Publication of this draft standard for trial use and comment has been approved by Health Level Seven International (HL7). This draft standard is not an accredited American National Standard. The comment period for use of this draft standard shall end 24 months from the date of publication. Suggestions for revision should be submitted at http://www.hl7.org/dstucomments/index.cfm.

Following this 24 month evaluation period, this draft standard, revised as necessary, will be submitted to a normative ballot in preparation for approval by ANSI as an American National Standard. Implementations of this draft standard shall be viable throughout the normative ballot process and for up to six months after publication of the relevant normative standard.

Custodian Work Group: www.hl7.org/Special/committees/homehealth/index.cfm
Custodian Work Group e-Mail: cbhs@lists.hl7.org
IMPORTANT NOTES:

A. If you are the individual that downloaded or ordered this HL7 Standard, specification or other work (in each and every instance "Material"), the following describes the permitted uses of the Material.

B. If you are NOT such individual, you are not authorized to make any use of the Material. To obtain an authorized copy of this Material, please visit http://www.hl7.org/implement/standards/index.cfm.

C. If you are not an HL7 Organizational Member, the following are your permitted uses of this Material:

1. Read and Copy License Only. HL7 hereby grants you the right, without charge, to download and copy (for personal use only) this Material for study purposes only. This license grant does not include the right to sublicense or modify the Material, or to implement the Material, either in whole in part, in any product or service.

Please see http://www.hl7.org/legal/ippolicy.cfm for the full license terms governing the Material.

D. If you are an HL7 Organizational Member, the following are your permitted uses of this Material.

1. Implementation License Terms.

1.1 Definitions. As used in this Agreement, the following terms shall have the following definitions:

"Compliant Product" is a product or service that implements Material that is an HL7 Specification in whole or in part.

"End User" is a company, entity or individual that is the ultimate purchaser or licensee from Licensee of a Compliant Product.

1.2 License. In consideration of becoming an Organizational member of HL7 and continuing to pay the appropriate HL7 Organizational membership fees in full, HL7 hereby grants to you without additional charge, on a perpetual (except as provided for in the full license terms governing the Material), non-exclusive and worldwide basis, the right to (a) download, copy (for internal purposes only) and share this Material with your employees and consultants for study purposes, and (b) utilize the Material for the purpose of developing, making, having made, using, marketing, importing, offering to sell or license, and selling or licensing, and to otherwise distribute, Compliant Products, in all cases subject to the conditions set forth in this Agreement and any relevant patent and other intellectual property rights of third parties (which may include members of HL7). No other license, sublicense, or other rights of any kind are granted under this Agreement.

Please see http://www.hl7.org/legal/ippolicy.cfm for the full license terms governing the Material.
# Table of Contents:

Introduction ........................................................................................................................................... 7
Stakeholder Recommendation .................................................................................................................. 7
Document Changes ................................................................................................................................... 8
Authors .................................................................................................................................................... 8
Glossary of Terms .....................................................................................................................................
Client Health Record ............................................................................................................................... 8
Consent Directive ...................................................................................................................................... 8
Custodian .................................................................................................................................................. 9
Electronic Health Record (EHR) ............................................................................................................... 9
Individually Identifiable Health Information (IIHI) .................................................................................... 9
Personal Health Record (PHR) ............................................................................................................... 9
Protected Health Information (PHI) ......................................................................................................... 9
Shared Secret ........................................................................................................................................... 10

## 1. Use Case Analysis ......................................................................................................................... 10
Client ....................................................................................................................................................... 13
Consenter ................................................................................................................................................. 13
Healthcare Provider ............................................................................................................................... 13
Information Requester ........................................................................................................................... 13
Information Sender (Custodian) ............................................................................................................. 13
Patient ..................................................................................................................................................... 13
Privacy Policy Author ............................................................................................................................ 13
Substitute Decision Maker (SDM).......................................................................................................... 13

## 2. Electronic Privacy Policy Information Analysis ............................................................................. 22

### 2.1 Information structure used to represent Privacy Policies

- Authority ................................................................................................................................................ 23
- ClinicalCondition ................................................................................................................................... 23
- Grantee ................................................................................................................................................... 23
- PrivacyPolicy ......................................................................................................................................... 24
- InformationReference ........................................................................................................................... 24
- JurisdictionalOrganization .................................................................................................................... 24
- InformationObject ............................................................................................................................... 24
- OperationType ....................................................................................................................................... 24
- PolicyProgramSource .......................................................................................................................... 25
- Population ............................................................................................................................................. 25
- ProviderOrganization ........................................................................................................................... 25
- PrivatInsurance ..................................................................................................................................... 25
- PublicServices .......................................................................................................................................... 25
- PublishedPrivacyPolicy ......................................................................................................................... 26
- Role ....................................................................................................................................................... 26
- FunctionalRole ....................................................................................................................................... 26

### 2.2 Applying privacy policies to individually identifiable health information

- Sample Privacy Policy ........................................................................................................................... 27

## 3. Electronic Data Consent Directives Information Analysis .......................................................... 28
Consenter ................................................................................................................................................ 29
Client ....................................................................................................................................................... 29
ConsentDirective ..................................................................................................................................... 30
PrivacyRule .............................................................................................................................................. 30
HealthRecord .......................................................................................................................................... 31
PublishedConsent ................................................................................................................................. 31

### 3.1 Sample Consent Directive for Substance Abuse and Addiction Clients

- ............................................................................................................................................................... 32
Appendix A: Detailed Use Cases and Scenarios

Grant Control of the Client Health Records to Individuals

Basic Scenario

Sample scenario: "Clients have authority over Substance Abuse records if covered by public programs"

Post-Condition

Actors

Manage Consent Directives

Pre-conditions

Basic Scenario

Actors

Request eConsent for a Client

Pre-Conditions

Basic Scenario

Alternate Flow

Post-condition

Actors

Provider Requests Client Health Records

Basic Scenario

Sample Scenario: "Third Party Opinion"

Sample Scenario "Sharing Data with Fitness Coach"

Post-condition

Actors

Information System Masks Health Record Information based on Client Preferences

Pre-conditions

Basic Scenario

Actors

Information System Flags Masked Health Record Information

Pre-condition

Basic Scenario

Actors

Provider Amends Client Health Records based on Client’s Consent Directive
Sample Scenario: Remote Monitoring

Sample Scenario: Substance Abuse

Appendix B: Consent Directive Lifecycle
Figure List:

Figure 1: Use Case Diagram Notation ........................................................................................................ 11
Figure 2: Actors Overview .................................................................................................................................. 12
Figure 3: Privacy Business Use Cases ......................................................................................................... 14
Figure 4: Privacy Policy Management and Inquiry ..................................................................................... 15
Figure 5: Consent Directive Management and Enforcement ........................................................................ 15
Figure 6: Privacy and Consent Management Operations - Dependency View ........................................... 16
Figure 7: Privacy Policy Structure Overview Diagram .............................................................................. 23
Figure 8: Privacy of Clinical Documents ..................................................................................................... 27
Figure 9: Privacy Policy based on "42 CFR Part2" regulation ...................................................................... 28
Figure 10: Consent Directive Overview Diagram ........................................................................................ 29
Figure 11: Sample Consent Directive based on 42 CFR Part 2 Policy ............................................................ 32
Figure 12: Manage Consent Directives Interactions .................................................................................... 34
Figure 13: Manage Privacy Policy Interactions ........................................................................................... 35
Figure 14: Request IIHI with Explicit Consent .............................................................................................. 36
Figure 15: Request IIHI based on Privacy Policy ........................................................................................ 37
Figure 16: Privacy Policy and Consent Directive Terminology .................................................................... 38
Figure 17: Common Privacy and Security Terminology ............................................................................... 41
Introduction

The emergence of Electronic Health Record Systems and the wide use of electronic and/or personal health records requires that medical information be protected from abuse and unauthorized disclosure. Currently national and state/province legislation, regulations, and/or privacy policies are already in place to protect individuals from the misuse of their individually identifiable health information (IIHI). This model contains the analysis of several representative use cases illustrating the use of electronic privacy policies (Privacy Policy) and electronic consent directive (Consent Directive) as it relates to the Privacy Policy. This analysis provides a "composite" view of Consent Directive and their underlying privacy policies.

Additionally, the model identifies several key abstractions that are important to describing data consent and its management over time. This model may be applied to the revision of the 'Composite Privacy Consent Directive R1' topic in the Medical Records domain or to the design of service-aware standards.

Domain Analysis Model

A Domain Analysis Model (DAM) is an abstract representation of a subject area of interest to provide a generic representation of a class of system or capability and suggest a set of approaches to implementation. In HL7 a DAM is complete enough to enable the development of downstream platform-independent models: HL7 RIM-based information and services models. A DAM may also be used to constrain other standards for use in healthcare (e.g. to constraint access control markup standards). The process used to create a DAM is documented in the HL7 Development Framework.

Therefore, the analysis model described here is the result of analyzing stakeholder requirements regarding safeguarding the privacy of health records in a digital world. The requirements are based on the need for next generation systems to provide electronic interoperability standards to exchange privacy policies and data consent directives. Based on business use cases, the analysis has revealed system interactions and information structures required to exchange both privacy policy rules and individual consent directives regarding the collection, access, use, or disclosure of health information.

The applicability of this DAM is limited to the requirements for the creation and use of privacy consent directives as they pertain to client health records and individually identifiable health information.

Stakeholder Recommendation

This domain analysis was based directly on the needs of policy makers such as the Substance Abuse and Mental Health Services Administration (www.samhsa.gov). Policy makers have been faced with the task of bridging the gap between specifying a privacy policy and ensuring that information systems are capable of enforcing it. The following is an example recommendation issued by SAMHSA in March 2008:

**Personal Health Records should possess the functional and technical capability to grant the individual client control of the collection, access, use, and disclosure of their individually identifiable health information (IIHI) according to the type of information, type of provider, and purposes/circumstances of the collection, access, use, or disclosure. The client control capability**
must remain associated with the IIHI as it travels through the electronic health information exchange so that such control is retained when the IIHI is further disclosed. Thus, client control of IIHI capability must span Electronic Health Records and Personal Health Records.

Document Changes
This document contains the following changes:

- Release 1: Initial - Informative Ballot: January 2009
  - Resolved ballot comments and republished: May 2009
- Release 2: Enhanced business use cases, added sample privacy policy and consent directive - DSTU Ballot: September 2009
- Release 2, DSTU: Resolved September 2009 Ballot comments, clarified the applicability of this specification to Individually-Identifiable Health Information (IIHI) referenced by the HealthRecord class, updated the use case list, clarified the use of ObligationCode to support accounting for disclosures.

Authors
Co-chairs:
Richard Thoreson, SAMHSA, Department of Health and Human Services, Richard.Thoreson@samhsa.hhs.gov
Suzanne Gonzales-Webb. Department of Veterans Affairs/SAIC, Suzanne.Gonzales-Webb@va.gov

Contributors:
Kathleen Connor, Microsoft Corporation, kathleen.connor@microsoft.com
Patrick Pyette, Perimind Corporation, pyette@perimind.com

Modeling Facilitator, Publishing Facilitator, Contributor:
Ioana Singureanu, Eversolve LLC, ioana@eversolve.com

Glossary of Terms
The following terms are used throughout this model:

**Client Health Record**
An electronic record of health-related information for an individual that conforms to nationally recognized interoperability standards that can be drawn from multiple sources. This term does not refer to a computer system, but instead to information that may be retrieved from Electronic Health Record (EHR-S) and Personal Health Record (PHR-S) systems.

**Consent Directive**
A client’s instructions regarding consent to collect, use, and/or disclose individually identifiable health information.

Additional definitions from ISO/IEC WD 29101.2 are included below:
Deemed consent: In the context of a statutory requirement, it does not matter whether the patient/person has actually consented; the law permits organizations to act as if the patient/person has consented; there is no right to withdraw or withhold consent. Therefore, the privacy policy may specify that consent may not be revoked.

Express consent: A voluntary agreement with what is being done or proposed that is unequivocal and does not require any inference on the part of the organization seeking consent. The analysis assumes that privacy policies allow clients or their substitute decision maker to exercise choices regarding their health records.

Implied consent: A voluntary agreement with what is being done or proposed that can be reasonably determined through the actions or inactions of the patient/person. The implied consent is specified by organizational or jurisdictional policy.

No consent: In the context of a statutory requirement, consent is not required for a particular purpose. The privacy policy may specify that consent is not required.

Custodian
A custodian is an individual or organization that collects, uses, or discloses IIHI for the purposes of care and treatment, planning, and management of the health system or health research.

Source: ACIET Glossary - [1]

Electronic Health Record (EHR)
An electronic record (not a computer system) of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be created, managed, and consulted by authorized clinicians and staff across more than one healthcare organization.

Source: National Alliance for Health Information Technology (NAHIT)

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. For example, this type of personal health information is specified in Standards for Privacy of Individually Identifiable Health Information - 45 CFR Parts 160 and 164.

Personal Health Record (PHR)
An electronic record (not a computer system) of health-related information on an individual that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared, and controlled by the individual.

Source: National Alliance for Health Information Technology (NAHIT)

Protected Health Information (PHI)
HIPAA definition - PHI is individually identifiable health information that is transmitted by or maintained in electronic media or any other form or medium. This information must relate to:

1. The past, present, or future physical or mental health, or condition of an individual
2. Provision of health care to an individual, or
3. Payment for the provision of health care to an individual

If the information identifies or provides a reasonable basis to believe it can be used to identify an individual, it is considered *individually identifiable health information* (refer to above).

**Shared Secret**

A “shared secret” is pass code used to provide Clients with an extra measure of assurance that access, use, and disclosure of their IIHI is consistent with their Consent Directives and local and jurisdictional policy. Once established, the Shared Secret (aka Keyword) can be used by the Client to perform Consent Directives Management activities, but most importantly, can use it to allow trusted providers to prove they have obtained the patient’s verbal consent to use the Client’s IIHI for specified purposes.

**1. Use Case Analysis**

The use cases in this section describe requirements for the creation and use of privacy consent directives as they pertain to client health records and individually identifiable health information. These use cases are based on the recommendations issued by SAMHSA [http://www.samhsa.gov] in May 2008 to the American Health Information Community (AHIC) client Empowerment Work Group. Use cases represent generalizations of specific scenarios that require interoperability between systems in support of business processes and workflow. The HL7 standard provides rules and guidelines to ensure that interoperable systems use a standard-based set of service interfaces, messages, or documents.

The following section documents the use cases used to drive the analysis and is intended to support the privacy policy and consent directive management needs of stakeholders.

**1.1 Use Case Notation**

Figure 1 shows the use of the UML diagram to identify actors, systems, and use cases. As seen here, the actor uses a capability implemented by a system. The capabilities supported by the system are directly based on the business use cases analyzed as a part of domain analysis. Those use cases that require interoperability are elaborated further and described using a sequence of interactions (See “5. System Interactions Analysis”).
Figure 1: Use Case Diagram Notation
1.1 Actors

The following section describes the actors involved in the main use cases identified for privacy policy and consent directives. An actor is an idealization of an external person, process, or thing interacting with a system, subsystem, or class. An actor cannot be controlled by the system and is defined as being outside the system. An actor is often thought of as a role, rather than an actual person. A single person in the real world can be represented by several actors if they have different roles and goals pertaining to a system. **Primary Actors** interact directly with a system to achieve their goals by initiating interactions with the system. **Stakeholders** can also be modeled as actors. They do not directly interact with the system but are affected by the success of Primary Actor interactions. **Passive Actors** receive requests or are activated by the system.

Figure 2 describes the relationships between the actors involved in privacy use cases. The **specialization** relationship is used to describe graphically that the role of Consenter may be played by a Client/Patient, or by a Substitute Decision Maker.

![Figure 2: Actors Overview](image-url)
Client
A client is a person who is enrolled and eligible to receive healthcare services.

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

Healthcare Provider
A provider of services, (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or healthcare services, (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other individual or organization that furnishes, bills, or is paid for health care in the normal course of business [45 CFR § 160.103].

Information Requester
An information requester is a healthcare provider who requires access to a client health record during the course of their normal employment responsibilities (i.e., a provider may require access to historical individually identifiable health information for treatment).

Information Sender (Custodian)
A healthcare provider that has the authority to send client health records to another provider who is similarly authorized to receive and make use of the information. See the Glossary for additional information regarding the “Custodian”.

Patient
A patient is a client who has received medical services over time from provider organizations or licensed providers. Throughout this document, the Patient is called “Client” and the role of Patient is replaced by the more generic “Consenter” role. A Patient/Client is a type of Consenter and these generalizations simplify the narrative.

Privacy Policy Author
This role is played by an individual policy expert in a territorial authority that protects the privacy of client health records based on local law and regulation. This authority is also responsible for establishing privacy policies that protect all the individuals in its territory.

Substitute Decision Maker (SDM)
A SDM is a person who is authorized to consent to the collection, use or disclosure of Individually Identifiable Health Information for a given client. Throughout this document, the SDM is referenced as a “Consenter” and these roles are considered to be equivalent for the purpose of this model.

1.2 Business Use Cases
Figure 3 shows the business use cases required to protect the privacy of client health records and to manage the privacy of those records in emergency situations. These business capabilities are exposed by Electronic Health Record Systems (EHR-S) to the providers that use them and include
specific interoperability and infrastructure capabilities for privacy management and enforcement. The figure illustrates the relationship between use cases.

**Note:** Since a Domain Analysis Model is a conceptual model all the model elements documented here represent conceptual abstractions, not a technical specifications. Therefore all data types used in operation and attribute signatures are intended to illustrate the business requirements not as technical specifications or platform-independent design.

**Figure 3: Privacy Business Use Cases**

**Privacy Policy Management and Inquiry**

Figure 4 illustrates the relationship between use cases as well as the systems responsible for implementing the use cases. The Consent Directive Decision Engine may query the privacy policy for a specific jurisdictional or organizational privacy policy.
Consent Directive Management and Enforcement

Figure 5 describes the use cases and actors involved in the management and enforcement of consent directives. It illustrates the relationship between use cases as well as the systems responsible for implementing the use cases. The figure shows that management of a consent directive is dependent on the choices and constraint options specified by the applicable privacy policy.
1.3 System Capabilities and Use Case Implementation

The conceptual systems that implement the business use cases provide capabilities to other systems that require such capabilities to fulfill specific business needs. Figure 6 summarizes the dependencies and identifies which systems use other systems’ capabilities to fulfill the business use cases identified in this document and detailed in Appendix A:

**Consent Directive Decision Engine**

The Consent Directive Decision Engine may use a technology-specific representation of the privacy rules to determine which parts of the client health record may be collected, accessed, used, or disclosed by a given type of user for a given request. The Consent Directive Decision Engine would be considered a Policy Decision Point or Access Control Decision Function in many Access Control solutions.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>evaluateConsent()</td>
<td>This operation provides rules enforcement based on an electronic privacy policy or consent directive. It evaluates a consent directive rule set.</td>
<td>None, not relevant for this analysis but expected to include a variety of criteria based on the coded attributes of IHI and consent directives. Possible exceptions may include: evaluateConsent() fails with either &quot;failed&quot; or &quot;out-of-band communication required&quot;.</td>
</tr>
</tbody>
</table>
**Use Cases Implemented**

**Evaluate Consent Directive**

Local policies may allow an authorized provider to know that restricted information is available in the client health record even though it was masked based on the Consenter's consent directive or local privacy policies. Upon Consenter's approval (perhaps using a Shared Secret) or by "breaking the glass" in an emergency, the provider may access the information that was masked. In emergency situations, a provider who is authorized by organizational policy or jurisdictional law can override the client's directives. Filtering mechanisms and algorithms are required that apply consent directive rules describing the client's preferences to their health records. Consent directives may include restricted access filters that are applied to a category of health information (i.e., all HIV-related information). A consent directive may also require that IHI be "masked" to protect the client's sensitive information.

*The detailed use cases implemented by the Consent Directive Decision Engine are listed in Appendix A.*

**Consent Directive Management System**

A Consent Directive Management System consists of a repository and associated services for creating, maintaining, and publishing consent directive rules (abbreviated term as used in ISO/IEC 29101). This system is used by consenters and makes consent directives available to other systems that have the ability to process the rules.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| createConsentDirective() | This operation is used to create a new consent directive for a client. Consents are directly derived from Privacy Policy. An exception will occur if the consent disagrees with the policy it references. | **ConsentDirective** [in] `consentDirective`  
This parameter contains the structure of an electronic consent directive. It contains the rules specified by the consenter.  
**OID** [return] `id`  
This return parameter is the unique identifier of the consent directive that references the policy it is associated with.  
Possible exceptions may include: createConsentDirective() fails with "Not allowed by jurisdiction" |
| getConsentDirective()  | This operation returns the detailed consent directive that matches the identifier passed as an input parameter.  | **ConsentDirective** [return] `consentDirective`  
This return parameter is the consent that matched the identifier specified in the input parameter.  
**OID** [in] `id`  
Unique identifier of the consent directive as it appears in... |
<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| hasAConsentDirective()     | This operation supports the need to mask uncodified (or insufficiently codified) free text fields if any consent directive is present for the client. | PurposeCode [in] purpose  
OID [in] targetRecordId |
| revokeConsentDirectives() | This operation is used to revoke a consent directive. | OID [in] id  
RevocationReasonCode [in] reason (0..1)  
Some scenarios may benefit from allowing a ReasonCode for revocation: e.g. requested vs. correction/error. An error would be a discrepancy between the intent of Consent Directive (as communicated by the Consenter) and that which was entered into the CDMS. |
| updateConsentDirectives() | This an optional capability to revise a consent directive based on new client needs. | ConsentDirective [in] consentDirectives  
This parameter contains the structure of an electronic consent directive. It contains the rules specified by the consenter.  
OID [in] id  
Unique identifier of the consent directive intended to be revised. |

Use Cases Implemented

Get consent directive for a client
Consent to collect, use, access, disclose client health records is determined by both a client's consent directive and the policies of the requester's organization and/or governing jurisdiction. The request for a client's consent directive must return all relevant policies.

Manage consent directive for a client
The Consenter (client or Substitute Decision Maker) interacts via a user interface with a Consent Directive Management System (CDMS) to manage the consent directive rules that are used to
evaluate the authority of healthcare providers, payers, and others to collect, use, access, or disclose the client's personal health record for a given set of purposes. The CDMS may be embedded in a PHR-S or some other healthcare platform.

**Manage shared secret**

The Consenter is able to create and revise the shared secret (or Keyword) pass code that is used to provide Clients with an extra measure of assurance that access, use, and disclosure of their IIHI is consistent with their Consent Directives and local and jurisdictional policy.

**Send consent directive**

This use case addresses those scenarios where the consent directive is sent to a specific system receiver (i.e., chronic disease management, EHR-S or PHR-S) upon its creation or revision.

*The detailed use cases implemented by the Consent Directive Management System are listed in Appendix A.*

**Health Records Repository**

A system that stores client health records and makes them available to other systems based on their credentials and privacy consents or policies.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
</table>
| getHealthRecord() | This operation is used to retrieve client health record information on behalf of a user. The recordId parameter cannot be linked to a specific client and thereby preserves anonymity. The information returned depends on privacy policies and consent directives. | OID [in] recordId  
PurposeCode [in] purpose  
FunctionalUserCode [in] role  
OperationType [in] permission |

**Use Cases Implemented**

**Get health record information**

Permission to access and use client health record information is determined by both a client's consent directive and the policies of the requester's organization and/or governing jurisdiction. The request for a client's consent directive must discover and reconcile all relevant policies prior to accessing client health record information.

*The detailed use cases implemented by the Consent Directive Management System are listed in Appendix A.*
Privacy Policy Management System

A system used to maintain and publish privacy policies in electronic form. It stores the privacy policies and maintains them over time. An individual with appropriate credentials may change a policy. The changes are communicated as necessary to all the organizations that need updates.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>createPrivacyPolicy()</td>
<td>This operation creates a new privacy policy.</td>
<td>PrivacyPolicy [in] newPolicy</td>
</tr>
<tr>
<td>deprecatePrivacyPolicy()</td>
<td>This operation deprecates an obsolete policy and, optionally, replaces it with another policy. If the deprecated policy is replaced, the return value represents the id of the new policy. Note that privacy policies are never actually deleted – this ensures an audit trail is always available.</td>
<td>OID [in] deprecatedId, OID [return] replacementId, PrivacyPolicy [in] replacementPolicy</td>
</tr>
<tr>
<td>getDefaultPrivacyPolicy()</td>
<td>This operation retrieves a policy identified for a specific territory or jurisdiction. Consent is directly derived from a privacy policy. If the consent disagrees with the policy it represents, an exception condition will occur.</td>
<td>string [in] territory</td>
</tr>
<tr>
<td>getPrivacyPolicy()</td>
<td>This operation retrieves a policy identified by its unique id.</td>
<td>OID [in] id</td>
</tr>
<tr>
<td>updatePrivacyPolicy()</td>
<td>This operation revises the contents of a policy. Ideally, major changes to a policy should first deprecate the current policy and replace it with a new policy.</td>
<td>OID [in] id, PrivacyPolicy [in] revisedPolicy</td>
</tr>
</tbody>
</table>

Use Cases Implemented

Get privacy policy for a jurisdiction or organization

In order to encourage consistent enforcement, privacy policy rules will be available in electronic form (consent directive). Provider organizations or client health record management systems will use the approved policies in the relevant territory, jurisdiction, or organization to determine which users can control specific aspects of client health records for individuals.
Manage privacy policy

A privacy policy is based on specific legislation, rules, and regulations. Since privacy policies change with regulations, it is necessary to maintain the computable representation and make it available to systems that need it.

*The detailed use cases implemented by the Privacy Policy Management System are listed in Appendix A.*

Requester System (EHR-S)

A system that accesses client health records on behalf of end-users. This may be a Point of Service (POS) system or a clinical information system (e.g. EMR, EPR, ADT, LIS, etc.) that operates at healthcare facilities. This system may access a Health Records Repository that stores the clients' health records.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>getHealthRecords()</td>
<td>The POS or CIS user may request information stored in client health records.</td>
<td>Query parameters based on standards.</td>
</tr>
</tbody>
</table>

**Use Cases Implemented**

**Assert Patient Consent (to override consent)**

Upon Consenter’s approval (using a “shared secret”) or in an emergency situation, the provider may access the information that was masked. In the latter case, a provider who is authorized by organizational or jurisdictional policy overrides the client's preferences. In non-emergency situations, the patient provides their “shared secret” pass code to unlock the information requested by a healthcare provider to deliver appropriate care.

**Modify health records**

At the end of an encounter, if the provider’s EHR-S has the capability, the EHR-S may automatically update the client’s IIHI stored in specific locations (other EHR-S, PHR-S) based on the client’s directive.

**Request health records**

When a healthcare provider requires access to the client’s medical history, medication list, problems, allergy, etc. stored in the health record, the provider must first retrieve any existing consent directive for that client. The information in the consent directive will provide guidance to the provider as to how the health record may be viewed, used, and updated.

**Transfer patient care**

As part of the activity of transferring/referring a client to another provider for care, several documents are provided to the new provider (*Information Requester*) by the current provider (*Information Sender*). To receive the documentation the Information Requester must agree to respect the obligations and conditions specified by the privacy policy and the client’s consent directive. For example, in the case of substance abuse treatment, in order to receive
assessments and progress notes from the current provider, the new provider must agree not to re-disclose the information and must agree to destroy it after a pre-defined length of time.

*The detailed use cases implemented by the Requester System (EHR-S) are listed in Appendix A.*

2. Electronic Privacy Policy Information Analysis

This section describes the attributes of a privacy policy that may be exchanged between systems in a semantically-interoperable manner across organization boundaries. The information model described here embodies the analysis of information requirements provided by business stakeholders. The following assumptions have been made for the analysis of electronic privacy policies:

1. Platform-independence - electronic Privacy Policies must be exchanged between a variety of systems using different means of decoding and evaluating the electronic privacy policies. Security infrastructure systems often employ unique and proprietary approaches for their enforcement mechanism; therefore, the electronic Privacy Policy must be expressed in a platform-independent way allowing ample flexibility for use in these systems.

2. Standard-based - electronic Privacy Policies must use standard structures and terminology to ensure interoperability across a variety of systems and organizations.

**Note:** Since a Domain Analysis Model is a conceptual model all the model elements documented here represent conceptual abstractions, not a technical specifications. Therefore all data types used in operation and attribute signatures are intended to illustrate the business requirements not as technical specifications or platform-independent design.

2.1 Information structure used to represent Privacy Policies

Figure 7 shows the elements of a privacy policy from a jurisdictional or organizational standpoint. Electronic privacy policies are exchanged in a platform-independent, semantically interoperable, and standard-based way. A privacy policy is intended to protect individually identifiable health information from unauthorized use and disclosure.
Figure 7: Privacy Policy Structure Overview Diagram

**Authority**
This abstract class is used to designate the authority that issues the policy. This is the authority that grants prescribed authorization described in the privacy policy. The Authority is an organization (either Jurisdictional or Provider) that is responsible for the Privacy Policy.

**ClinicalCondition**
The health condition(s) associated with the policy. Conditions when specified are coded concepts expressed in a standard vocabulary (e.g., LOINC, SNOMED CT, etc.). These may include indications of "substance abuse" or "HIV-related" illnesses, etc. On obligationCode may be implemented as a "condition".

**Grantee**
This class is used to designate who is delegated privacy policy. For example, in the case of substance abuse related information, the authority to grant, withhold, or withdraw consent to the disclosure of the information, under certain conditions, is delegated to the client. As an intermediary, a Clearinghouse may act as an agent/proxy for a provider organization and therefore can be a grantee as well.
PrivacyPolicy
This is the main/focal class for electronic privacy policies. It contains a set of rules that are intended to be enforced by security systems and are used as the basis for client consent directive.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Narrative description of the privacy policy.</td>
</tr>
<tr>
<td>policyId</td>
<td>This attribute specifies the unique identifier of for a privacy policy.</td>
</tr>
</tbody>
</table>

InformationReference
The attributes and associations of this class describe those data elements of Individually Identifiable Health Information that are subject to privacy policy or consent directives.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Information category (e.g. medication, allergies, laboratory).</td>
</tr>
<tr>
<td>confidentialityIndicator</td>
<td>The confidentiality indicator is a coded attribute that assigns access controls on client health records based on the information or type of access.</td>
</tr>
</tbody>
</table>

JurisdictionalOrganization
This class is used to represent a territorial authority organization that may be issuing privacy policies for a territory.

InformationObject
This class represents a reference to a specific type of information object (i.e., document, order, etc.) that may be referenced by a policy or consent directive.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>Coded attribute that identifies the type of object referenced in the policy. Default: ProgressNote</td>
</tr>
</tbody>
</table>

OperationType
This class specifies the permission that is assigned by the consenter to specific users of client health record information. The permission may control collection, access, use, or disclosure of a specific type of IIHI.
## Operation Code

### Policy Program Source

This class specifies the source of payment for the healthcare services documented by electronic health records. In order to meet specific privacy policy needs, it is necessary to specify if the information protected by the rule was produced through public healthcare or other type of insurance.

### Population

This class specifies that the target of a policy may be an entire population.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Type of population affected by the policy.</td>
</tr>
<tr>
<td>description</td>
<td>Text description.</td>
</tr>
</tbody>
</table>

### Provider Organization

This class is used to specify a healthcare provider and its most important properties.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>providerType</td>
<td>The provider type may be based on specialization or certification. This attribute is intended to be coded.</td>
</tr>
</tbody>
</table>

### Private Insurance

This class references the insurance or self-pay type used by the patient in obtaining the services that produced health records including IIHI.

### Public Services

This class references the public service program that produced the information. This may be an important criterion in privacy policies - especially jurisdictional policies.
### PublishedPrivacyPolicy

This class encapsulates the location of a human-readable version of the Electronic Privacy Policy. The human-readable version is accessible to any authorized system and user via the supplied URI.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
</table>
| uri       | string
Public    [0..1] |

The location (in a registry) of published privacy policy.

### Role

This class is used to specify the role of a user of a computer system. The role is typically associated with the Information Requester and specifies what capabilities are available to a specific type of computer user (i.e., in the Windows operating system, a user may have the role of *Administrator* which enables the capability to add new users).

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
</table>
| name      | string
Public    [0..1] |

User role name, if specified.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
</table>
| roleCode  | StructuralRoleCode
Public    [0..1] |

This attribute refers to a coded structural role specified by an external coding system.

### FunctionalRole

Functional Roles can be grouped according to their authorization to access IIHI and perform various operations on health care information. E.g., A health care provider in Organization A is authorized to access IIHI from Organization B (when Organization A & B have entered into a trusted relationship), when that provider is associated with the Functional Group whose permissions grant access per that FunctionalRole.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Notes</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>name string</td>
<td>User role name, if specified.</td>
</tr>
<tr>
<td>roleCode FunctionalRoleCode</td>
<td>The functional role may specify that the user is part of the</td>
</tr>
<tr>
<td></td>
<td>healthcare team that is directly involved in the client's care.</td>
</tr>
<tr>
<td></td>
<td>This attribute refers to a functional role assigned by an organization to computer users.</td>
</tr>
</tbody>
</table>

2.2 Applying privacy policies to individually identifiable health information

This section demonstrates how privacy policies and consent directives may be used computationally to determine how client health records should be protected. Examples are provided showing techniques for enforcing the privacy of clinical documents and instantiating a policy intended to protect substance abuse records.

Figure 8 demonstrates how a system may use the coded attributes of a clinical document to enforce the appropriate privacy policy. Note that this is only an example. The information references in the privacy policy structure are referring to precise, coded attributes that would appear in the header or body of a clinical document and the coding scheme and process/protocols will have to ensure that a document has either been fully classified or not yet classified, e.g. differentiate between "no code" because none were applicable, and "no code" because it hasn't yet been codified.

Figure 8: Privacy of Clinical Documents
Sample Privacy Policy

The "42 CFR Part2" regulation is intended to protect the privacy of healthcare records produced as a result of a client receiving substance abuse treatment using public services. As seen in Figure 9, the privacy policy assigns the authority over the disclosure of substance abuse records to the client or their designated Substitute Decision Maker. This policy applies to those clients who receive their treatment through public programs (i.e., SAMHSA or Medicaid). This policy instance is a computable representation of the rules contained in the regulation.

Figure 9: Privacy Policy based on "42 CFR Part2" regulation

3. Electronic Data Consent Directives Information Analysis

This section describes the structure and attributes of consent directives issued by individual clients in the context of a default/existing privacy policy. These consent directives are intended to be exchanged as messages or document containing structured content.

Figure 10 describes the structure of those directives specified by a client in order to specify additional privacy rules. As seen here, the consent directive references one or more policies and contains a set of consent rules. The consent directive is expressed using a permission, information category, and user role, similar to the way privacy policy rules are described. This is not surprising considering that a client's consent represents a further constraint of default privacy policies applicable in that territory.

Note: Since a Domain Analysis Model is a conceptual model all the model elements documented here represent conceptual abstractions, not a technical specifications. Therefore all data types used in operation and attribute signatures are intended to illustrate the business requirements not as technical specifications or platform-independent design.
Consenter

This class is intended to capture the properties of a Consenter/Substitute Decision Maker - see the Glossary and the "Actors" section for additional detail.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>relationship string</td>
<td>This coded attribute is intended to specify the relationship between the consenter and the client. The Consenter may be a Substitute Decision Maker, legal guardian, etc.</td>
</tr>
<tr>
<td>public</td>
<td></td>
</tr>
<tr>
<td>digitalSignature</td>
<td>This attribute is intended to store the signature of the person signing off on the consent directive.</td>
</tr>
<tr>
<td>public [0..1]</td>
<td></td>
</tr>
<tr>
<td>signatureRecorded</td>
<td>This attribute records whether a signature was recorded in a paper form.</td>
</tr>
<tr>
<td>boolean public [0..1]</td>
<td></td>
</tr>
<tr>
<td>name string</td>
<td>The name of the consenter</td>
</tr>
<tr>
<td>public</td>
<td></td>
</tr>
</tbody>
</table>
This class is intended to capture the properties of a Consenter/Client - see the “Actors” section for additional detail. A consenter may be the client or their designated Substitute Decision Maker.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>keywordDigitalId</td>
<td>This shared secret/keyword may be used by a consenter to provide temporary access to their electronic health records.</td>
</tr>
<tr>
<td>type</td>
<td>Client type, if necessary.</td>
</tr>
</tbody>
</table>

ConsentDirective
This is the focal class representing a set of consent directives issued by a consenter on behalf of themselves or someone else. It is the root or entry class into the consent directive structure.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>id OID</td>
<td>Unique identifier that refers to a specific consent directive instance. This id or the published URI may be used to lookup the client's consent directives in order to apply them to the collection, access, use, or disclosure of client health records.</td>
</tr>
<tr>
<td>documentImage</td>
<td>This optional attribute references a signed paper document containing the client's consent directive.</td>
</tr>
<tr>
<td>effectiveTime</td>
<td>This attribute specifies the date when the policy/consent is in effect.</td>
</tr>
<tr>
<td>expirationTime</td>
<td>This attribute specifies when the consent directive automatically expires. A consent directive may be revoked prior to its expiration date.</td>
</tr>
<tr>
<td>statusCode</td>
<td>This attribute indicates whether the consent directive is active or not.</td>
</tr>
<tr>
<td>reason</td>
<td>This attribute is used to specify the reason for revoking a Consent Directive, e.g. requested vs. correction/error. An error would be a discrepancy between the intent of Consent Directive (as communicated by the Consenter) and that which was entered into the CDMS.</td>
</tr>
</tbody>
</table>

PrivacyRule
A privacy or consent rule specifies the permission allowed for a specific type of information to a user type by the consenter. The person consenting may be either the subject of the record or a designated Substitute Decision Maker. One or more consent rules comprise a consent directive or privacy policy.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>sequence int</td>
<td>This attribute specifies the sequence of a specific consent directive in the Consent Directive set.</td>
</tr>
<tr>
<td>purpose PurposeCode</td>
<td>This attribute is used to specify the purpose to permit a specific type of action/operation according to the policy. Default: TREATMENT</td>
</tr>
<tr>
<td>obligationCode ObligationCode</td>
<td>This coded attribute specifies a pre-defined obligation associated with a policy or consent.</td>
</tr>
</tbody>
</table>

**HealthRecord**

This class is used to store a reference to the health record that is the subject of the consent rules in the consent directive.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>recordId OID</td>
<td>The id of the record that is the target of a consent directive.</td>
</tr>
<tr>
<td>recordLocation string</td>
<td>The location of the record that is the target of a consent directive.</td>
</tr>
</tbody>
</table>

**PublishedConsent**

This specialization of the ConsentDirective class is used to describe a consent directive published to a registry. If a client’s consent directive is published, a URL/URI is made available for reference. The client may use this URI to allow providers access to the consent directive created by the consenter.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>uri string</td>
<td>If a specific consent directive (for a client) is published, this attribute provides the means to locate and download the consent directive from a registry.</td>
</tr>
</tbody>
</table>
3.1 Sample Consent Directive for Substance Abuse and Addiction Clients

Figure 11 illustrates how the analysis model is applied to represent an instance of a consent directive for a client that is subject to 42 CFR Part 2 due to their coverage and health condition.

As seen here the client grants the provider permission to disclose Progress Notes and Severity Assessments for the purpose of treatment. The consent may instruct the receiver of this information not to re-disclose it, as specific types of information (e.g. substance abuse records) may be shared for a specific purpose only and not intended for re-disclosure (e.g., the obligation is that the provider cannot re-disclose).

As specified by the policy, the consent covers substance abuse-related information and services covered by public healthcare programs.

Figure 11: Sample Consent Directive based on 42 CFR Part 2 Policy
4. System Interactions Analysis

The following sub-sections describe use cases for system interoperability as documented in the previous section. The systems and interactions described here are conceptual relationships and information exchanges, not concrete implementations or software design. The interactions are intended to demonstrate how the business use cases are assigned to specific systems that support required capabilities and how those systems interact with other systems to support the business needs of stakeholders.

**Note:** Since a Domain Analysis Model is a conceptual model all the model elements documented here represent conceptual abstractions, not a technical specifications. Therefore all data types used in operation and attribute signatures are intended to illustrate the business requirements not as technical specifications or platform-independent design.

### 4.1 Manage Consent Directives

This use case realization specifies the system interactions required to maintain the rules contained in a client's consent directive record. These interactions assume that a healthcare systems client has well-defined privacy options that can be exercised via consent directives.

Figure 12 shows the sequence diagram for the interactions necessary to maintain a client's privacy preferences. This sequence supports the business needs of stakeholders and computer system users. The very first action is to retrieve the privacy policies that are applicable to a specific territory. Using the default policy as a basis, a consenter is able to create a set of consent directives and maintain them over time as their privacy needs evolve.
4.2 Manage Privacy Policy

This use case realization specifies the system interaction required to manage the states of privacy policies specified in territorial jurisdictions.
Figure 13 shows the sequence diagram for the interactions necessary to manage a privacy policy in a territorial jurisdiction. These interactions illustrate the entire life cycle of privacy policy from the standpoint of the organization that issues and disseminates the privacy policy. The benefit of an ePolicy is that it is maintained electronically, thus eliminating the guesswork from processing privacy rules at runtime using Consent Directive Decision Engines. Additionally, the Consent Directive Decision Engines hosted by other jurisdictions or organizations (e.g. healthcare providers) may be automatically notified when a rule is added, changed, or deprecated by policy makers in those jurisdictions.
4.3 Request Info with Explicit Consent or Privacy Policy

This section describes the interactions necessary to retrieve health records using either explicit client consent directives or a default privacy policy applicable in a territorial jurisdiction.

Figure 14 shows a sequence diagram containing the users, systems, and interactions required to access client health records for clients who use consent directives or a default privacy policy. The system that requests the record must provide information about the specific type of information required, the intended user's role, the type of permission/operation, and purpose of the inquiry.

Figure 14: Request IIHI with Explicit Consent

4.4 Request Info with Implicit or Deemed Consent

This section describes the interactions required to retrieve electronic health records using an implicit client agreement employing the default privacy policy applicable in a territorial jurisdiction.

Figure 15 shows a sequence diagram containing the interactions required to protect the privacy of electronic health information in those jurisdictions where the policy does not allow any additional options to clients. The default privacy policy is applied whenever information needs to be disclosed, for example.
Figure 15: Request IIHI based on Privacy Policy
5. Vocabulary Analysis
The following sub-sections describe an analysis of the controlled vocabulary required to support electronic privacy policies and consent directives.

Note: The enumerations in this section list only example coded concepts. Implementers will rely on the appropriate terminology standards to create value sets and specify the values allowed for coded concepts identified in this analysis.

5.1 Privacy Policy and Consent Directive terminology
This section describes the terminology required for electronic privacy policy and consent directives. Note that the enumerations in this section list only sample coded concepts. The actual value sets will be defined by the authorities (e.g. jurisdiction, organization). Figure 16 shows the value sets required to support the requirements for interoperable privacy policies and consent directives. The focus of the enumerations seen here is primarily to describe privacy policies and consent directives.

Figure 16: Privacy Policy and Consent Directive Terminology
**AccessOperation**

This value set describes the operations subsumed under the "access" to client health records. Note that operations listed here are examples to illustrate the coded concept, not a reference or implementation value set.

**ActionOperation**

A process or series of acts involved with the collection, access, use, and disclosure of client health records. This concept relates to the "operation" specified in the Role-based Access Control (RBAC) permission.

**CollectOperation**

This value set describes the operations subsumed under the "collection" to client health records. Note that operations listed here are examples to illustrate the coded concept, not a reference or implementation value set.

**ConditionCode**

This coded concept and associated value set are used to describe the medical condition associated with information or encompassing encounter that produced the information.

Note: The codes included here are for illustration only.

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUBSTANCE_ABUSE</td>
<td>Substance abuse and addiction</td>
</tr>
<tr>
<td>ConditionCode</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>MENTAL_HEALTH_DISORDERS</td>
<td>Mental health</td>
</tr>
<tr>
<td>ConditionCode</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
<tr>
<td>HIV</td>
<td>HIV Positive</td>
</tr>
<tr>
<td>ConditionCode</td>
<td></td>
</tr>
<tr>
<td>Public</td>
<td></td>
</tr>
</tbody>
</table>

**Confidentiality**

This reference value set is an example of the various types of privacy policies (a.k.a. "confidentiality") that apply to the various components of a client health record. The examples provided here specify a type of access of access (e.g. business-related, treatment-related, etc.)

**DiscloseOperation**

This value set describes the operations subsumed under the "disclosure" to client health records. Note that operations listed here are examples to illustrate the coded concept, not a reference or implementation value set.
OverrideCode
An override code is intended to specify the reason why a provider had to override the consent directive specified by the client.

Sensitivity
This value set illustrates the types of coded values used to indicate the sensitivity of a client health record. This coded concepts is also used to specify the sensitivity of data that specific user type is allowed to access. The sample value sets are from representative value sets specified by the HL7 Version 3 vocabulary specification.

UseOperation
This value set describes the operations subsumed under the "use" of client health records. Note that operations listed here are examples to illustrate the coded concept, not a reference or implementation value set.

5.2 Common Privacy and Security Terminology
This section describes terminology identified as common to both Role-Based Access Control and Privacy/Consent Directive Enforcement.

Figure 17 shows the common concepts that support the requirements for interoperable privacy policy and consent directives as well as Role-based Access Control. The UML enumeration used to describe the coded concepts contain sample coded values/literals to illustrate the range of values that are applicable. The purpose of the enumerations/value sets is to be equally applicable to describing RBAC permissions, privacy policies, and a client's consent directives. New concepts may be identified with additional analysis and requirements.
Figure 17: Common Privacy and Security Terminology
ArtifactType
This enumeration refers to any client health record artifacts.

CategoryType
This enumeration refers to the various types of client health record information that may be controlled by privacy policies or client consent. These values may include a variety of categories including "Problems", "Results", "Medication", etc.

Note: The codes included here are for illustration only.

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MedicationList</td>
<td>Client's medication list</td>
</tr>
<tr>
<td>CategoryType Public</td>
<td></td>
</tr>
<tr>
<td>Laboratory</td>
<td>Laboratory results including chemistry, microbiology, etc.</td>
</tr>
<tr>
<td>CategoryType Public</td>
<td></td>
</tr>
<tr>
<td>Encounter</td>
<td>Client encounters</td>
</tr>
<tr>
<td>CategoryType Public</td>
<td></td>
</tr>
<tr>
<td>Allergies</td>
<td>Client allergies including food, drug, etc.</td>
</tr>
<tr>
<td>CategoryType Public</td>
<td></td>
</tr>
<tr>
<td>Problems</td>
<td>Client problems</td>
</tr>
<tr>
<td>CategoryType Public</td>
<td></td>
</tr>
</tbody>
</table>

DocumentType
This value set may contain the codes (i.e., LOINC) corresponding to document types used for interoperability (i.e., CDA document types).

Note: The codes included here are for illustration only.

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProgressNotes</td>
<td>Clinical Progress Notes including nursing.</td>
</tr>
<tr>
<td>ObjectCode Public</td>
<td></td>
</tr>
<tr>
<td>DischargeSummary</td>
<td>Client Discharge Summary</td>
</tr>
<tr>
<td>DocumentType Public</td>
<td></td>
</tr>
</tbody>
</table>
### FunctionalUserCode

This user group identifies the relationship of various functional roles that users play in relation to the client.

*Note: The codes included here are for illustration only.*

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectCareTeam</td>
<td>This includes attending physician, nurse, and ancillary users that are directly involved with a client during an episode of care.</td>
</tr>
<tr>
<td>SupportingClinicalServices</td>
<td>This type of user includes all ancillary services (i.e., lab, diagnostic testing, etc.)</td>
</tr>
<tr>
<td>Administrative</td>
<td>This includes payer, billing, etc. and other supportive roles Default: Administrative User</td>
</tr>
</tbody>
</table>

### ObjectCode

This enumeration refers to the operations that users may apply to parts of a client health record, including those specified in the *RBAC Permission Catalog* specification.

*Note: The codes included here are for illustration only.*

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeverityAssessment</td>
<td>Severity Assessment</td>
</tr>
<tr>
<td>InitialAssessment</td>
<td>Substance Abuse and Addiction Assessment</td>
</tr>
</tbody>
</table>
ObligationCode
Action that is required to receive the permission specified in the privacy rule.

*Note: The codes included here are for illustration only.*

<table>
<thead>
<tr>
<th>Code</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteAfterUse</td>
<td>The information must be deleted after use</td>
</tr>
<tr>
<td>Encrypt</td>
<td>The information must be encrypted</td>
</tr>
<tr>
<td>Anonymize</td>
<td>The information must be anonymized by the receiver</td>
</tr>
<tr>
<td>AuditDisclosure</td>
<td>This type of code is used to indicate that a specific event (i.e., disclosure, consent directive override) should be tracked for audit purposes. This code may be used to support &quot;Accounting for Disclosure&quot; regulation in the United States.</td>
</tr>
</tbody>
</table>

ProviderTaxonomy
This enumeration refers to the HIPAA Provider Taxonomy or other applicable categorization systems.

PurposeCode
This enumeration refers to the various possibilities for issuing permission or denying it.

StructuralRoleCode
This value set/enumeration is used to illustrate the type of roles that may be used in a privacy policy or RBAC permission. Structural codes are currently provided by ASTM. The structural role is often used specifying Role-Based Access Control.
Appendix A: Detailed Use Cases and Scenarios

The following use cases were used to specify the scope of this specification and document the requirements analyzed by the project team:

Grant Control of the Client Health Records to Individuals

This use case is the basis of the entire Consent Directive specification. If the clients do not own/control their IIHI, then they cannot specify consent directives or privacy preferences.

Basic Scenario

Based on the current regulation, the Jurisdictional Authority assigns the right to grant, withdraw, or withhold consent to the collection, access, use, and disclosure of individually identifiable health information to the individual who is its subject or to their designated Substitute Decision Maker (SDM) that acts on behalf of that individual. An individual's control may be limited to one or more specified purposes of use as well as a finite range of granular options based on the consent model adopted by the jurisdiction.

In addition to providing limited control, the regulation specifies a default privacy policy. An individual (or their SDM) may customize their privacy preferences through Consent Directives, however the jurisdiction may also identify certain purposes of use, classifications of IIHI (e.g. health system planning, positive communicable disease test results), etc., for which consent is deemed or not required -- effectively removing control over that IIHI from the individual in those situations.

Sample scenario: "Clients have authority over Substance Abuse records if covered by public programs"

Compliance with 43 CFR Part 2 requires the providers may not disclose/re-disclose substance abuse records without the explicit consent of clients if the clients are covered and receive treatment from public programs. Therefore the regulation grants control over the disclosure of substance abuse records to the clients.

Post-Condition

- The IIHI of every client who has or may have IIHI accessed under the Jurisdictional Authority will be collected, accessed, used, and disclosed in accordance with the default privacy policy until an individual specifies their own specific consent directives.
- The individual (consenter) may grant, withdraw, or withhold consent for the collect, access, use, or disclosure of their IIHI, within the limitations established by the jurisdictional consent model.

Actors

See also: Actor definitions

- Jurisdictional Authority
- Consenter
- Substitute Decision Maker (SDM)
Manage Consent Directives

The Consenter, an individual or Substitute Decision Maker (SDM) uses a Consent Directive management system (also referred to as a Consent Directives Management Service or CDMS) to manage the consent rules that are used, in conjunction with Jurisdictional defaults and imperatives, to control what, if any IIHI may be shared with healthcare providers, payers, and others. The CDMS may be embedded in the PHR-S, EHR-S or in any other healthcare platform and access to IIHI may be via any of those systems.

Pre-conditions

- The Consenter will have an access to a set of enumerated consent options that are appropriate for that jurisdiction, either directly or via a "Consent Registrar" that has the authority to act as a proxy for the Consenter.
- Each option will have a jurisdictional default selection or value associated with it.
  - The above pre-condition relies on the ability of the web portal to access jurisdictional/organizational policies.
- An authenticated Consenter and Client identity have been established.
- The consent directive options must be comprehensible by the Consenter (i.e. consent must be knowledgeable and informed).
- The consent directive options must allow the Consenter to establish, withhold, or withdraw consent to collect, access, use, and disclose their IIHI (contained within the PHR-S, EHR-S, or other system) within the limitations established by legislation and/or jurisdictional/organizational policy.
- The individual has a trusted relationship with the organization(s) that is providing the CDMS capability.
- [appropriate only for the Request eConsent for a Client scenario below] The individual has established a PHR with a vendor and the Consenter (if different from the individual) has gone through a registration process with the PHR vendor in order to establish their identity and relationship to the individual.

Basic Scenario

- Consenter accesses a Consent Directives Management System via a publicly-accessible Web Portal.
- The Consenter is allowed to add, modify, or revoke consent directive regarding the disclosure of the IIHI contained within his/her Client Health Records.
- Verify that added or modified consent directive rules do not conflict with existing federal or local rules.
- The CDMS will include default jurisdictional policy rules that are applicable across all requesting organizations. Other organizational or local jurisdiction policies must be applied by each consent requester. The user must not be able to disable the directives derived from these default jurisdictional policies.
  - For example, specific client consent policies are required for Alcohol and Substance Abuse information, as specified by 42 CFR, Part 2.

Actors

See also: Actor definitions

- Consenter
- Consent Registrar
• Consent Directives Management Service (CDMS)

Request eConsent for a Client

An Information Requester retrieves a client's eConsent to determine the permission to collect, access, use, or disclose client health records as governed by the client's eConsent and the policies of the requester's organization and/or governing jurisdiction.

Pre-Conditions

• An authenticated Client identity has been established.
• The Consenter may be SDM acting on behalf of a Client.
• Access control must apply to requests for this data.

Basic Scenario

• The Information Requester uses the client's identity to query the CDMS Registry (if available) and discover the location of the specific CDMS that stores the client's eConsent.
• Query the CDMS and retrieve the client's eConsent.
• Reconcile client’s eConsent with Information Requester’s organizational and jurisdictional consent rules.
  o If the client’s eConsent contradicts the organizational or jurisdictional policies, then Information Requester must flag conflict and attempt to reconcile the differences.

Alternate Flow

• There are no consent directives for the client, or no registered CDMS.
• Apply only the organizational and jurisdictional rules applicable in the Information Requester's jurisdiction.

Post-condition

• The client’s eConsent is retrieved, if available
• If the client's eConsent and the organizational directives cannot be reconciled, the client may sign a waiver or refuse medical services.

Actors

See also: Actor definitions

• Information Requester
• Consent Directives Management Service (CDMS)
• CDMS Registry
• Client

Provider Requests Client Health Records

A healthcare provider requests access to the client's medical history, medication list, problems, allergy, etc. stored in a client's health records. Prior to disclosing the requested IIHI, the consent directives associated with that client are evaluated, in conjunction with jurisdictional/organizational...
imperatives and default rules. Based on the evaluation, the entire request may be satisfied, partially satisfied, or completely denied. In cases where the request is partially satisfied or completely denied, an optional notification may be given to the provider to indicate that some or all of the information requested information has been withheld.

Basic Scenario

- Invoke use case: Request Consent Directives for a Client.
- Query the Health Records Repository (or repositories) to retrieve client’s health records including Individually Identifiable Health Information (IIHI)
- Invoke use case: Consent Directives Filter Health Record Information
- Use the consent directive rules to filter the client health records allowing only content appropriate for the various type of professionals involved in direct care (e.g. nurses, physicians), supporting care (e.g. medical technicians, dieticians, etc), administration, and payment.

Sample Scenario: "Third Party Opinion"

Mary is registered with a disease management organization (DMO). Her DMO offers an advanced remote patient monitoring service that collects health information from a couple of health measurement devices installed at the client’s home. At the time of registration with DMO, Mary fills in a consent form as the EHR-S of the DMO supports the manage consent and authorization functionality as well as client privacy and confidentiality. This consent form (privacy policy) will govern the access and usage to Mary’s IIHI in the future. Mary specifies in her privacy policy that her data can be used for legitimate healthcare purposes by nurses at the DMO and that they could share it with her General Practitioner (GP). In addition to the client’s consent, there may be DMO privacy/security policy that together with the client specified consent may govern disclosure and usage of the client’s health data to third parties. Mary doesn’t do well in the program and develops a specific condition. Therefore, a nurse from the DMO wants to consult Mary’s GP. The nurse can share the health data collected by Mary in a secure way with Mary’s GP as she is allowed to do so according to Mary’s privacy policy. Since the EHR-S of the DMO has the functionality to support referrals, the nurse prepares her referral report which may include Mary’s demographics and vital signs measurements. The nurse forwards her referral report in protected manner (e.g. encrypting it) together with the client’s privacy policy and/or DMO privacy/security policy. These policies will govern the access and usage to her referral report. After successful authentication to his EHR-S system, the GP (or the specialist) notices a new message from the nurse, which contains Mary’s referral report. The GP clicks on the report and gives his opinion on Mary’s status. The application of the GP only allows him to view the report and not to forward it (as he is not allowed to do so according to Mary’s privacy policy). Note that if the nurse from the DMO sends the report by mistake to another care provider and not to Mary’s GP, that care provider will not be able to access the data as it is cryptographically protected.

Sample Scenario "Sharing Data with Fitness Coach"

Mary is concerned with her blood pressure and wants to more actively manage her health; hence she registers with a PHR-S service (e.g. WebMD, Microsoft Health Vault etc.) where she can upload her blood pressure, activity and other measurements data related to her health. At the time of registration with PHR-S, she fills in a consent form as the PHR-S supports the manage consent and authorization functionality as well as client privacy and confidentiality. This consent form will govern the access and usage to Mary’s personal health data in the future. After collecting her blood pressure (BP) for a month and confirming her fears Mary registers with a disease management organization (DMO) to get help in managing her hypertension. Mary updates her privacy policy allowing access to her data for legitimate healthcare purposes by a nurse at the DMO. Mary takes
her BP by herself and uploads it in combination with other measurements data such as her weight to the PHR-S. The nurse at the DMO logs in and authenticates successfully to the PHR-S system. The nurse can view Mary’s self reported data according to her privacy policy. The nurse examines Mary’s self reported data and at one point suggests her to register with a health and wellness centre to decrease her blood pressure. Mary registers with a fitness service. In addition, Mary modifies her privacy policy in order to allow a fitness coach to view parts of her personal health data. Since the PHR-S has the functionality to support referrals, the nurse prepares her report which may include vital signs and other demographic data. The nurse forwards her referral report in protected manner (e.g. encrypting it) together with the client’s privacy policy that governs the access and usage to her referral report. After successful authentication to his fitness application, the fitness coach notices a new message from the nurse at DMO, which is the referral report for Mary. The fitness coach prepares a personalized program for Mary. The fitness coach application only allows the fitness coach to view Mary’s report and selected data from her PHR. However his application does not allow him to view the other data at her PHR and to further disclose (e.g. forward) the referral and the selected data as specified in Mary’s privacy policy.

Post-condition

- The Provider's EHR-S stores a copy of the client's health record that was created by that provider. This information must be retained for legal reasons.
- The Provider's EHR-S must update the client's health record in the PHR Repository with the new data that was created by the provider. The Provider must flag the personal health records created during the visit and the Individually Identifiable Health Information (IIHI) contained in it according to the clients’ eConsent.

Actors

See also: Actor definitions

- Provider's EHR System (EHR-S)
- PHR Repository

Information System Masks Health Record Information based on Client Preferences

Filtering mechanisms and algorithms are required that apply eConsent rules describing the client’s preferences to that individual's client health records. Consent directives may include restricted access filters that are applied to a category of health information (e.g., all HIV related information). A consent directive may also require that individually identifiable health information is "masked" to protect the client's sensitive information.

A provider's (functional) role is based on their relationship to the client and their (structural) role within the organization. For example, a member of the immediate care team may be a physician, nurse practitioner, etc. These users may be allowed to see and update the client health records while other clinicians (e.g. laboratory medical technicians, consulting physicians, etc.) will be allowed access only to the information intended for their use (e.g. laboratory order or consult request).

Pre-conditions

- An individual, through their consent directive, may be able to exclude or include specific types of users of client health records based on various criteria (e.g. exclude a physician who happens to have a personal relationship or a certain role within the provider organization).
• A provider requests a client’s health record in order to care for the individual. The information may be provided in the form of structured or unstructured clinical documents.
Basic Scenario

Depending on whether the information is structured or unstructured, masking client health records may be applied at the document level, or on document sections. Structured information and coded information may be masked or filtered at the data element level. Unstructured information can only be filtered or masked at the document or document section level.

Actors

See also: Actor definitions

- Consent Directives Management Service (CDMS)
- Information Requester

Information System Flags Masked Health Record Information

Local policies may determine whether an authorized provider can know that restricted information is available in the client health record when it was masked by the Client's eConsent or local privacy policies. When the policy allows the provider to know masked information exists, the provider may access masked information with Consenter's approval (by entering a shared secret) or by "breaking the glass" in an emergency. "Breaking the glass" occurs when a provider who is authorized by organizational policy or jurisdictional law overrides the client’s dissent.

Pre-condition

Based on local policy rules, provider may or may not know that a set of individually identifiable health information was masked as a result of a client’s preferences. Some jurisdictions may eliminate the option of breaking the glass by not allowing providers to know that they cannot access is otherwise included in the client’s health records.

Basic Scenario

If the consenter authorized a specified type of provider (e.g. one involved in supporting care services) to access specific parts of the client health record but not other parts, the IIHI Repository will provide the information allowed in the consent and provide flags indicating that other types of IIHI was excluded (e.g. flag that substance-abuse-related information exists). In case of an emergency or based on consenter's approval, the provider may retrieve the masked information, thus "breaking the glass".

- A provider's use of restricted information upon may be limited to read-only for a specified time period, after which the consent approval will expire.
Actors

See also: Actor definitions

- Healthcare Provider
- Consent Directives Management Service (CDMS)
- Health Records Repository

Provider Amends Client Health Records based on Client’s Consent Directive

If the client requested it, the provider will update the client health records stored at a location specified by the client at the end of a visit, encounter, procedure, etc. The provider agrees to update the client's health records before the client agrees to receive medical services.

Pre-condition

- The provider's role and/or other attributes allows them to use (create, read, update, and delete) information in the individual's client health record from an organizational perspective.
- The individual's consent preferences allow the provider to use clinically relevant information contained in the client health record.

Post-condition

- The provider produces additional information as a result of treating the client.
- The client’s health records are updated in the Health Records Repository.
- It must be possible to interpret the information added to the client health records such as a system can correctly differentiate information that may be sensitive under jurisdictional, organizational, or under client’s own eConsent preferences.

Actors

See also: Actor definitions

- Consenter
- Provider
- Provider’s Electronic Health Record System

Request Privacy Policies from Organization or Jurisdiction

In order to correctly manage individually identifiable health information, various EHR-S will need to have access to computable privacy policies. Similarly, CDMSs will require access privacy policies to establish what type of control the owner of the information has placed on that IHHI.

Pre-condition

- Clients have trusted digital identities
- Jurisdictional Authorities (national, state, etc.) and other organizations issue privacy policies that apply to client health records (including IHHI).
- These polices may vary from national to state/province to local/organization. They may also vary across organizations or states/provinces.
• A system is required to evaluate/access the policies that apply in a jurisdiction or organization
• Privacy policies are available in electronic form and may be used by EHR-Ss and CDMSs to determine how to manage client health records in accordance to privacy policies and consent directive.

Basic Scenario

• Based on a user request, a system sends a query for current privacy policy rules that apply in a jurisdiction or organization.

Post-condition

• The requesting system receives a copy of the policy rules for the designated organization or jurisdiction

Actors

• Policy Directory or a Policy Management Service
• Requesting system (e.g. CDMS)

Provide electronic Consent Directive (eConsent) to a specific healthcare provider/service

In many situations it is necessary to provide a set of computable consent directives along with client health records in order to make sure that the receiving system and its user observe the privacy preferences of the client.

Pre-condition

• An authenticated consenter identity has been established
• The consenter can also be a substitute decision maker (SDM)
• The options provided by the eConsent directive must be understandable to the consenter in such a way that it allows them to take control of their health records.

Basic Scenario

• The consent directives are sent to the EHR-S/PHR-S receiving system. The system can then request client health records according to consent directives.
• Consenter shall be able to specify, update or revoke his/her consent regarding the use and disclose of his client health records.
• Consent directives may be translated into machine-readable polices so that they can be used to govern access to healthcare data.

Sample Scenario: Substance Abuse

A client receives substance abuse treatment at facility A. As the needs of the client evolve, facility A refers the client to facility B. Facility A requests permission from the client to forward to facility B the relevant assessments and notes to ensure a smooth transfer of care. The client signs a consent upon which the information is transferred on condition that facility B may not forward this information
and may use it for predetermined length of time (e.g. 30 days, 60 days) after which the information must removed.

Sample Scenario: Remote Monitoring

Consenter registers with an organization e.g. Disease Management Organization (DMO) which uses a remote patient monitoring service to collect health information from health measurement devices installed at client's home. During the time of registration, client fills in an eConsent form on the application hosting device (e.g. home PC, mobile phone, or dedicated medical hub) at his home. The eConsent form consists of the options regarding who will be able to access, use, update and disclose different types of vital signs that are collected by the remote client monitoring system. The eConsent form is then sent from his/her application hosting device to the DMO service. The eConsent directive governs access to the client data at the DMO and if client data is sent to third parties (given that this is allowed, e.g. to a client's PHR), the eConsent will be included and sent with the data. This might require reconciliation of different eConsent directives (which are given to different services).

Post-condition

- An electronic Consent Directive is available to the provider/service that becomes responsible for treating the client along with relevant client health records.

Actors

- Consenter (client)
- Consent Directive Management Service (CDMS) of a healthcare service (e.g. DMO)

See also: Actor definitions

Client provides verbal consent at point of service

This use case involves a provider who has been restricted from accessing a client's IIHI by the client's consent directive. The provider attempts to retrieve the individual's IIHI with the individual present and is denied. The provider receives an indication that there may be more information contained in the clinical repository, but access to that information has been restricted by the individual's consent directives.

The provider explains reasons for wanting access to the information to the individual and after some discussion, the individual provides verbal consent to have the IIHI disclosed to the provider.

Assumptions

- Records that are masked as a result of the evaluation of a Consent Directive will remain masked for other requests throughout the period the user is given access to the records.
- Override with consent allows only the user who initiated the request to access the masked records unless the person consents to allowing others e.g. user delegates, to also view the masked records.
- The duration of permission to view the masked data will be determined by relevant legislated and policy requirements as well as jurisdictionally specified criteria. Within that duration, the same user may re-access the data multiple times.
• The override will not create a “temporary” Disclosure Directive, but will need to accompany each subsequent request for the previously masked information.
• Policies will need to be implemented regarding the copying and sharing of masked data that is disclosed for a limited time to a specific user or users.
• Policies and protocols will need to be developed and implemented identifying the obligations of the provider to ensure that knowledgeable, informed consent is obtained without coercion or misrepresentation.

Pre-condition

• An individual has active consent directives that prevent disclosure of IIHI to a Provider.
• The provider has unsuccessfully attempted to retrieve the individual’s IIHI.
• The Provider has asked for and received the client’s verbal consent for disclosure of IIHI.

Basic Scenario

• The Provider requests access to a clinical profile of any IIHI sent to the EHR-S in the past month for the client.
• The system retrieves the requested information, but masks some of the information based on the evaluation of the client’s Consent Directives. It displays a message indicating that some or all of the information has been masked as a result of the decision of a client or substitute decision maker. The system also provides an option for the provider to override the masking decision.
• The Provider asks the client if they’d be willing to identify the general nature of the information that has been masked in order to determine if any of it might be relevant to the current encounter.
• The client reveals the nature of the information as requested.
• The Provider asks for the client’s consent to override the Consent Directive and remove the mask from the information. The Provider explains the potential risks and identifies how the requested information will be used.
• The client provides verbal consent to the temporary disclosure of all of her individually identifiable health information to the Provider.
• The Provider selects the “Override” option.
• The system displays a screen with a selection of override reasons and an input area for ad-hoc text. One of the override reasons is “Client has provided express consent for the temporary disclosure of individually identifiable health information”.
• The Provider selects the option described in the previous step and submits the request.
• The system ascertains that the client has previously established a shared secret and responds with a message asking the client to enter their shared secret.
• The Provider asks the client to enter their shared secret into the system.
• The client enters the shared secret and the screen displays asterisks for each character entered to hide the shared secret from display.
• The Provider submits the request, which transmits a query to the client’s health record, with the override attached. The override indicator and shared secret are retained by the EHR-S or Point of Service system in order to resend when necessary for the appropriate duration.
• The system responds by
  o Notifying the provider of the success/failure of the Override request
  o Displaying requested information
  o Logging the override request in the Secure Audit Service log.

Post-condition
• The information that had been previously masked, for that provider, are temporarily unmasked.
• Once the access duration expires, the mask is reapplied for further access requests.

Actors

See also: Actor definitions

Provider Requests IIHI from another Jurisdiction

This use case involves the transfer of IIHI from one jurisdiction to another, while respecting client preferences where possible and complying with privacy legislation and policy established in both jurisdictions. Only relevant information will be sent to the provider based on the Consent Directives of the client.

Specialization/scenario for #Provider Requests IIHI

Pre-condition

• Any necessary data-sharing agreements have been put into place between jurisdictions involved in the cross-border transfer of individually identifiable health information.

Basic Scenario

A client from Ontario is visiting her aunt in Saskatoon for the first time. She develops throat pain and difficulty swallowing and decides to visit the local walk-in clinic in case she needs an antibiotic. The clinic has no records for the client. She does not have a Personal Health Number (unique identifier) in Saskatchewan. She has no records in the Saskatchewan EHR-S. She advises the receptionist that the doctor should be able to "see all of her records in Ontario" using his own computer.

Post-condition

• An EHR record, Consent Directive, and shared secret exists for the client in the Saskatchewan EHR-S
• An Ontario Consent Directive expressly allowing the transfer of the client’s individually identifiable health information exists and is active until it expires.

Basic Flow

• The receptionist registers the client and creates their Saskatchewan (SK) EHR
• The receptionist uses an EHR-S function to resolve the client’s client IDs between Saskatchewan and Ontario.
• The provider requests access to the person’s records in the Ontario EHR
• The EHR-S forwards the request to the Ontario EHR-S.
• The Ontario EHR evaluates the consent status for this client and determines that no extra-jurisdictional Consent Directive exists that would expressly allow disclosure of individually identifiable health information. The Ontario EHR-S denies the request.
• The Saskatchewan EHR receives notification that access to the Ontario records is denied and displays that notice to the provider. There is no electronic option for the provider to override that decision.
The provider gains the client’s express consent and places a call to the client’s family practitioner or other Ontario Consent Registrar and asks that a Consent Directive be created on the client’s behalf to allow the disclosure of her IIHI outside of Ontario.

The Consent Registrar verifies the client and provider identity and the provider’s credentials and executes Manage Consent Directives on behalf of the client, setting the Consent Directive to expire on the client’s expected date of return to Ontario. The Consent Registrar confirms the creation of the new Consent Directive with the provider.

The provider re-issues the request to access the person’s records in the Ontario EHR-S

The system forwards the request to the Ontario EHR.

The Ontario EHR evaluates the consent status and determines that the disclosure is allowed. The Ontario EHR discloses the client’s individually identifiable health information to the Saskatchewan EHR and records an audit event of the transaction.

The Saskatchewan EHR-S receives the client’s individually identifiable health information and displays it to the provider who treats the client appropriately.

The client is concerned that her individually identifiable health information now in the Saskatchewan EHR might be used inappropriately and asks to create a Consent Directive in Saskatchewan to mask her entire EHR and establish a shared secret to allow her to control access as required.

**Actors**

- Consenter
- Provider
- Home Jurisdiction Consent Registrar

See also: [Actor definitions](#)

**Request for Pre-Fetch of Diagnostic Imaging (DI) Exams**

**Pre-condition**

A regional or jurisdiction DI Repository maintains DI Exam results and reports to enable sharing between a number of healthcare delivery organizations.

This appears to be a Diagnostic Imaging domain-specific scenario for [#Information System Flags Masked Health Record Information](#)

**Basic Scenario**

A referring physician schedules a DI exam for her client at a facility associated with a regional DI Repository. The client has placed a consent directive on her IIHI restricting disclosure to only the referring physician. The scheduled exam is sent to the Radiology Information System (RIS) system for filling. The RIS system notifies the Picture Archiving System (PACS system) and the DI Repository in order to pre-fetch any relevant prior exams.

**Post-condition**

The decision to transfer the relevant prior exams to a local DI cache will be based on data sharing agreements between the Repository and the requesting organization, and the privacy policies in place at both locations. At least two options exist:
The relevant prior exams are transferred, but marked as masked. When the Radiologist attempts to open them, the PACS viewer interprets the masked attribute and enforces the directive unless the Radiologist determines that it is medically necessary and within his authority to override the client's restriction (see Break Glass).

The relevant prior exams are not transferred, but a stub record is transferred to the local RIS/PACS system. Should the Radiologist have the authority and legally acceptable rationale to do so, he can override the Consent Directive (see Break Glass).

Actors

- Consenter Referring Provider Radiologist See also: Actor definitions

Provider overrides Consent Directive (Break Glass)

A client is brought to the local hospital ER by ambulance in an unconscious state. She appears jaundiced and minimally responsive. Identification found on her person is used to confirm her identity. While the ER physician is dealing with the client's immediate life threats, he requests the ER Charge Nurse to access and review the client's records in the EHR. The Charge Nurse logs onto the EHR-S and validates the client's identity. She attempts to access the client's IIHI and receives a message that states "There are masked records that were not returned." The ER physician asks the nurse to submit an override request invoking an emergency situation.

Assumptions

- Only authorized users whose assigned role(s) includes override privileges will be permitted to submit an emergency override request.
- Emergency override may be used to override all existing Consent Directives or only those specific to certain IIHI that the user has a need to access e.g. to support clinical decision-making.
- The reason for emergency override will be provided by the authorized user requesting the override and will be logged in the EHR-S.
- Emergency override may allow only the authorized user who requested the override to view the masked/restricted data or may allow a group of authorized users e.g. in a facility or department to view the data.
- All the patient health data are recorded into the client health record (note that this is not always the case, since consent directives can prevent the collection of some data into the client health record).
- The EHR-S knows there are masked records.
- The jurisdiction rules allow masked records to be revealed.

Pre-conditions

- An active Disclosure Directive exists that will restrict disclosure of individually identifiable health information to the provider.
- The provider has been authenticated in the EHR-S and is currently logged on.
- The provider has been granted the authority by the jurisdiction to override a client's Consent Directives without their consent under certain, defined circumstances.

Basic Scenario
The nurse requests access the client’s IIHI.

The system retrieves the requested information, but masks some of the information based on the evaluation of the client’s Disclosure Directives. It displays a message indicating that some or all of the information has been masked as a result of the decision of a client or their substitute decision maker. The system also provides an option for the Nurse to override the masking decision.

The ER nurse selects the Override option.

The system displays a screen with a selection of override reasons and an input area for ad-hoc text. One of the override reasons is “To prevent the risk of serious bodily harm” (or similar language provided by the jurisdiction). The screen also displays a message advising that:

- The override event will be logged in the EHR-S Secure Auditing Services including the reason for override
- A notice will be sent to the Chief Privacy Officer (CPO) of the hospital who will then notify and follow-up with the person whose directives are being overridden.

The nurse selects the option described above, and enters some text in the text area indicating the client’s condition and identifies the physician on whose behalf she is submitting the request. The override request is submitted to the system.

The system responds by:

- Creating and transmitting a record of the override to the Security Audit Service, which would likely initiate an alert to the appropriate Chief Privacy Officer for follow up.
- Notifying the nurse if the override was successful/unsuccessful
- Displaying with the requested information.

At the end of the nurse’s session, she logs out. Her access privileges to view the previously unmasked data are terminated either at that point, at a later time as specified by jurisdictional emergency override rules (e.g. for 24 hours post-override).

**Post-condition**

- Other than the ER Nurse, requests for the client’s IIHI continue to be masked based on her active Consent Directive(s).
- Once the override period has ended, the ER Nurse’s no longer has the authority to access the client’s IIHI without re-executing the use case.

**Actors**

See also: [Actor definitions](#)

**Accounting for Disclosures**

Specifying the need to account for disclosure is enforced by the Composite Privacy DAM by setting Obligation.code = "AuditDisclosure".

Presently, informal surveys of AHIMA membership have revealed that in the 6 years that the HIPAA Accounting of Disclosures requirement has been in place only about half of our members have ever been asked to provide an Accounting of Disclosures to a patient. And, of the survey responder population; approximately half have only prepared an Accounting of Disclosures one time. All responders that report having prepared an Accounting of Disclosures concur that the process of preparing the Accounting of Disclosures is very time consuming, labor intensive, and expensive. The same group reports that in the majority of cases the patient is disappointed. Further research is...
needed to determine exactly why the patients are disappointed. Anecdotal justifications for patient
disappointment point out that the patient does not want to know that their nurse or the lab tech has
appropriately viewed their records X number of times; they want to catch individuals in the act of
breaching their records. So, the current process is expensive and time consuming and the patient is
not always happy with the findings. Finding a way to make Accounting of Disclosures compliance
easier would be welcomed by all stakeholders.

Each disclosure event would be logged. The log entries would contain the date of the request, the
requesting party identification, and the purpose. The log entry would match the information criteria in
the consent directive. Meeting the HIPAA content requirements for a Accounting of Disclosures. It
would be easier to capture, archive, and report the Accounting of Disclosures if it used the general-
purpose audit mechanism but an enhanced audit entry.

Presently the current information that must be provided in an Accounting of Disclosures by HIPAA are:

- Date of disclosure
- Name of the person or organization that received the information
- Recipients address (if known)
- Brief description of the PHI disclosed
- Brief statement explaining the purpose of the disclosure.

Pre-conditions

A healthcare provider discloses information to another provider in accordance to privacy policies and
patient consent directives. The disclosure event is recorded in a log in a way similar to other types of
events.

Basic Scenario

A patient requires an accounting of every disclosure of IIHI by specifying it as an element of their
consent directive.

Once the provider organization accepts the consent directive of the patient, the provider organization
automatically generates a report based on the disclosure log entries that have been stored over time.

Actors

See also: Actor definitions

Actor Definitions

These actors are used in all CBCC use cases, with a common meaning and definition.

Consent Directives Management Service (CDMS)

Repository and associated services for creating, maintaining, and evaluating consent directive rules
( Abbreviated term as used in ISO/IEC 29101).
CDMS Registry

Registry and location identifier of authorized consent directive management services.

Consenter

Consumer or Substitute Decision Maker (SDM) who has rights for controlling IIHI content.

Consent Registrar

A person, other than an SDM who has been assigned the authority to act on behalf the Consenter when the Consenter cannot directly manage their own directives.

Consent Requestor

Person or organization requesting access to PHI, may be a heath care provider, insurance payer, research organization, government agency, or other authorized party.

Jurisdictional Authority

Jurisdictional Authority assigns the right to control protected health information and determines default jurisdictional consent rules. See also: Jurisdiction.

Patient

Consumer who is subject of IIHI and received medical services in the past. This is a role played by a consumer in relation to a provider organization or licensed providers.

IIHI Repository

Repository of Individually Identifiable Health Information (IIHI). General actor that includes EHR Systems, EMR Systems, PHR Systems, and other health platform repositories and portals.

Provider

A healthcare organization that is providing services to a Patient.

Substitute Decision Maker (SDM)

A person who is authorized under legislation to consent on behalf of the patient/person (See also: Glossary definition).
Appendix B: Consent Directive Lifecycle

The following diagram illustrates the lifecycle of a client's consent directive as a state machine. Each block represents a possible state of a consent directive and each arrow represents a possible state transition. The information between "[]" represents the condition that must be true in order to allow the state transition to occur. In this example a consent directive may be explicitly revoked or revised by the client anytime for any reason. A consent directive expires under specific circumstances at the end of its effective time period.

Figure 18: Consent Directive Lifecycle

If a Consent Directive is explicitly revoked, the consenter may provide a reason for the action (e.g. "RevokationReasonCode"). The reason may be encoded to ensure semantic interoperability.