



Implementation Guide for CDA Release 2.0

Privacy Consent Directive

Draft Standard for Trial Use

Levels 1, 2 and 3

Universal Realm

Second Ballot
May 2010

Co-Chair/Editor Richard Thoreson
Substance Abuse and Mental Health Services Administration
(SAMHSA)
Richard.Thoreson@samhsa.hhs.gov

Co-Chair Suzanne Gonzales-Webb
SAIC
SUZANNE.L.GONZALES-WEBB@saic.com

Primary Editor: Ioana Singureanu
Eversolve, LLC
ioana@eversolve.com

Co-Editor: Serafina Veraggi
Eversolve, LLC
serafina@eversolve.com

Technical Editor Anthony Sute
Eversolve, LLC
anthony@eversolve.com

Working Group also includes: Tom Davidson (SSA), Walter Suarez, MD, MPH (KP)

Acknowledgments

This ballot was produced and developed through the efforts of the Substance Abuse and Mental Health Services Administration (SAMHSA), the Department of Veterans Affairs (VA), and the Social Security Administration (SSA) with modeling support provided by Eversolve, LLC.

The co-editors appreciate the support and sponsorship of the HL7 Structured Documents Work Group (SDWG).

Finally, we acknowledge the foundational work by HL7 Version 3, the Reference Information Model (RIM), and the HL7 domain committees, especially Patient Care, and the work done on Clinical Document Architecture (CDA) itself. We also acknowledge the [IHE BPPC specification](#) as the precursor to this specification and HITSP TP 30 Manage Consent Directives Transaction Package. All these efforts were critical ingredients to the development of this ballot; the degree to which this ballot reflects these efforts will foster interoperability across the spectrum of health care.

SNOMED CT[®] is a registered trademark of the International Health Terminology Standard Development Organisation (IHTSDO). LOINC[®] is a registered United States trademark of Regenstrief Institute, Inc.

Revision History

Rev	Date	By Whom	Changes	Notes
ballot 1.0	19 October 2009	Ioana Singureanu	Initial ballot draft	
2.0	22 February 2010	Serafina Versaggi	Ballot comments applied to document	
2.0	19 March 2010	Ioana Singureanu	Template changes and revised XML snippets	
2.0	28 March 2010	Serafina Versaggi	Outstanding ballot comments applied	
2.0	30 March 2010	Ioana Singureanu	Applied templated identifiers, updated samples	
2.0	31 March 2010	Serafina Versaggi	Additional edits, including fix to Figure 21	
2.1	24 May 2010	Ioana Singureanu, Anthony Sute	Apply ballot persuasive comments, convert document format to fix publication to PDF	
2.2	15 Sept 2010	Serafina Versaggi	May 2010 Ballot Reconciliation and added Security Considerations section 1.9	

Table of Contents

1	INTRODUCTION.....	8
1.1	Purpose.....	8
1.2	Audience.....	9
1.3	Approach.....	9
1.4	Organization of This Guide.....	10
1.5	Use of Templates.....	11
1.5.1	Originator Responsibilities: General Case.....	11
1.5.2	Recipient Responsibilities: General Case.....	11
1.6	Conventions Used in This Guide.....	12
1.6.1	Conformance Requirements.....	12
1.6.2	Vocabulary Conformance.....	12
1.6.3	Keywords.....	12
1.6.4	XML Examples.....	12
1.7	Glossary of Terms.....	13
1.8	Scope.....	13
1.8.1	Levels of Constraint.....	15
1.8.2	Future Work.....	16
1.9	Security Considerations.....	17
2	CDA HEADER CONSTRAINTS.....	18
2.1	ClinicalDocument Constraints Specific to Privacy Consent Directives.....	18
2.2	ClinicalDocument Attributes and Elements.....	18
2.2.1	ClinicalDocument/templateId.....	18
2.2.2	ClinicalDocument/recordTarget.....	19
2.2.3	ClinicalDocument/author.....	19
2.2.4	ClinicalDocument/custodian.....	20
2.2.5	ClinicalDocument/informationRecipient.....	21
2.2.6	ClinicalDocument/legalAuthenticator.....	21
2.2.7	ClinicalDocument/authenticator.....	22
2.2.8	ClinicalDocument/documentationOf/serviceEvent.....	22
2.2.9	ClinicalDocument/relatedDocument.....	23
2.3	Rendering Header Information for Human Presentation.....	23
3	BODY.....	25
3.1	Section Descriptions.....	25
3.2	Required Sections.....	25

3.2.1	Privacy Consent Directive Details Section.....	26
3.3	Optional Sections.....	32
3.3.1	Signatures	32
4	REFERENCES.....	34
APPENDIX A —	ACRONYMS AND ABBREVIATIONS.....	35
APPENDIX B —	TEMPLATE IDS IN THIS GUIDE	36
APPENDIX C —	PRIVACY CONSENT DIRECTIVE REQUIREMENTS	37
APPENDIX D —	GENERAL HEADER CONSTRAINTS COMPARISON	38

Table of Figures

Figure 1: Derivation Approach	10
Figure 2: ClinicalDocument example	13
Figure 3: Composite Privacy Consent Directive Domain Analysis	15
Figure 4: Future Work	16
Figure 5: Clinical Document/general header constraints, templateId example	18
Figure 6: ClinicalDocument Privacy Consent Directive header example.....	19
Figure 7: ClinicalDocument/documentationOf/recordTarget example.....	19
Figure 8: ClinicalDocument/documentationOf/author example.....	20
Figure 9: ClinicalDocument/documentationOf/custodian example.....	21
Figure 10: ClinicalDocument/informationRecipient example.....	21
Figure 11: ClinicalDocument/documentationOf/legalAuthenticator example.....	22
Figure 12: ClinicalDocument/documentationOf/serviceEvent example.....	23
Figure 13: ClinicalDocument/relatedDocument example.....	23
Figure 14: Privacy Consent Directive Header rendered – example.....	24
Figure 15: Privacy Consent Directive Details Section example.....	26
Figure 16: Privacy Consent Directive Details Entry example.....	27
Figure 17: Information Receipt example.....	27
Figure 18: Information Receipt example.....	28
Figure 19: Action/Operation example.....	29
Figure 20: Information Type and Sensitivity component.....	30
Figure 21: Privacy Policy Reference and Obligation component.....	31
Figure 22: Privacy Consent Section example.....	32
Figure 23: Signatures Section example.....	33
Table 1: TemplateIds in This Guide.....	36
Table 2: Comparison of Privacy Consent Directive IG and CDA General Header Constraints ..	38

1 INTRODUCTION

1.1 Purpose

The purpose of this document is to describe constraints on the Clinical Document Architecture Release 2 (CDA R2) header and body elements used to express Privacy Consent Directive documents.

Privacy policies define how Individually Identifiable Health Information (IIHI) is to be collected, accessed, used and disclosed. A Privacy Consent Directive is a record of a client's (e.g., patient, consumer) health information privacy policy. A Privacy Consent Directive grants or withholds authorization to collect, access, use, or disclose IIHI about the client. A client may author/publish their privacy preferences as a self-declared Privacy Consent Directive. Effective Privacy Consent Directives are a bilateral agreement between the client and an individual/organization that is in accord with law, regulation and organizational policies with regard to their content. In addition, Privacy Consent Directives provide the ability for a healthcare client to delegate authority to a Substitute Decision Maker who may act on behalf of that individual.

The CDA R2 IG for Privacy Consent Directives provides support for alternative representations for expressing health information privacy consent directives in a standard form for the exchange of privacy policies that can be enforced by consuming systems (e.g., scanned documents, computable structured entries).

The implementation guide also supports backward compatibility by incorporating the IHE Basic Patient Privacy Consents (BPPC) mechanism of acknowledging a Privacy Policy identifier and expands this with privacy policy attributes captured in the CDA document according to this CDA-IG specification. This guide allows for the capture of a scanned document in the `structuredBody` of a CDA document to support manual interpretation of the meaning of the privacy consent directive as well as to support the capture of a client's wet signature.

This guide supports sending a computable representation of privacy consent directives using structured entries based on a mapping of the [HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive, Draft Standard for Trial Use \(DSTU\) Release 2](#) (CPCD DAM) to HL7 RIM attributes, or by using standard access control markup languages (XACML, XrML and others). It is expected that other SDOs will use the Privacy domain analysis model to create profiles (e.g., OASIS Cross-Enterprise Security and Privacy Authorization (XSPA) Technical Committee) and that for encoding capabilities, formal policy languages will be used.

Five categories of Privacy Consent Directives are described in the Office of the National Coordinator for Health Information (ONC) Consent Directives Document released March 31, 2010, and include the following US-specific "Core consent options" for electronic exchange:

- **No consent:** Health information of patients is automatically included—patients cannot opt out;
- **Opt-out:** Default is for health information of patients to be included automatically, but the patient can opt out completely;

- **Opt-out with exceptions:** Default is for health information of patients to be included, but the patient can opt out completely or allow only select data to be included;
- **Opt-in:** Default is that no patient health information is included; patients must actively express consent to be included, but if they do so then their information must be all in or all out; and
- **Opt-in with restrictions:** Default is that no patient health information is made available, but the patient may allow a subset of select data to be included.

1.2 Audience

The audience for this document includes software developers, system architects, policy makers and analysts responsible for implementation of secure Electronic Health Record (EHR) systems, Personal Health Record (PHR) systems, dictation/transcription systems, and document management applications; and local, regional, and national health information exchange networks that wish to create and/or process CDA documents developed according to this specification.

1.3 Approach

This specification is intended to provide a CDA R2 representation of the Privacy Consent Directive structure described in the [HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive, Draft Standard for Trial Use \(DSTU\) Release 2](#) (CPCD DAM) DSTU. During the trial period, the implementers will be using a CDA R2 with the expectation that the final representation of this implementation guide will target CDA Release 3.

The approach taken in the development of this specification was to leverage existing specifications and terminology standards to create a backwards-compatible document specification graphically described in Figure 1.

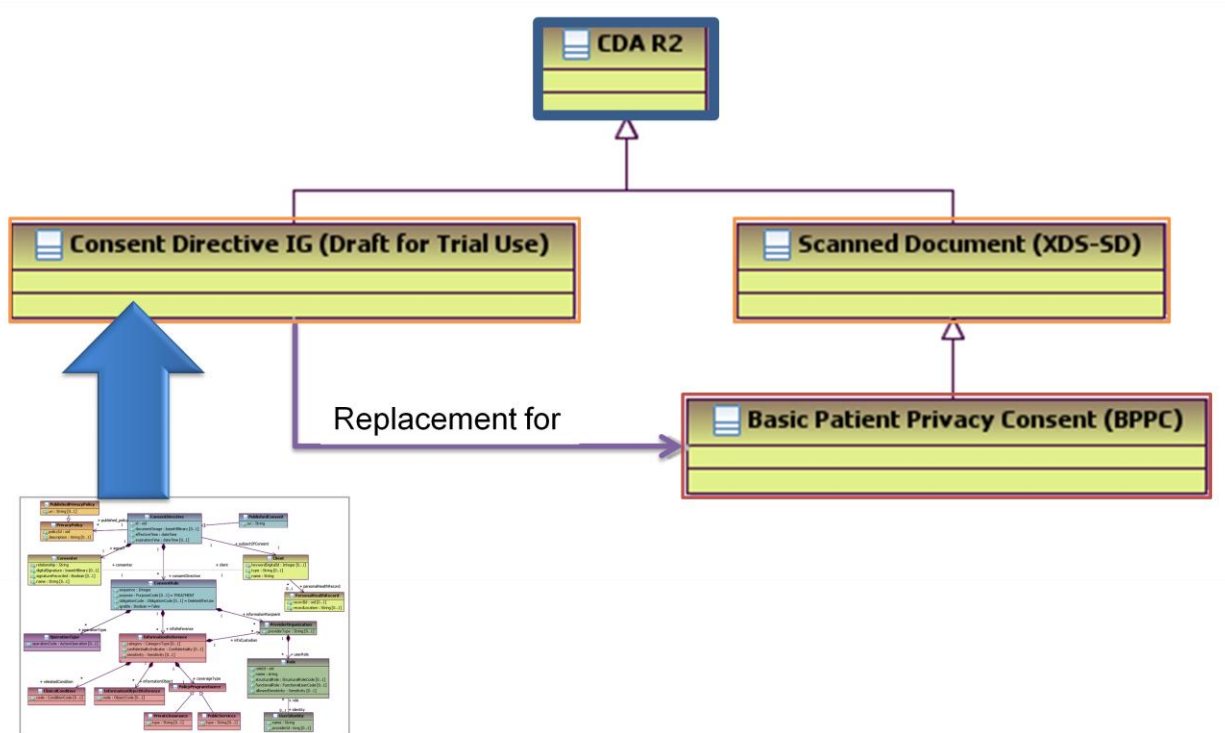


Figure 1: Derivation Approach

The following list of specifications was used in the creation of this implementation guide:

- [Clinical LOINC® document and section codes](#)
- [Health Information Technology Standards Panel \(HITSP\) Constructs](#), Transaction Package (TP30) - Manage Consent Directives
- [HL7 Clinical Document Architecture, Release 2 Normative Edition 2005](#),
- [Integrating the Healthcare Enterprise \(IHE\) Profiles](#), including the content profiles within Cross-Enterprise Sharing Document (XDS) Sharing Scanned Documents Integration Profile (XDS-SD) and Basic Patient Privacy Consents (BPPC) that is based on it
- [HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive, DSTU Release 2 \(CPCD DAM\)](#) – <http://www.hl7.org/dstucomments/>
- Sample privacy consent authorization forms provided by the state and federal agencies (e.g., SAMHSA, SSA ,VHA, Sate of New York, State of California, British Columbia)

1.4 Organization of This Guide

This Implementation Guide is based on the [CPCD DAM](#) and the content of the Domain Analysis Model is referenced throughout this Implementation Guide. This CDA R2 Implementation Guide for Privacy Consent Directives is a DSTU and along with the CPCD DAM, both are on track to become normative after a trial period. They will be subject to change under the policies for DSTU as specified by the [HL7 Governance and Operations Manual](#).

This guide is organized into the following major sections:

- CDA R2 Header Constraints
- CDA R2 Header – Privacy Consent Directive-Specific Constraints
- Body (structuredBody) – Privacy Consent Directive-Specific Constraints

The structuredBody representation of a CDA R2 Privacy Consent Directive document is described in [3.1 – Section Descriptions](#). This section of the document is organized to provide:

- A narrative description of the privacy consent directive
- A computable representation of the privacy consent directive using widely implemented access control markup (e.g., XrML, XACML, etc.)
- Structured entries based on the [CPCD DAM](#)
- CDA R2 constraints for each of these business-specific constraints

1.5 Use of Templates

When valued in an instance, the template identifier signals the imposition of a set of template-defined constraints. The value of this attribute provides a unique identifier for the template in question.

In this specification, all templates are traceable to use case and information requirements documented in the CPCD DAM.

1.5.1 Originator Responsibilities: General Case

A system that originates a document may apply a `templateId` to assert conformance with a particular template. The template allows the receiving system to validate the content of a document against the constraints specified.

This implementation guide asserts when `templateIds` are required for conformance.

1.5.2 Recipient Responsibilities: General Case

A recipient may reject an instance that does not contain a particular `templateId` (e.g., a recipient looking to receive only CCD documents can reject an instance without the appropriate `templateId`).

A recipient may process objects in an instance document that do not contain a `templateId` (e.g., a recipient can process entries that contain `Observation` acts within a Privacy Consent Details section, even if the entries do not have `templateIds`).

If an object does not have a `templateId`, a recipient shall not report a conformance error about a failure to conform to a particular template on classes that do not claim conformance to that template and that are not required to be conformant by other templates.

Depending on the type of service agreement between parties, the receivers of a CDA privacy consent directive instance have an obligation to abide by the client's privacy policy set forth in the privacy consent directive.

1.6 Conventions Used in This Guide

1.6.1 Conformance Requirements

The conformance statements are numbered and listed within the body of the DSTU as follows:

CONF-ex1: Conformance requirements original to this DSTU are numbered CONF-CD1, CONF-CD2, etc.

1.6.2 Vocabulary Conformance

Formalisms for value-set constraints are based on the latest recommendations from the HL7 Vocabulary Committee. Value-set constraints can be “**STATIC**,” meaning that they are bound to a specified version of a value set, or “**DYNAMIC**,” meaning that they are bound to the most current version of a value set or coding system. A simplified constraint is used when binding is to a single code.

Syntax for vocabulary binding to **DYNAMIC** or **STATIC** value sets:

A (pathname of coded element) element (**SHALL** | **SHOULD** | **MAY**) be present where the value of (pathname of coded element) is selected from Value Set valueSetOID localValueSetName [**DYNAMIC** | **STATIC** (valueSetEffectiveDate)].

CONF-ex2: A code element **SHALL** be present where the value of @code is selected from Value Set 2.16.840.1.113883.19.3 LoincDocumentTypeCode **DYNAMIC**.

CONF-ex3: A code element **SHALL** be present where the value of @code is selected from Value Set 2.16.840.1.113883.19.3 LoincDocumentTypeCode **STATIC** 20061017.

Syntax for vocabulary binding to a single code:

A (pathname of coded element) element (**SHALL** | **SHOULD** | **MAY**) be present where the value of (pathname of coded element) is code [displayName] codeSystemOID [codeSystemName] **STATIC**.

CONF-ex4: A code element **SHALL** be present where the value of @code is 34133-9 Summarization of episode note 2.16.840.1.113883.6.1 LOINC **STATIC**.

1.6.3 Keywords

The keywords **SHALL**, **SHALL NOT**, **SHOULD**, **SHOULD NOT**, **MAY**, and **NEED NOT** in this document are to be interpreted as described in the [HL7 Version 3 Publishing Facilitator's Guide](#):

1.6.4 XML Examples

XML examples appear in various figures in this document in this monospace font. Portions of the XML content may be omitted from the content for brevity, marked by an ellipsis (...) as shown in the example below.

Figure 2: ClinicalDocument example

```
<ClinicalDocument xmlns='urn:h17-org:v3'>
  ...
</ClinicalDocument>
```

1.7 Glossary of Terms

Client

A client is a person who may receive or has received healthcare services in the past. Patient is a role played by a client in the context of a health care encounter.

Consent

Within the scope of this document, Consent refers to any client instructions that declare their preferences with respect to health care privacy policies.

Individually Identifiable Health Information (IIHI)

For the purposes of this document, IIHI refers to health data that is transmitted by or maintained in electronic media or any other form or medium that can be uniquely associated with an individual. The use of this term is without respect to any jurisdiction.

Privacy Consent Directive

A client's instructions regarding consent to collect, use and/or disclose IIHI.

Consenter

The person who consents to the collection, use or disclosure of a Client's IIHI. The Consenter may be the client or a Substitute Decision Maker (SDM).

1.8 Scope

This specification applies to privacy consent directives intended to protect health information maintained in electronic health records (EHRs), personal health records (PHRs), Health Information Exchange systems (HIEs) and other forms of electronics collection and maintenance of health information.

The scope of this project is to specify a Privacy Consent Directive in a format that may be used to sign the privacy consent as well as to allow information systems and specific rule engines to decode the assertions contained therein.

This implementation guide is a conformance profile, as described in the [Refinement and Localization](#) section of the HL7 Version 3 standards. The base standard for this implementation guide is the [HL7 Clinical Document Architecture, Release 2.0](#). As defined in that document, this implementation guide is both an annotation profile and a localization profile. CDA R2 is not fully described in this guide, so implementers must be familiar with the requirements of the base specification.

As an annotation profile, portions of this guide summarize or explain the base standard; therefore, some requirements stated here originate not in this DSTU but in the base specification. Requirements that do not add further constraints to the base standard and that can be validated through CDA R2 XML Schema Description and conform to

the CDA R2 General Header constraints do not have corresponding conformance statements in this DSTU.

This Privacy Consent Directive Implementation Guide provides a mechanism to record a client's health information privacy consent(s) and to exchange those privacy consent directives with entities that are custodians of the client's health records including Individually Identifiable Health Information (IIHI).

This DSTU implementation guide for Privacy Consent Directives is the second such implementation guide intended to exchange health information privacy preferences for clients as privacy consent authorizations. The current specification, BPPC allows only for binary acknowledgement of an externally identified and defined policy of no specific format and does not provide the ability to encode policy in a computable format. Stakeholders however, require support for a computable representation of client privacy consents. This specification includes the requirements specified in the CPCD DAM. Additional constraints on CDA R2 header and body elements used in a BPPC Document are defined by this specification, including general header constraints for consenter and information recipient as documented in the [CPCD DAM](#) graphically presented in Figure 3 below. (See also [2 CDA Header Constraints](#)).

This implementation guide specifies a structure for formatting client health information privacy preferences and is only intended to describe the business requirements and semantics of the information required to specify a Privacy Consent Directive (Enterprise and Information viewpoints). This guide does not provide an Engineering point of view and is not intended to describe a policy language.

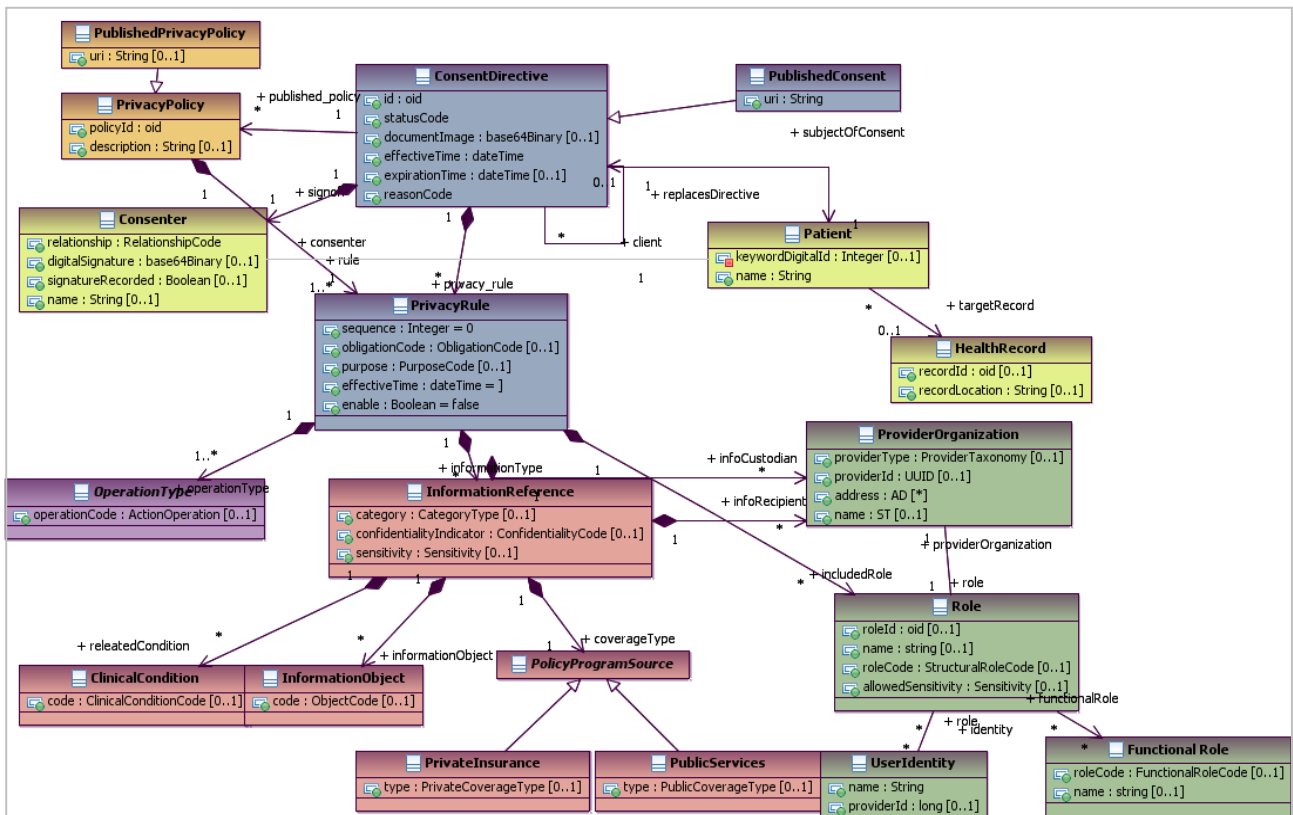


Figure 3: Composite Privacy Consent Directive Domain Analysis

Where no constraints are stated in this guide, the Privacy Consent Directive document instances are subject to, and are to be created in, accordance with the base CDA R2 specification. For instance, where the CDA R2 declares an attribute to be optional and the Privacy Consent Directive specification (or any of its parent specifications) contains no additional constraints, that attribute remains optional for use in a Privacy Consent Directive instance.

1.8.1 Levels of Constraint

This DSTU identifies the required and optional health information within a privacy consent document. The DSTU specifies three levels of conformance requirements:

- Level 1 requirements specify constraints upon the CDA header and the content of the document. Their use is required.
- Level 2 requirements specify constraints at the section level of the `structuredBody` of the `ClinicalDocument` element of the CDA document. Their use is required.
- Level 3 requirements specify constraints at the entry level within a section. Their use is optional.

Note that these levels are rough indications of what a recipient can expect in terms of machine-processable coding and content reuse. They do not reflect the level or type of health information within the privacy consent; many additional distinctions in reusability could be defined. The CDA R2 specification consists of a single CDA XML

Schema, and the architecture arises from the ability to apply one or more of a hierarchical set of HL7 Templates which serve to constrain the richness and flexibility of CDA. See CDA R2 section 1.2.2 for a full description of the notion of levels in CDA R2.

1.8.2 Future Work

During the effort to map the [CPCD DAM](#) to a CDA R2 document, the project team identified several instances where Privacy Consent Directive concepts could not be mapped to a corresponding class or attribute in a CDA R2 document structure. These issues were addressed by defining workarounds within CDA R2 instead of employing CDA R2 extensions. For example, there is no way include an electronic signature (e.g., digital signature, scanned wet signature) with the identity of an author, authenticator, or legal authenticator in the document header that is often mandatory for legally binding documents. This is because CDA R2 does not allow the RIM element, **Participation.signatureText** to be used in the header to represent **legalAuthenticator**, authenticator, etc. The workaround specified in this implementation guide uses **observationMedia** to specify a "Signature" section in the structured body of a CDA document.

If approved in May 2010, this CDA R2 specification will be available for a trial period of two years or until the Normative specification is issued to replace it.

Extension requirements to support Privacy Consent Directive were submitted to the Structured Documents Work Group in the form of CDA R3 enhancement proposals. The CDA R3 document model is expected to be approved in May or September 2011. If approved, the project team will then revise this Implementation Guide by mapping the missing Privacy Consent Directive concepts to the CDA R3 specification. A normative release of this specification will then be issued as soon as the CDA R3 model becomes available.

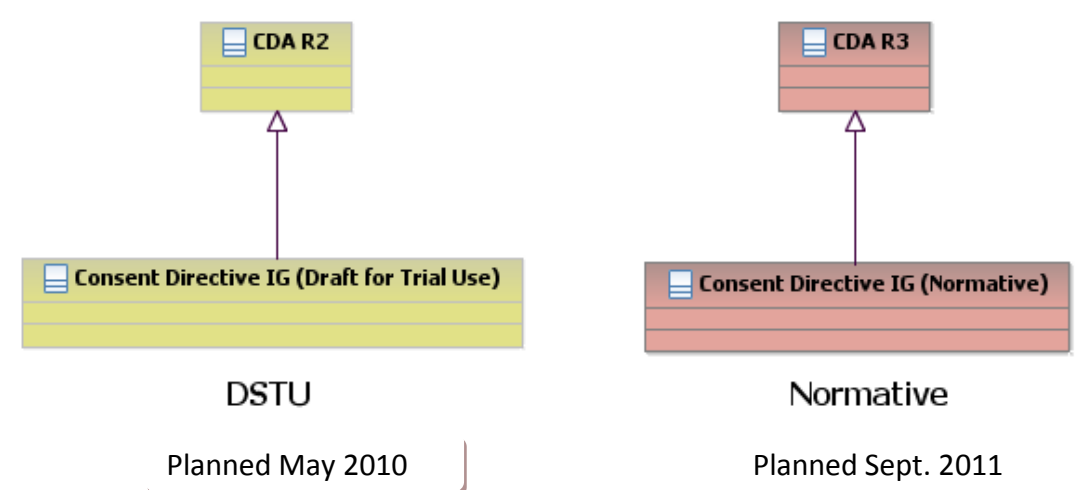


Figure 4: Future Work

1.9 Security Considerations

There are times when a client may wish to constrain sensitive healthcare topics (e.g., HIV status). To encode this restriction to a policy in a CDA R2-Privacy Consent document instance might be seen as a strong indicator that the client is positive for these sensitive healthcare topics. Thus the CDA R2 Privacy Consent document instance itself would need to be similarly constrained. There is nothing more that the HL7 specification can do on this topic, so it is itemized here as a risk that should be mitigated in implementation or deployment. There are a few ways to handle this:

- a) The sensitive health topics that a patient may want to block could be blocked by default. Thus those clients who are not sensitive to these health topics could indicate that they do not want these topics to be restricted. This will work well if the number of clients that allow unrestrained access to the sensitive topics is a small number, but as this number of clients gets larger, the same problem will exist.
- b) The CDA R2 Privacy Consent document instance that contains these constraints could be identified with the confidentialityCode appropriate for the environment. Typically documents that include sensitive topics or for which there are other reasons to restrict their access would be labeled with a higher data classification such as “R” for Restricted. Since there are many reasons for a document (object) to be identified as Restricted, this higher definition of a data classification will restrict access to the CDA R2 Privacy Consent document instance without exposing the specific reason. Use of the HL7 confidentialityCode value set ‘confidentialityByInfoType’ codes are specifically concerning.
- c) The CDA R2 Privacy Consent document instances could all be restricted as a class of document to very specific permissions/roles, e.g., only the Privacy Office and Access Control engine. In this way, no CDA R2 Privacy Consent documents would be viewable by clinicians.

2 CDA HEADER CONSTRAINTS

The CDA R2 Implementation Guide for Privacy Consent Directives DSTU defines a set of general constraints against the CDA R2 header. Conformance to this DSTU carries with it an implicit adherence to Level 1 which asserts header element constraints.

Conformance to the DSTU at Level 1, whether specified or implicit, asserts header element constraints but allows a non-XML body or an XML body that may or may not conform to additional templates defined herein. Likewise, conformance to this DSTU at Level 2 does not require conformance to entry-level templates, but does assert conformance to header- and section-level templates. In all cases, required privacy clinical content must be present. For example, a CDA R2 Discharge Summary carrying the `templateId` that asserts conformance with Level 1 may use a PDF or HTML format for the body of the document that contains the required health information privacy consent.

A Privacy Consent Directive is enforced if the `ClinicalDocument/statusCode` is set to “active” or if it is revoked, the `ClinicalDocument/statusCode` code is set to “aborted”. If the Consent Directive is expired, the `ClinicalDocument/statusCode` is set to “completed”.

2.1 *ClinicalDocument Constraints Specific to Privacy Consent Directives*

This section describes the `ClinicalDocument` constraints specific to Privacy Consent Directive Documents.

CONF-CD-1: A document conforming to the CDA R2 General Header template **SHALL** include the `ClinicalDocument/templateId` “2.16.840.1.113883.10.20.3”.

Figure 5: Clinical Document/general header constraints, templateId example

```
<?xml version="1.0" encoding="UTF-8"?>
<ClinicalDocument xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
classCode="DOCCLIN" moodCode="EVN">
  <!-- General Header Constraints -->
  <templateId root="2.16.840.1.113883.10.20.3"/>
  <!-- Privacy Consent Directive Header Constraints -->
  <templateId root="2.16.840.1.113883.3.445.1"/>
  <!-- Document instance id-->
```

2.2 *ClinicalDocument Attributes and Elements*

2.2.1 /ClinicalDocument/templateId

Conformant Privacy Consent Directives must carry the document-level `templateId` asserting conformance with this DSTU as well as the `templateId` for the CDA R2 General Header Constraints template.

CONF-CD-2: `ClinicalDocument/templateId` element **SHALL** be present with the value “2.16.840.1.113883.3.445.1”.

Figure 6: ClinicalDocument Privacy Consent Directive header example

```
<ClinicalDocument xmlns="urn:hl7-org:v3"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
classCode="DOCCLIN" moodCode="EVN" >
  <!-- Privacy Consent Directive DSTU Header-->
  <realmCode code="US"/>
  <typeId root="2.16.840.1.113883.1.3" extension="09230"/>
  <!-- General Header Constraints -->
  <templateId root="2.16.840.1.113883.10.20.3"/>
  <!-- Privacy Consent Directive Header Constraints -->
  <templateId root="2.16.840.1.113883.3.445.1"/>
  <!-- Document instance id-->
  <id root="1.3.6.4.1.4.1.2835.888888" extension="221"/>
  <code code="57016-8" codeSystem="2.16.840.1.113883.6.1"
codeSystemName="LOINC"
displayName="Privacy Policy Acknowledgement Document"/>
  <title representation="TXT"
mediaType="text/plain"> Privacy Consent Authorization</title>
  <effectiveTime value="200910262244+0500"/>
  <confidentialityCode code="N"/>
```

2.2.2 ClinicalDocument/recordTarget

Each Privacy Consent Directive must specify a healthcare client whose IIHI is affected by the privacy consent directive. The classes of Patient and patientRole describe the healthcare client whose IIHI is referenced in document.

Figure 7: ClinicalDocument/documentationOf/recordTarget example

```
<!-- Client/Record Target Reference-->
<recordTarget>
  <patientRole>
    <id extension="266666666" root="2.16.840.1.113883.3.933"/>
    <addr>
      <streetAddressLine>5555 Home Street</streetAddressLine>
      <city>Ann Arbor</city>
      <state>MI</state>
      <postalCode>99999</postalCode>
      <country>USA</country>
    </addr>
    <patient>
      <name>
        <prefix>Mrs.</prefix>
        <given>Susan</given>
        <family>Everyperson</family>
      </name>
      <administrativeGenderCode code="F" />
      <birthTime value="19600127"/>
    </patient>
  </patientRole>
</recordTarget>
```

2.2.3 ClinicalDocument/author

The author of the document (assignedAuthor) need not be the author of the policy (author). The document header may also identify the device used to scan the signed

hardcopy document that contains the privacy consent directive of the client (assignedAuthoringDevice). The following asserts conformance to the Privacy Consent Directive DSTU.

- CONF-CD-3:** ClinicalDocument/author element **SHALL** be present and specify a templateId of “2.16.840.1.113883.3.445.2”.
- CONF-CD-4:** ClinicalDocument/author/functionCode/ **MAY** be present to specify function/relationship of the author to the client who is the record target. This element may be used to specify the client’s relationship to the Substitute Decision Maker – if one is involved in the creation of the privacy consent directive.

Figure 8: ClinicalDocument/documentationOf/author example

```
<!-- Person and/or organization issuing the privacy consent directive form-->
<author>
  <templateId root="2.16.840.1.113883.3.445.2" />
  <functionCode code="POACON"
    displayName="healthcare power of attorney consent author"
    codeSystem="2.16.840.1.113883.1.11.19930"
    codeSystemName="ConsenterParticipationFunctionDecisionMaker"/>
  <time value="201003122244"/>
  <assignedAuthor>
    <id extension="11111111" root="1.3.5.35.1.4436.7"/>
    <assignedPerson classCode="PSN">
      <name>
        <given>Bernard</given>
        <family>Everyperson</family>
        <suffix>Sr.</suffix>
      </name>
    </assignedPerson>
    <representedOrganization>
      <id root="1.3.6.4.1.4.1.2835.2" extension="980983"/>
      <name>Level Seven Healthcare, Inc.</name>
      <telecom value="409-444-2353"/>
      <addr>
        <streetAddressLine>
          4444 Healthcare Drive
        </streetAddressLine>
        <city>Ann Arbor</city>
        <state>MI</state>
        <postalCode>99999</postalCode>
        <country>USA</country>
      </addr>
    </representedOrganization>
  </assignedAuthor>
</author>
```

2.2.4 ClinicalDocument/custodian

This element of the header identifies the custodian of the Privacy Consent Directive document as specified by CDA R2.

Figure 9: ClinicalDocument/documentationOf/custodian example

```
<!-- Information Custodian -->
<custodian>
  <assignedCustodian>
    <representedCustodianOrganization>
      <id root="1.3.6.4.1.4.1.2835.2" extension="980983"/>
      <name>Level Seven Healthcare, Inc.</name>
      <telecom value="409-444-2353"/>
      <addr>
        <streetAddressLine>4444 Healthcare Drive</streetAddressLine>
        <city>Ann Arbor</city>
        <state>MI</state>
        <postalCode>99999</postalCode>
        <country>USA</country>
      </addr>
    </representedCustodianOrganization>
  </assignedCustodian>
</custodian>
```

2.2.5 ClinicalDocument/informationRecipient

Information Recipient is used to specify the recipients of the Privacy Consent Directive. In the case of consultations and referrals, the Privacy Consent Directive recipient may be the same person/entity as the intended recipient of the client IHI that is disclosed as a result of the permission granted using the Privacy Consent Directive.

Figure 10: ClinicalDocument/informationRecipient example

```
<!-- Information Recipient -->
<informationRecipient typeCode="PRCP">
  <intendedRecipient classCode="ASSIGNED">
    <id root="1.3.6.4.1.4.1.2835.2" extension="7878"/>
    <addr>
      <streetAddressLine>999999 Healthcare Drive</streetAddressLine>
      <city>Ann Arbor</city>
      <state>MI</state>
      <postalCode>99999</postalCode>
    </addr>
    <informationRecipient classCode="PSN" determinerCode="INSTANCE">
      <name>
        <prefix>Mr.</prefix>
        <family>Hippocrates</family>
        <given>Harold</given>
      </name>
    </informationRecipient>
    <receivedOrganization classCode="ORG" determinerCode="INSTANCE">
      <id root="1.3.6.4.1.4.1.2835.2"/>
      <name>Ann Arbor Hospital</name>
    </receivedOrganization>
  </intendedRecipient>
</informationRecipient>
```

2.2.6 ClinicalDocument/legalAuthenticator

The legalAuthenticator is as defined in CDA. For a Privacy Consent Document this element may be either the client or their Substitute Decision Maker. If necessary, the Signatures section may provide the signature associated with the consenter's signature.

Figure 11: ClinicalDocument/documentationOf/legalAuthenticator example

```
<!-- Substitute Decision Maker or Client/Patient that signs the Privacy
Consent Directive -->
<legalAuthenticator contextControlCode="OP" typeCode="LA">
  <time value="20091025"/>
  <!-- Signed, signature on file-->
  <signatureCode code="S"/>
  <assignedEntity classCode="ASSIGNED">
    <id extension="11111111" root="1.3.5.35.1.4436.7"/>
    <assignedPerson classCode="PSN">
      <name>
        <given>Bernard</given>
        <family>Everyperson</family>
        <suffix>Sr.</suffix>
      </name>
    </assignedPerson>
  </assignedEntity>
</legalAuthenticator>
```

2.2.7 ClinicalDocument/authenticator

In some cases, a Privacy Consent Directive may identify and record the signature of a person who witnessed the consenter's signature. This may occur if the authenticator/consenter makes a mark instead of a signature.

2.2.8 ClinicalDocument/documentationOf/serviceEvent

Each Privacy Consent Directive may have an explicit duration by specifying the related service associated with issuing a privacy consent directive. The effective duration of a Privacy Consent Directive establishes the valid period for the privacy consent or authorization as directed by the client or Substitute Decision Maker. This constraint applies specifically for those jurisdictions where Privacy Consent Directives are issued for a pre-defined length of time.

The following asserts conformance to the Privacy Consent Directive DSTU.

- CONF-CD-5:** ClinicalDocument/documentationOf/serviceEvent/ element with a templateId of "2.16.840.1.113883.3.445.3" **MAY** be present.
- CONF-CD-6:** ClinicalDocument/documentationOf/serviceEvent/id element **MAY** be present.
- CONF-CD-7:** ClinicalDocument/documentationOf/serviceEvent/effectiveTime element **MAY** be present.
- CONF-CD-8:** ClinicalDocument/documentationOf/serviceEvent/effectiveTime/low/@value element **MAY** be present. It **MAY** be different than the value of the ClinicalDocument/effectiveTime/@value and represents the first time the Privacy Consent Directive takes effect.
- CONF-CD-9:** ClinicalDocument/documentationOf/serviceEvent/effectiveTime/high/@value element **MAY** be present to specify the date/time when the Privacy Consent Directive expires.
- CONF-CD-10:** ClinicalDocument/documentationOf/serviceEvent/code/@code attribute **SHALL** be present and indicates the OID of the externally

identified and defined privacy policy corresponding to the “Privacy Policy Acknowledgement Document”.

CONF-CD-11: ClinicalDocument/documentationOf/serviceEvent/code/@code System attribute **SHALL** be present and indicates the assigning authority of the externally identified and defined privacy policy corresponding to the “Privacy Policy Acknowledgement Document”.

CONF-CD-12: ClinicalDocument/documentationOf/serviceEvent/code/@code SystemName attribute **MAY** be present and be a descriptive text of the privacy policy being acknowledged.

Figure 12: ClinicalDocument/documentationOf/serviceEvent example

```
<!-- Effective time for the Privacy Consent Directive -->
<documentationOf typeCode="DOC">
  <serviceEvent moodCode="EVN">
    <templateId root="2.16.840.1.113883.3.445.3"/>
    <id root="2.16.840.1.113883.3.72.4.2.5"/>
    <code code="57016-8"
          codeSystem="2.16.840.1.113883.6.1"
          codeSystemName="LOINC"
          displayName="Privacy Policy Acknowledgement Document"/>
    <effectiveTime>
      <low value="20091020"/>
      <high value="20100221"/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
```

2.2.9 ClinicalDocument/relatedDocument

A Privacy Consent Directive may replace a previous (revoked) or expired Privacy Consent Directive. This element references a Privacy Consent Directive that is intended to be replaced by the current document.

Figure 13: ClinicalDocument/relatedDocument example

```
<!-- Previous Privacy Consent Directive Reference -->
<relatedDocument typeCode="RPLC">
  <parentDocument classCode="DOCCLIN" moodCode="EVN">
    <id root="1.3.6.1.4.1.19376.1.5.3.1.2.6" extension="2345"/>
  </parentDocument>
</relatedDocument>
```

2.3 Rendering Header Information for Human Presentation

Metadata carried in the header may already be available for rendering from clinical systems or other sources external to the document; therefore, there is no strict requirement to render directly from the document.

Good practice would recommend that the following be present whenever the document is viewed:

- Document title and document dates
- Service and date ranges indicating the period of the time the Privacy Consent Directive is valid
- Names of all persons along with their roles, participations, participation date ranges, identifiers, address, and telecommunications information
- Names of selected entities along with their roles, participations, participation date ranges, identifiers, address, and telecommunications information
- Legal and other authenticators (witnesses)
- Target Record Information regarding referenced client/patient

Figure 14: Privacy Consent Directive Header rendered – example

Patient:	Mrs. Susan Everyperson		
Date of birth:	January 27, 1960	Sex:	Female
Patient's Address:	5555 Home Street Ann Arbor, MI 99999, USA	Patient Id	266666666 2.16.840.1.113883.3.933
Document Id:	221 1.3.6.4.1.4.1.2835.888888		
Document Created:	October 26, 2009, 22:44 +0500		
Originator:	Bernard Everyperson, Sr., Level Seven Healthcare, Inc.Level Seven Healthcare, Inc.		
Entering clerk:	Ms. Joan Clerk on October 26, 2009, 22:44 +050		
Witness:	Ms. Assigned Amanda on October 25, 2009		
Intended recipient:	Mr. Harold Hippocrates, MD Ann Arbor Hospital		
Intended Recipient's Address:	999999 Healthcare Drive Ann Arbor, MI 99999		
Signed by :	Bernard Everyperson, Sr. signed on October 25, 2009		
Consent Directive Document stored by:	Level Seven Healthcare, Inc.		
Address:	4444 Healthcare Drive Ann Arbor, MI 99999, US		

3 BODY

CDA R2 does not allow a structured and a non-XML body to be specified in the same document. However, this limitation may be eliminated in a future CDA release (e.g., CDA Release 3). Currently, implementers must choose between using a non-XML body or a `structuredBody` for exchanging Privacy Consent Directives. If systems cannot support structured content, implementers can choose the Unstructured Documents CDA Implementation Guide or BPPC. This Implementation Guide provides support for a `structuredBody` only. In addition to structured entries, this specification allows for a scanned image of a privacy consent directive to be included as an `observationMedia` instance in the `structuredBody` to provide backward compatibility for BPPC.

CONF-CD-13: A Privacy Consent Directive **SHALL** have a `structuredBody` element.

The content of the `structuredBody` element includes the human readable text of the document.

The `structuredBody` of a conformant Privacy Consent Directive document includes one of the following in addition to a formatted narrative representation of a Privacy Consent Directive:

- 1) An interoperable representation of a client's health information privacy preferences using HL7-based sections and entries that enables the exchange of privacy consent directives between entities using dissimilar security frameworks to enforce the assertions made by the consenter.
- 2) An equivalent representation using prevailing, platform-specific assertions to enable the exchange of computable privacy consent directives across similar systems using a common security infrastructure. This representation will use a well-defined assertion language corresponding to the appropriate access control markup or digital rights management technology used by the implementers.

The purpose for this CDA R2 document is to create a computer-readable representation of a Privacy Consent Directive that can be consumed by an Access Control System. This document expresses the parameters that would be used by a privacy policy language. This is accomplished using either mechanism above to provide a series of computable attributes that can be used to represent the multiple forms of policies defined within jurisdictions (e.g., "authorizations", "restriction requests" or other types of privacy consent directives).

3.1 Section Descriptions

The following conformance statements define the required and optional sections necessary to assert conformance to the Privacy Consent Directive DSTU.

3.2 Required Sections

The following describes the required section in a Privacy Consent Directive:

CONF-CD-14: A Privacy Consent Directive **SHALL** contain a Privacy Consent Directive Details section.

3.2.1 Privacy Consent Directive Details Section

This section is intended as container for the narrative description of the privacy consent directive and for the entry needed to provide its structured/computable equivalent.

The following asserts conformance to the Privacy Consent Directive DSTU.

CONF-CD-15: This section **SHALL** include the `templateId` for the Privacy Consent Directive section with the value “2.16.840.1.113883.3.445.17” and a title of “Privacy Consent Directive Details”.

Figure 15: Privacy Consent Directive Details Section example

```
<structuredBody>
  <component typeCode="COMP">
    <section classCode="DOCSECT" moodCode="EVN">
      <templateId root="2.16.840.1.113883.3.445.17"/>
      <code code="57016-8" codeSystemName="LOINC"/>
      <title>Privacy Consent Directive Details</title>
      <!-- Narrative privacy consent directive-->
      <text mediaType="text/x-hl7-text+xml">
        <content> </content>
      </text>
    </section>
  </component>
</structuredBody>
```

3.2.1.1 Privacy Consent Directive Entry

The section shall contain a composite entry for describing the privacy consent directive assertions in computable and scanned image forms.

The following asserts conformance to the Privacy Consent Directive DSTU and supports:

- Purpose of Use allowed by the Privacy Consent Directive
- Attributes of information recipients including role and identity
- The custodian(s) of the IIHI specified in the Privacy Consent Directive
- Actions/Operations authorized or restricted by the Privacy Consent Directive
- Information category or objects (IIHI) specified by the Privacy Consent Directive including Related Condition/Diagnosis and sensitivity specified by the Privacy Consent Directive
- Privacy Policy on which the Privacy Consent Directive was based
- Information recipient obligations regarding handling IIHI disclosed as a result of the Privacy Consent Directive

CONF-CD-16: This section **SHALL** include an `entry` element with `templateId` of “2.16.840.1.113883.3.445.4” and a `typeCode` of “COMP” to organize the structure of a Privacy Consent Directive entry.

CONF-CD-17: The entry element **SHALL** include an `act` element with `templateId` of “2.16.840.1.113883.3.445.5” and a `moodCode` of “DEF” to specify the execution of Privacy Consent Directive.

CONF-CD-18: The `act` element **SHALL** include a `code` element to specify the purpose of use for which the privacy consent is applicable.

Figure 16: Privacy Consent Directive Details Entry example

```
<!--Privacy Consent Directive Entry -->
<entry typeCode="COMP">
  <templateId root="2.16.840.1.113883.3.445.4"/>
  <!-- Structured/computer-readable Privacy Consent Directive Specification -->
  <act classCode="ACT" moodCode="DEF">
    <templateId root="2.16.840.1.113883.3.445.5"/>
    <!-- Purpose of use -->
    <code code="TREATMENT" codeSystem="2.16.840.1.113883.3.18.7.1"
      codeSystemName="nhin-purpose" displayName="Treatment"/>
    <statusCode code="active"/>
  </act>
</entry>
```

CONF-CD-19: This section **SHOULD** include one or more entry/act/informant/[@typeCode='CST'] elements with a templateId of "2.16.840.1.113883.3.445.6" to represent the custodian of the referenced IIHI. This may be different than the custodian of the Privacy Consent Directive document identified in the header. Note, if the informant is different from the custodian of the IIHI, then the informant is re-disclosing, which typically is not allowed.

Figure 17: Information Recipient example

```
<!-- Custodian organization -->
<informant typeCode="INF" contextControlCode="OP">
  <templateId root="2.16.840.1.113883.3.445.6"/>
  <assignedEntity>
    <id root="1.3.6.4.1.4.1.2835.2" extension="980983"/>
    <representedOrganization>
      <name>Level Seven Healthcare, Inc.</name>
      <telecom value="409-444-2353"/>
      <addr>
        <streetAddressLine>
          4444 Healthcare Drive
        </streetAddressLine>
        <city>Ann Arbor</city>
        <state>MI</state>
        <postalCode>99999</postalCode>
        <country>USA</country>
      </addr>
    </representedOrganization>
  </assignedEntity>
</informant>
```

CONF-CD-20: This section **SHOULD** include one or more entry/act/participant/[@typeCode='IRCP'] elements with a templateId of "2.16.840.1.113883.3.445.7" to represent the provider organization or person intended to use, access, collect information as allowed or prevented by the action specified in this privacy consent directive.

CONF-CD-21: The participant element **MAY** include participantRole/codeSystem specification of "2.16.840.1.113883.11.19682" corresponding to the receiving provider's role [DYNAMIC].

CONF-CD-22: The `participantRole` element **SHOULD** include `playingEntity` element corresponding to the organization or provider intended to receive the information specified in this Privacy Consent Directive document.

Figure 18: Information Recipient example

```
<!-- Receiving provider -->
<participant typeCode="IRCP" contextControlCode="OP">
  <templateId extension="2.16.840.1.113883.3.445.7"/>
  <participantRole classCode="ASSIGNED">
    <id extension="4564" root="1.3.5.35.1.4436.7"/>
    <!-- Role code - optional -->
    <code code="ATND" displayName="Attending Physician"
      codeSystemName="HL7 HealthcareProviderRoleType"
      codeSystem="2.16.840.1.113883.11.19682"/>
    <addr>
      <streetAddressLine>999999 Healthcare Drive</streetAddressLine>
      <city>Ann Arbor</city>
      <state>MI</state>
      <postalCode>99999</postalCode>
      <country>USA</country>
    </addr>
    <!-- Organization
    <playingEntity classCode="ORG">
      <name>Ann Arbor Hospital</name>
    </playingEntity> -->
    <!-- Person -->
    <playingEntity classCode="PSN" determinerCode="INSTANCE">
      <name>
        <prefix>Mr.</prefix>
        <family>Hippocrates</family>
        <given>Harold</given>
        <suffix>MD</suffix>
      </name>
    </playingEntity>
  </participantRole>
</participant>
```

CONF-CD-23: This section **SHOULD** include one or more `entry/act/participant/` elements to represent the provider organization or person intended to use, access, collect information, as allowed or prevented by the action specified in this privacy consent directive.

CONF-CD-24: This section **MAY** include an `entry/act/entryRelationship` with a `templateId` of “2.16.840.1.113883.3.445.8” to represent the action allowed and problem associated with the information allowed by the Privacy Consent Directive.

CONF-CD-25: This `entryRelationship` **SHALL** include an `act` element with default `classCode`=“ACT” and `moodCode`=“DEF”.

CONF-CD-26: This `act` element **SHOULD** include a `@negationId` attribute with a default value of “false” indicating that the action specified is enabled, and a value of “true” if the action is not allowed by the

Privacy Consent Directive. When the negationInd attribute is not transmitted, the receiver must assume the default (specified action is enabled).

CONF-CD-27: The act element **SHALL** include a code element with default of codeSystem="2.16.840.1.113883.5.4" to specify the Privacy Consent Directive operation or action [DYNAMIC].

Figure 19: Action/Operation example

```
<!-- Action -->
<entryRelationship typeCode="COMP" contextConductionInd="true">
  <templateId root="2.16.840.1.113883.3.445.8" />
  <!-- negationInd='false' specifies that the action is authorized-->
  <act classCode="OBS" moodCode="DEF" negationInd="false">
    <!-- Action/Operation -->
    <code code="DISCLOSE" codeSystem="2.16.840.1.113883.5.4"
          displayName="Disclose"
          codeSystemName="ActConsentType"/>
  </act>
</entryRelationship>
```

CONF-CD-28: This section **MAY** include an entry/act/entryRelationship/ with a templateId of "2.16.840.1.113883.3.445.9" to represent the entire set of protected information (IIHI) including specific attributes of that information (e.g., category type, related diagnosis, sensitivity/confidentiality).

CONF-CD-29: The observation element **SHOULD** include one or more organizer/component/observation[@moodCode='DEF']/ elements with a templateId of "2.16.840.1.113883.3.445.10" to specify each information type (IIHI) included in the authorization contained in the Privacy Consent Directive document.

CONF-CD-30: The observation element **SHOULD** include a code element to specify the code corresponding to the information type (IIHI) included in the authorization contained in the Privacy Consent Directive document.

CONF-CD-31: The observation element **MAY** include a precondition[@typeCode="PRCN"]/ element with a templateId of "2.16.840.1.113883.3.445.11" to specify the diagnosis or problem associated with the information.

CONF-CD-32: The observation element **MAY** include a precondition[@typeCode="PRCN"]/ element with a templateId of "2.16.840.1.113883.3.445.12" to specify the sensitivity of the protected information (IIHI) specified in Privacy Consent Directive.

Figure 20: Information Type and Sensitivity component

```

<!-- Information references:
           category, object id, sensitivity, related problem -->
<entryRelationship typeCode="COMP" contextConductionInd="true">
  <templateId root="2.16.840.1.113883.3.445.9"/>
  <organizer classCode="CLUSTER" moodCode="DEF">
    <statusCode code="active"/>
    <component typeCode="COMP">
      <observation classCode="OBS" moodCode="DEF">
        <templateId extension="2.16.840.1.113883.3.445.10"/>
        <code code="GAIN"
              codeSystemName="ActInformationCategoryCode"
              codeSystem="2.16.840.1.113883.5.4"
              displayName="Global Appraisal of Individual Needs (GAIN)"/>
        <!-- Related Condition/Problem -->
        <precondition typeCode="PRCN">
          <templateId
                root="2.16.840.1.113883.3.445.11"/>
          <criterion classCode="OBS" moodCode="EVN.CRT">
            <code code="371422002" codeSystemName="VA/KP
                  Problem Value Set"
                  codeSystem="2.16.840.1.113883.3.88.12.3221.7.4"
                  displayName="History of substance abuse" />
            </criterion>
          </precondition>
          <precondition typeCode="PRCN">
            <templateId root="2.16.840.1.113883.3.445.12"/>
            <criterion classCode="COND" moodCode="EVN.CRT">
              <code code="V"
                    codeSystemName="ConfidentialityByAccessKind"
                    codeSystem="2.16.840.1.113883.1.11.10229"
                    displayName="Very Restricted"/>
              </criterion>
            </precondition>
          </observation>
        </component>
      </organizer>
    </entryRelationship>

```

CONF-CD-33: This section **MAY** include an entry/act/entryRelationship with a templateId of “2.16.840.1.113883.3.445.13” to represent references to **Privacy Policies** on which the Privacy Consent Directive is based along with the information recipient Obligation.

CONF-CD-34: The component element **SHALL** include an act/code element to specify the Privacy Policy or regulation that is basis for requesting the authorizations specified in the Privacy Consent Directive.

CONF-CD-35: The component element **MAY** include a precondition element with a templateId of “2.16.840.1.113883.3.445.14” and an element of @typeCode=“PRCN” to specify any additional obligations imposed on the recipient of the IIHI referenced in the Privacy Consent Directive.

CONF-CD-36: The component element **SHOULD** include a criterion[classCode=“OBS”]/code element to specify the coded

obligations imposed on the recipient of the IIHI referenced in the Privacy Consent Directive.

Figure 21: Privacy Policy Reference and Obligation component

```
<!-- Health Information Privacy Policy and Obligation -->
<component typeCode="COMP" contextConductionInd="true">
  <templateId root="2.16.840.1.113883.3.445.13"/>
  <!-- Policy Reference -->
  <act classCode="CONS" moodCode="DEF">
    <code codeSystemName="SAMSHA" code="42CFRPart2"/>
    <precondition typeCode="PRCN">
      <templateId root="2.16.840.1.113883.3.445.14"/>
      <!-- Obligation -->
      <critierion classCode="OBS" moodCode="EVN.CRT">
        <code code="AUDIT"
          displayName="Audit access to information"
          codeSystemName="Obligation"/>
      </critierion>
    </precondition>
  </act>
</component>
```

3.2.1.2 Privacy Consent Directive – Alternative Representations

The section may also contain a scanned image or a platform-specific representation of the privacy consent directive for those environments that require it.

- CONF-CD-37:** This section **MAY** include an `entry/act/entryRelationship` with a `templateId` of “2.16.840.1.113883.3.445.15” to include a scanned image of the paper-based Privacy Consent Directive.
- CONF-CD-38:** The `entryRelationship` element **SHOULD** include an `observationMedia[@classCode="OBS"]` element to embed a scanned document representation of the Privacy Consent Directive including required signatures.
- CONF-CD-39:** This section **MAY** include an `entry/act/entryRelationship` with a `templateId` of “2.16.840.1.113883.3.445.16” to represent an alternative representation of the Privacy Consent Directive (e.g., ODRL, XrML, XACML).

Figure 22: Privacy Consent Section example

```

<!-- Other representations: Scanned document and policy language -->
<entryRelationship typeCode="COMP" >
    <templateId root="2.16.840.1.113883.3.445.15"/>
    <observationMedia classCode="OBS" moodCode="EVN">
        <value mediaType="application/pdf" representation="B64">
JVBERi0xLjMKJcfsj6IKNSAwIG9iago8PC9MZW5ndGggNiAwIFIvRmlsdGVyIC9GbGF0
ZURlY29kZT4+CnN0cmVhbQp4nGWPMWsDMQyFd/8Kj fJwqmVbkr0GQqFbg7fQoSRNWuhB
Q/4/1L67TEEYme+9J1s3CMQQRm39NLUxg8H17gK89nN1N8eLAbZ2mmHXuql2QDVUhnZx
a5iBcyQtoMIUM7TZHbH5KZEVDgm//SSUswbFHx/JzBLEu5yYxOIze8bPcRWqdaGDMcZO
Bwc/9bfUNOPfOte4409jxtcIKskqp0JZouJ5deYqeBn58ZmKtIU+2ptjqWQRJpGyrHDu
XIK7Ce2be+/1DzXQP+RlbnRzdHJlYW0KZW5kb2JqcjYgMCEvYmoKMjAxcmVuZG9iago0
...
SW5mbyAyIDAgUgovSUQgWzXGNENDN0FFQjU0QjM2RkIyODNDNUMzMjQ3OUFEMjgzRj48
RjRDQzdBRUI1NEIzNkZCMjgzQzVDMzI0Nz1BRDI4M0Y+XQo+PgpzdGFydHhyZWYKMzAx
...
        </value>
    </observationMedia>
</entryRelationship>
<entryRelationship typeCode="COMP">
    <!-- Sample policy language representation -->
    <templateId root="2.16.840.1.113883.3.445.16"/>
    <observationMedia classCode="OBS" moodCode="EVN">
        <value mediaType="text/xml" representation="TXT">
...
        </value>
    </observationMedia>
</entryRelationship>

```

3.3 Optional Sections

An optional section in a Privacy Consent Directive is intended to hold the signatures (as scanned images of wet signatures or an XML-Digital signature) . While electronic signatures cannot be captured in a CDA R2 document, CDA R2 supports external digital and scanned wet signatures that can be included using RIM-based extensions. An XML digital signatures wrapper may be used to wrap the CDA document according to local policy. This section may be used to authenticate the origin and attest to the integrity of the Privacy Consent.

CONF-CD-40: A Privacy Consent Directive **MAY** contain the sections described hereunder.

3.3.1 Signatures

This section provides a narrative block to reference an entry to enumerate the signatures that could not be included in the document header. At this time, CDA R2 does not support any type of digitized signature. This section describes a workaround for this version of the Implementation Guide and will become obsolete if CDA R3 adds the ability to specify not only that signatures were collected, but allows the addition of scanned as well as digital signatures in line with the rest of the authenticator’s details.

CONF-CD-41: If included, this section **SHALL** include the `templateId` for the Signatures section “2.16.840.1.113883.3.445.18” and a title of “Signatures”.

CONF-CD-42: This section **MAY** include the `entry/observationMedia` for each signature (e.g., `legalAuthenticator`, `authenticator`) or a scanned version of the entire privacy consent directive form including the signatures.

Figure 23: Signatures Section example

```
<component typeCode="COMP" contextConductionInd="true">
  <section classCode="DOCSECT" moodCode="EVN">
    <!-- Signature Section -->
    <templateId root="2.16.840.1.113883.3.445.18"/>
    <title>Signatures</title>
    <text mediaType="text/x-hl7-text+xml">
      <paragraph> This section contains the signatures of the consenter.
    </paragraph>
    <paragraph>
      <renderMultiMedia referencedObject="Page_1">
        <caption>Page 1</caption>
      </renderMultiMedia>
    </paragraph>
    <paragraph>
      <renderMultiMedia referencedObject="Page_2">
        <caption>Page 2</caption>
      </renderMultiMedia>
    </paragraph>
    </text>
    <entry typeCode="COMP">
      <observationMedia ID="Page_1" classCode="DGIMG" moodCode="EVN">
        <value mediaType="image/jpeg">
          <reference value="P1.jpg"/>
        </value>
      </observationMedia>
    </entry>
    <entry typeCode="COMP">
      <observationMedia ID="Page_2" classCode="DGIMG" moodCode="EVN">
        <value mediaType="image/jpeg">
          <reference value="P2.jpg"/>
        </value>
      </observationMedia>
    </entry>
  </section>
</component>
```

4 REFERENCES

- [Composite Privacy Consent Directive Domain Analysis Model](#) (CPCD DAM) – DSTU February 2010
- LOINC[®]: Logical Observation Identifiers Names and Codes, Regenstrief Institute. <http://www.loinc.org>
- CDA: Clinical Document Architecture Release 2: Clinical Document Architecture (CDA) Release 2, May 2005. <http://www.hl7.org/v3ballot/html/infrastructure/cda/cda.htm>
- Health Information Technology Standards Panel (HITSP) Constructs, including the Encounter Document Using IHE Scanned Document (XDS-SD) Component (C48). <http://www.hitsp.org/>

APPENDIX A — ACRONYMS AND ABBREVIATIONS

BPPC	Basic Patient Privacy Consent
CCD	Continuity of Care Document
CDA	Clinical Document Architecture
CONF	Conformance
CPCD	Composite Privacy Consent Directive
DAM	Domain Analysis Model
DSTU	Draft Standard for Trial Use
EHR	Electronic Health Record
HITSP	Healthcare Information Technology Standards Panel
HL7	Health Level Seven
IG	Implementation Guide
IIHI	Individually Identifiable Health Information
IHE	Integrating the Healthcare Enterprise
LOINC	Logical Observation Identifiers Names and Codes
ODRL	Open Digital Rights Language
R2	Release 2 (CDA Level 2)
R3	Release 3 (CDA Level 3)
RIM	Reference Information Model
SDO	Standards Development Organization
SAMHSA	Substance Abuse and Mental Health Services Administration
SDWG	Structured Documents Working Group
SDM	Substitute Decision Maker
SNOMED-CT	Systematized Nomenclature of Medicine--Clinical Terms
SSA	Social Security Administration
TBD	To be determined
TP	Transaction Package
VA	Department of Veterans Affairs
XACML	OASIS eXtensible Access Control Markup Language
XDS	Cross-Enterprise Document Sharing profile
XDS-SD	Cross-Enterprise Document Sharing – Scanned Document profile
XML	Extensible Markup Language
XrML	eXtensible rights Markup Language

APPENDIX B — TEMPLATE IDS IN THIS GUIDE

Table 1: TemplateIds in This Guide

Template ID	Source	Description
2.16.840.1.113883.10.20.3	CONF-CD-1	General Header Constraints
2.16.840.1.113883.3.445.1	CONF-CD-2	Privacy Consent Directive Header Constraints (Document code)
2.16.840.1.113883.3.445.2	CONF-CD-3	Author function code
2.16.840.1.113883.3.445.3	CONF-CD-5	Documentation of service
2.16.840.1.113883.3.445.4	CONF-CD-16	Privacy Consent directive entry
2.16.840.1.113883.3.445.5	CONF-CD-17	Purpose of use code
2.16.840.1.113883.3.445.6	CONF-CD-19	Protected information custodian
2.16.840.1.113883.3.445.7	CONF-CD-20	Receiving provider
2.16.840.1.113883.3.445.8	CONF-CD-24	Action/operation, negation indicator
2.16.840.1.113883.3.445.9	CONF-CD-28	Information references collection
2.16.840.1.113883.3.445.10	CONF-CD-29	Information reference
2.16.840.1.113883.3.445.11	CONF-CD-31	Related diagnosis/clinical condition
2.16.840.1.113883.3.445.12	CONF-CD-32	Confidentiality and sensitivity
2.16.840.1.113883.3.445.13	CONF-CD-33	Health Information Privacy Policy
2.16.840.1.113883.3.445.14	CONF-CD-35	Receiver Obligation
2.16.840.1.113883.3.445.15	CONF-CD-37	Scanned document
2.16.840.1.113883.3.445.16	CONF-CD-39	Alternative representation of the Privacy Consent Directive
2.16.840.1.113883.3.445.17	CONF-CD-15	Privacy Consent Directive Details Section
2.16.840.1.113883.3.445.18	CONF-CD-41	Privacy Consent Directive Signature Section

APPENDIX C — PRIVACY CONSENT DIRECTIVE REQUIREMENTS

This Implementation Guide was derived from the [Composite Privacy Consent Directive Domain Analysis Model](#) (CPCD DAM) – DSTU February 2010

Comments regarding implementations of this DSTU are available at:
<http://www.hl7.org/dstucomments/showdetail.cfm?dstuid=54>

APPENDIX D – GENERAL HEADER CONSTRAINTS COMPARISON

Table 2: Comparison of Privacy Consent Directive IG and CDA General Header Constraints

Privacy Consent Directive Element	Req?	CDA Element	Req?
XDSDocumentEntry.formatCode		ClinicalDocument	Shall
XDSDocumentEntry.uniqueId		ClinicalDocument/ realmcode	Shall
ClinicalDocument/ typeId	Shall	ClinicalDocument/ typeId	Shall
ClinicalDocument/ templateID	Shall	ClinicalDocument/ templateID	Shall
ClinicalDocument/ id	Shall	ClinicalDocument/ id	Shall
ClinicalDocument/ code	Shall	ClinicalDocument/ code	Shall
ClinicalDocument/ title	Should	ClinicalDocument/ title	Shall
ClinicalDocument/ effectiveTime	Shall	ClinicalDocument/ effectiveTime	Shall
ClinicalDocument/ confidentialityCode	Shall	ClinicalDocument/ confidentialityCode	Shall
ClinicalDocument/ languageCode	Shall	ClinicalDocument/ languageCode	Shall
ClinicalDocument/ documentationOf/ serviceEvent/ effectiveTime	Shall		
ClinicalDocument/recordTarget	Shall	ClinicalDocument/ recordTarget	Shall
ClinicalDocument/ recordTarget/ patientRole/ id	Should	ClinicalDocument/ recordTarget/ patientRole	Shall
ClinicalDocument/ recordTarget/ patientRole/ addr	Should	ClinicalDocument/ recordTarget/ patientRole/ addr	Shall
ClinicalDocument/ recordTarget/ patientRole/ telecom	Should	ClinicalDocument/ recordTarget/ patientRole/ telecom	Shall
ClinicalDocument/ recordTarget/ patientRole/ patient/ name	Should	ClinicalDocument/ recordTarget/ patientRole/ patient/ name	Shall
ClinicalDocument/ recordTarget/ patientRole/ patient/ administrativeGenderCode	Should	ClinicalDocument/ recordTarget/ patientRole/ patient/ administrativeGenderCode	Shall
ClinicalDocument/ recordTarget/ patientRole/ patient/ birthTime	Should	ClinicalDocument/ recordTarget/ patientRole/ patient/ birthTime	Shall
ClinicalDocument/ author/ time	Should	ClinicalDocument/ author/ time	Shall
ClinicalDocument/ author (original)	Should	ClinicalDocument/ author/ assignedAuthor	Shall
ClinicalDocument/ author/ assignedAuthor/ assignedPerson (original)	Should	ClinicalDocument/ author/ assignedAuthor/ id	Shall
ClinicalDocument/ author/ assignedAuthor/ addr	Should	ClinicalDocument/ author/ assignedAuthor/ addr	Shall
ClinicalDocument/ author/ assignedAuthor/ telecom	Should	ClinicalDocument/ author/ assignedAuthor/ telecom	Shall
ClinicalDocument/ custodian	Should	ClinicalDocument/ custodian	Shall
ClinicalDocument/ custodian/	Shall	ClinicalDocument/ custodian/	Shall

Privacy Consent Directive Element	Req?	CDA Element	Req?
assignedCustodian/ representedCustodianOrganization/ name		assignedCustodian/ representedCustodianOrganization/ name	
ClinicalDocument/ custodian/ assignedCustodian/ representedCustodianOrganization/ addr	Shall	ClinicalDocument/ custodian/ assignedCustodian/ representedCustodianOrganization/ addr	Shall
ClinicalDocument/ custodian/ assignedCustodian/ representedCustodianOrganization/ telecom	Should	ClinicalDocument/ custodian/ assignedCustodian/ representedCustodianOrganization/ telecom	Shall
ClinicalDocument/ legalAuthenticator	Shall		
ClinicalDocument/ component/ structuredBody	Shall		