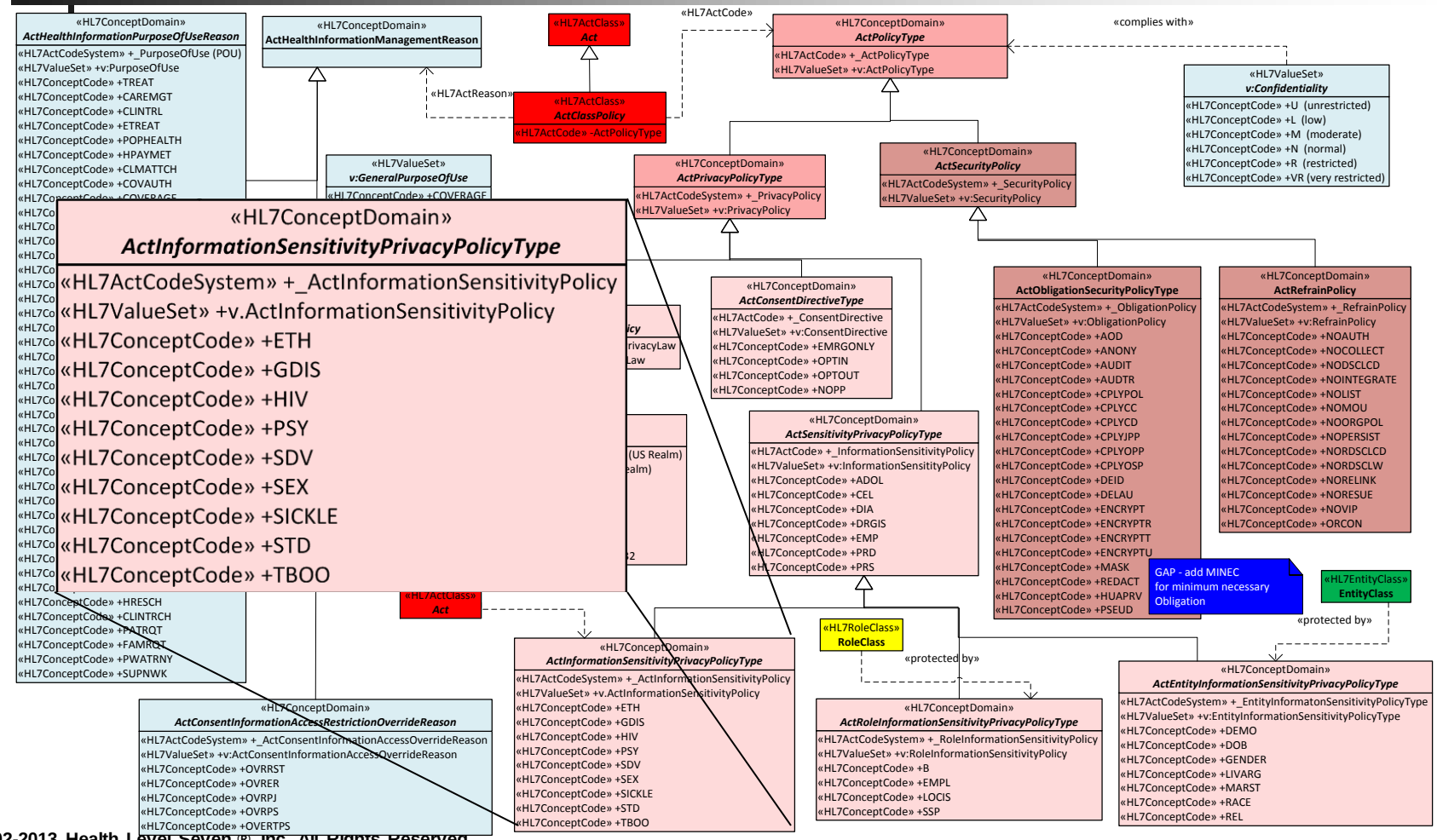
HCS Security Label Field Usage Notes
Field 5: Handling Caveats – Purpose of Use



HCS Security Label Field Usage Notes
Field 5: Handling Caveats – Refrain Policy



HL7 Data Tags



Applied Example: FHIR Connectathon Security Labeling Services Virtual Demonstration

Fast Healthcare Interoperability Resources (FHIR, pronounced "Fire") defines a set of "Resources" that represent granular clinical concepts. The resources can be managed in isolation, or aggregated into complex documents.

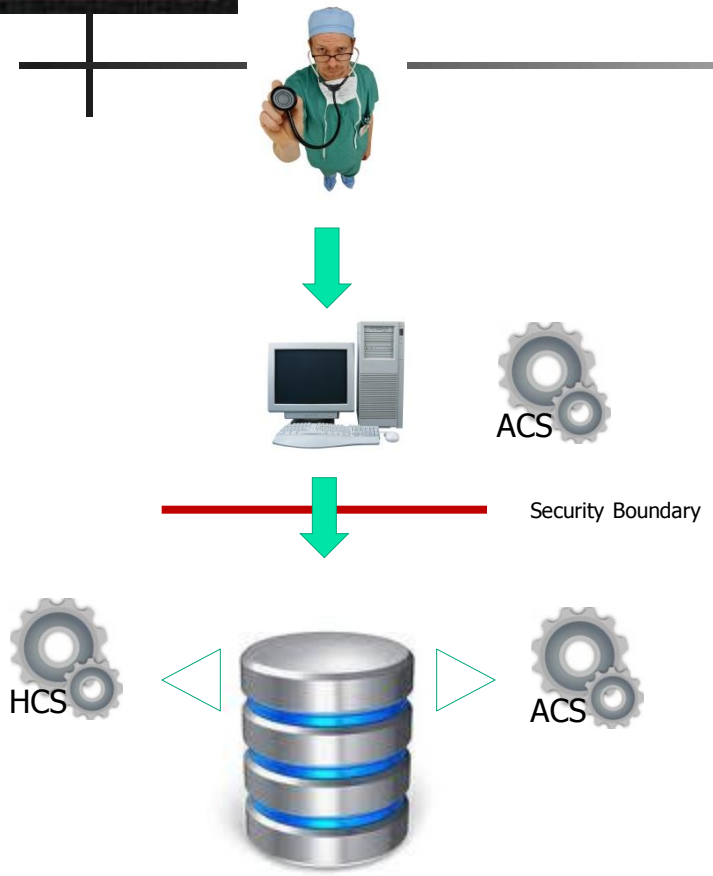
These clinical concepts require an corresponding set of granular segmentation concepts *that sequester FHIR resources through labeling.*

Health Level Seven (HL7) 27TH Annual Plenary & Working Group Meetings
September 21-22, 2013 Hyatt Regency Cambridge (Boston)

- Integration with HCS – Security Labeling Services
- DS4P Use Cases – Share All, Share Partial, Breakglass
- VA/DoD iEHR Use Cases

FHIR Connectathon Security Labeling Services Virtual Demonstration

FHIR Security and Healthcare Classification System



The consumer that is using a healthcare related system.

The client application this user is using (application, mobile App, website, etc).

ACS
The security system that authenticates and/or authorizes the user.

HCS
The Healthcare Classification System that applies security Labels, and segments the resultant resource stream.

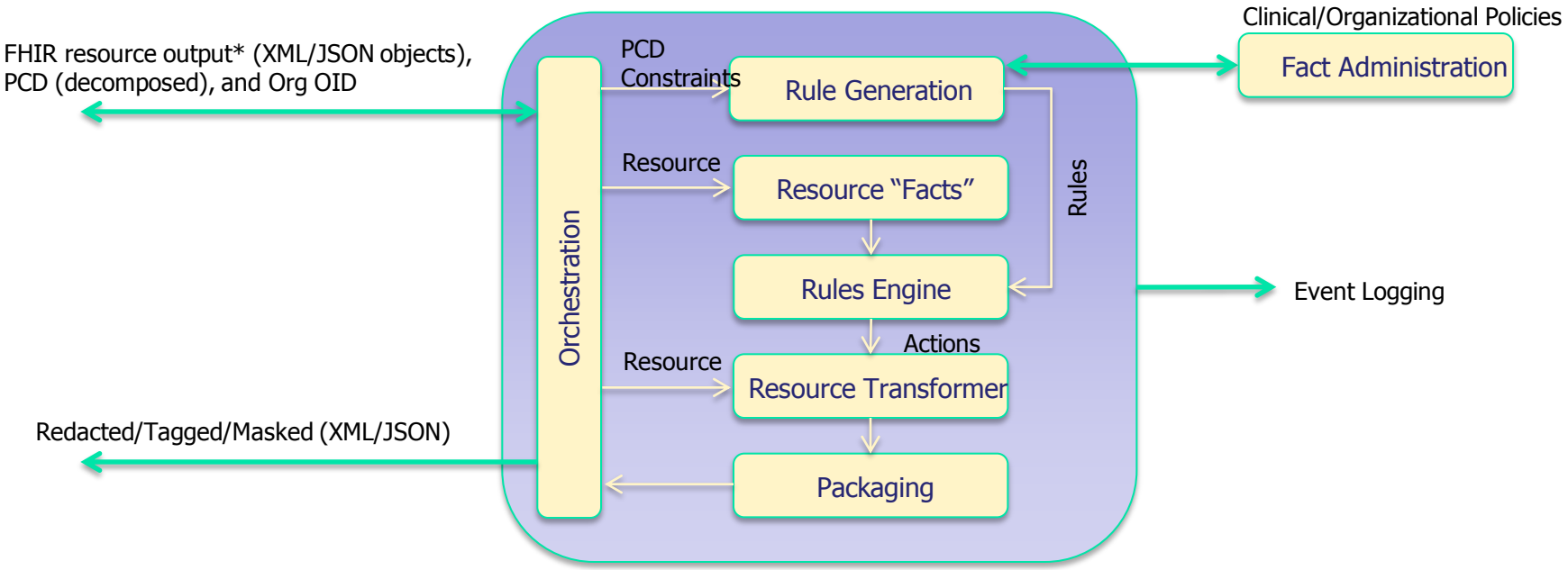
The Clinical/Healthcare repository.

Draft

VA HEALTH CARE Defining EXCELLENCE in the 21st Century

FHIR Connectathon Security Labeling Services Virtual Demonstration

HCS Security Labeling Services



Simplified View

VA HEALTH CARE Defining EXCELLENCE in the 21st Century

Privacy Tagged Summary Document

UNMASKED

Transformed C32

Summarization of episode note

RESTRICTED

Created On: January 9, 2013

Patient: Asample Patientone
14235 South St
Baltimore, Maryland, 21075
555-255-5454
MRN: PUI100010060001

Birthdate: May 10, 1971 **Sex:** Male

Guardian: **Next of Kin:**

Table of Contents

- Problems
- Medications

Problems **(RESTRICTED// HIV)**

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	N	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 **(NORMAL)**

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

MASKED

Transformed C32

Summarization of episode note

NORMAL

Created On: January 9, 2013

Patient: Asample Patientone
14235 South St
Baltimore, Maryland, 21075
555-255-5454
MRN: PUI100010060001

Birthdate: May 10, 1971 **Sex:** Male

Guardian: **Next of Kin:**

Table of Contents

- Problems
- Medications

Problems **(NORMAL)**

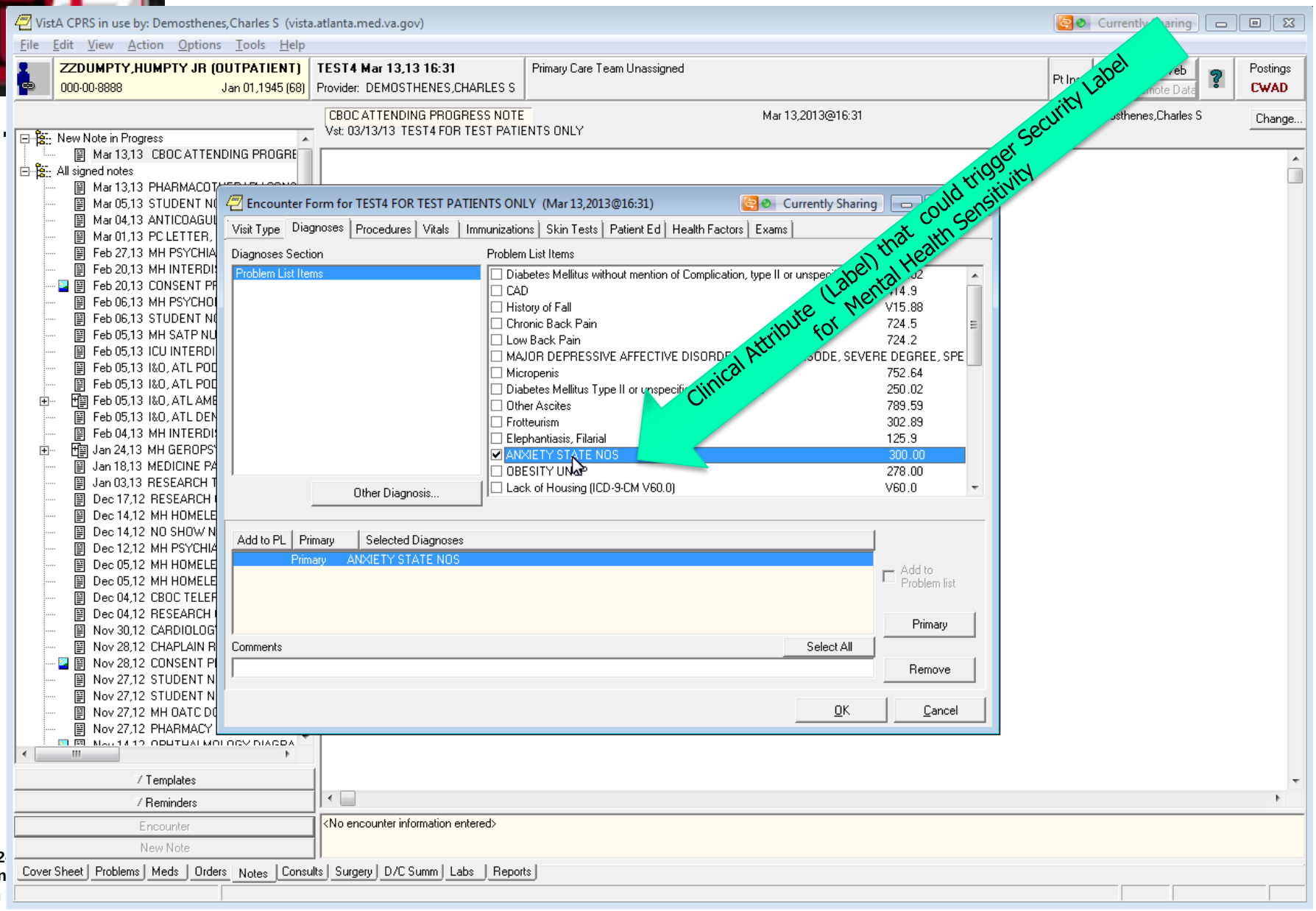
Problem Name	Problem Code	Class	Problem Status
[MASKED ENTRY]			
Diabetes mellitus type 2 (disorder)	44054006	N	Resolved
Asthma (disorder)	195967001	N	Inactive
Coronary artery atheroma (disorder)	67682002	N	Inactive
Hyperlipidemia (disorder)	55822004	N	Active
Hypertension associated with transplantation (disorder)	427889009	N	Active

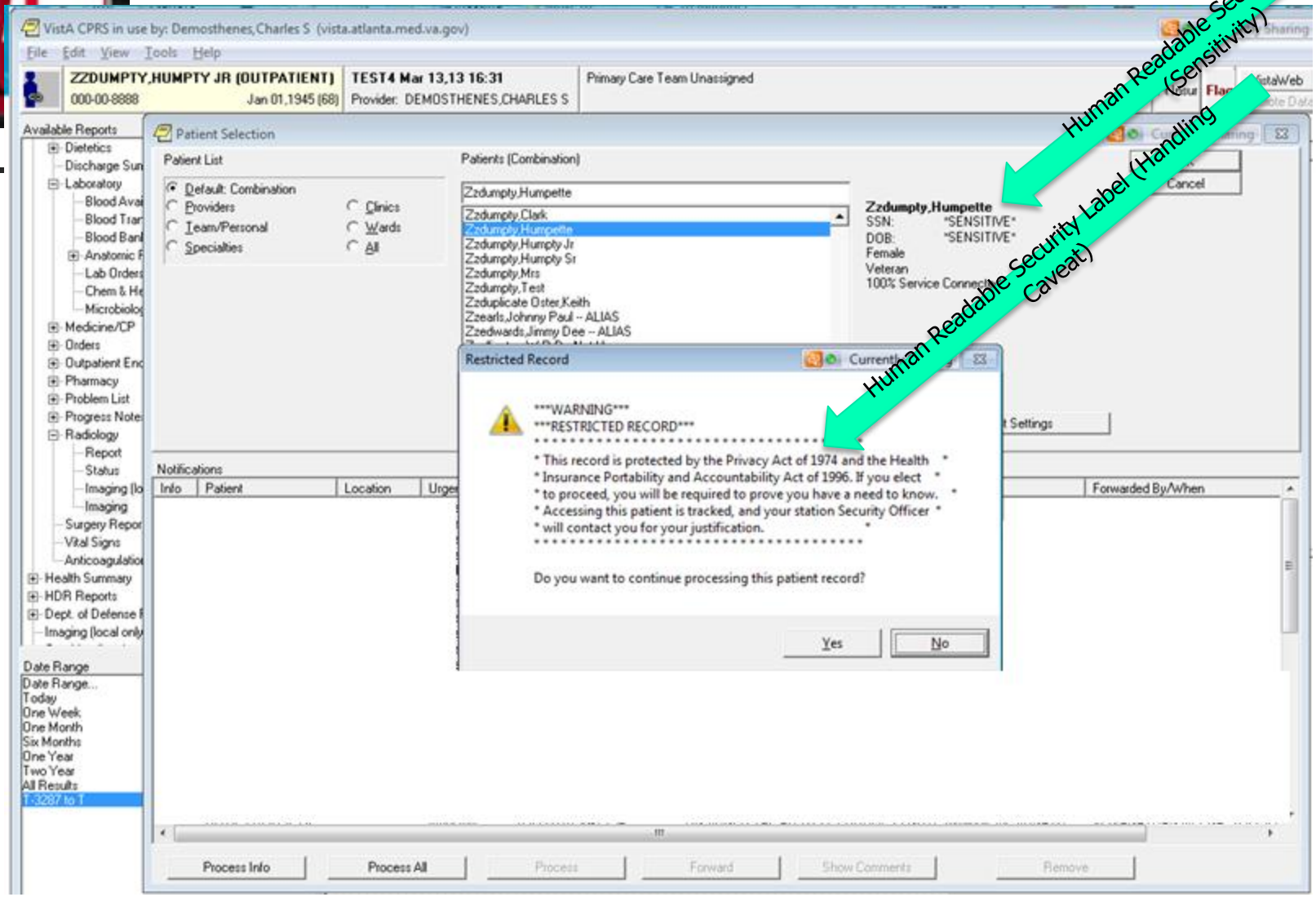
Medications **(NORMAL)**

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

Secret Key
User Authorization

Clinical Attributes





Summary

Clinical Benefits

- **Improves clinician ability to search patient records**
- **Essential for Cognitive Support, Knowledge Management, and Clinical Decision Support**
- **More robust Records Management capabilities**
- **Improves ability to leverage encounter data for secondary uses such as research and quality improvement lab**

Privacy and Security Benefits

- **Application-level security services aligned with Clinical requirements**
- **Improves enforcement of patient preferences and organizational privacy policy**
- **Mitigates risk of unauthorized access or disclosure including breach**
- **Enables Coarse to Fine Grain Access Control by Clearance Attributes in addition to Roles**

Conclusion

- **Data segmentation and labeling provides a means for protecting specific elements of health information, both within an EHR and in broader electronic exchange environments, which can prove useful in implementing current legal requirements and honoring patient choice.**

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
- (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
- 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
- (OASIS XACML) Organization for the Advancement of Structured Information Standards eXtensible Access Control Markup Language (XACML) Version 2.0, 1 Feb 2005
- (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
- (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

HL7 Points of Contact

Security WG : **Mike Davis**, Mike.Davis@va.gov

US Department of Veterans Affairs

CBCC: **Richard Thoreson**, Richard.Thoreson@samhsa.hhs.gov

Substance Abuse and Mental Health Services Administration