HL7 Finland ry: CDA 2011 projekti

Suostumusten ja kieltojen kehityslinjat CDA R3:ssa

Versio 1.00
13.1.2012

Versiohistoria

Versio:	Pvm:	Laatijat:	Muutokset:
0.00			Dokumenttipohja
0.10-0.X0	10.11.2011	TS	Työversioita
0.30	29.11.2011	TS	Versio HL7 yhdistyksen avointa kommenttikierrosta varten
1.00	13.1.2012		Versionumero päivitetty, kommenttikierroksella ei tullut kommentteja.

TK = Timo Kaskinen, Salivirta Oy
TS = Timo Siira, Salivirta Oy
JN = Jarkko Närvänen, Salivirta Oy

SISÄLLYSLUETTELO

1. JOHDANTO

1.1 Työn tausta ja lähestymistapa

Työdokumentti on osa HL7 Finland ry:n CDA 2011 -projektia, jonka tehtävänä on raportoida CDA R3 -standardin hyödyntämisestä ja muutoksista CDA R2-standardiin. Yhtenä tehtävänä oli kuvaus suostumuksiin ja kieltoihin liittyvien tietojen linkittämisestä CDA R3-määrittelyihin.

1.2 Tavoite ja kohderyhmä

Tavoitteena on kuvata kansainvälistä tilannetta siitä, miten suostumuksia ja kieltoja on ajateltu käsiteltävän CDA R3:ssa.

Työdokumentin kohderyhmänä ovat ne henkilöt, jotka miettivät, suunnittelevat ja toteuttavat ratkaisuja terveydenhuoltoon liittyviin suostumuksiin ja kieltoihin.

1.3 Rajaukset ja oletukset

Työdokumentissa ei ole kuvattu sitä, miten suostumuksia ja kieltoja on käsitelty terveydenhuollon ratkaisuissa, vaan pyritään kuvaamaan, miten CDA R3:ssa ne on ajateltu ratkaistavan. Lukijoiden oletetaan tietävän perusasiat CDA R2:sta sekä muita tapoja, joilla suostumuksia ja kieltoja on pyritty ratkaisemaan (esim. IHE BPPC).

1.4 Viitatut lähteet

[1]	HL7 Version 3 Domain Analysis Model: Medical Records; Composite Privacy Consent Directive, HL7 Draft Standard for Trial Use, Release 2, February 2010, (Updated April 15 th, 2010 to include an additional appendix on the Consent Directive Lifecycle)
[2]	HL7 Implementation Guide for Clinical Document Architecture, Release 2: Consent Directives, Release 1, HL7 Draft Standard for Trial Use, January 2011

2. SISÄLTÖ

2.1 Taustaa

CDA R3 –standardin julkaisu on viivästynyt eikä tämä työdokumentti perustu valmiiseen standardiin, vaan kahteen standardiluonnokseen, jotka on julkaistu koekäyttöä varten. [1 ja 2]

Standardiluonnoksissa esitetään yleiset periaatteet yksityisyyden suojan käytännöille ja suostumusten hallinnalle [1], sekä soveltamisopas CDA R2:sta varten [2].

2.2 Standardiluonnosten sisältö

HL7 Custodian Work Group on julkaissut alakohtaisen analyysimallin (DAM, Domain Analysis Model), jonka kohteena on Medical Records –alueen ohje, jossa on yhdistetty yksityisyyden ja suostumuksen hallinta (Composite Privacy Consent Directive). Dokumentti on standardiluonnos koekäyttöä varten (DSTU, Draft Standard for Trial Use). [1]

Alakohtainen analyysimalli on määritelty seuraavasti:

> *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. [1]*

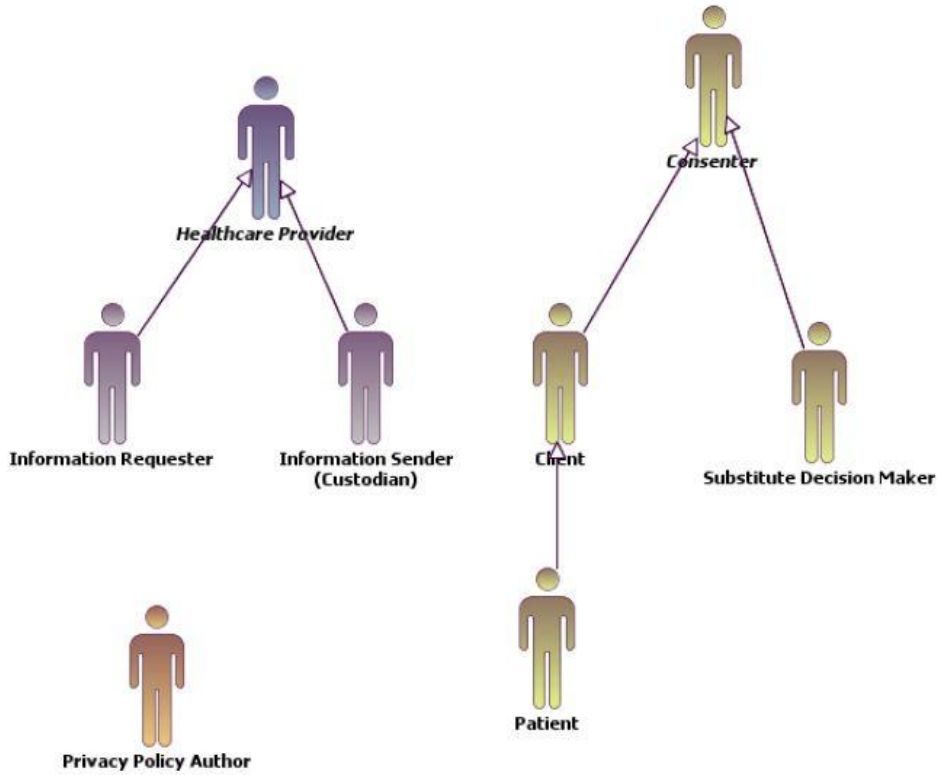
DAM on käsitteellinen malli ja sitä ei tule tulkita teknisenä määrityksenä tai alustariippumattomana suunnitelmana.

Standardiluonnoksessa kuvattu malli on syntynyt sen tuloksena, että on kuvattu eri sidosryhmien vaatimukset liittyen yksityisyyden suojaamiseen terveydenhuollossa. Vaatimukset kuvaavat tarpeen seuraavan sukupolven järjestelmien standartoidulle yhteentoimivuudelle vaihdettaessa yksityisyyteen ja suostumuksiin liittyviä ohjeita, joiden perusteella voidaan varmistua, että järjestelmät käsittelevät henkilökohtaista terveystietoa suunnitellulla tavalla. Standardiluonnos on syntynyt mm. the Substance Abuse and Mental Health Services Administration (www.samhsa.gov) tarpeista.

Käsitteellisessä mallissa on analysoituna toimijoita, käyttötapauksia, yksityisyyden suojaan ja suostumuksiin liittyviä tietoja, järjestelmien vuorovaikutusta ja aiheeseen liittyvää sanastoa.

Standardiluonnoksen [1] pohjalta on laadittu toteutusohje CDA R2:sta varten [2], jonka status on myös standardiluonnos koekäyttöä varten (DSTU).

2.3 Toimijat



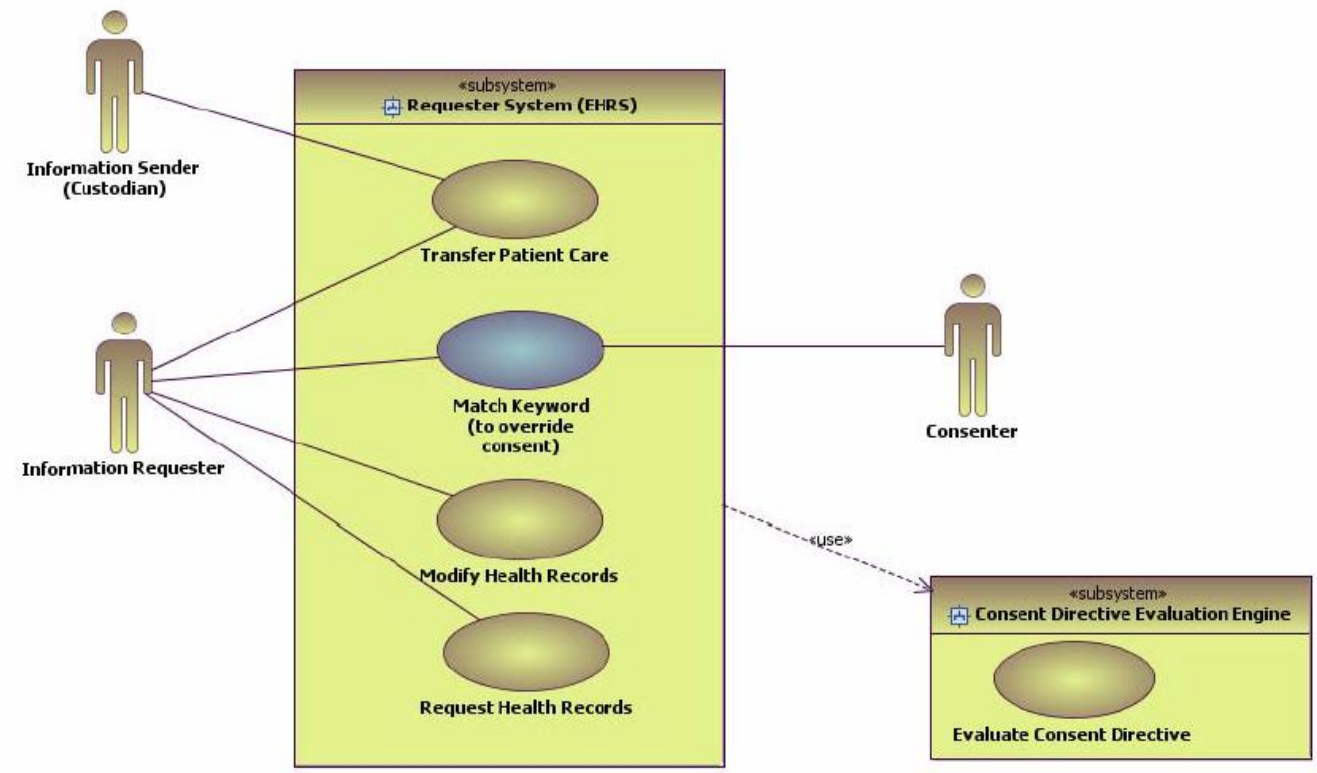
Kuva 1 Suostumuksen hallinnan toimijat

Toimijoita ovat palveluntuottaja (Healthcare Provider), joka voi tarvita potilaan tietoja (Information Requester) tai joka voi luovuttaa hallussaan olevia tietoja (Information Sender (Custodian)). Suostuja (Consenter), joka voi olla asiakas (Client) tai valtuutettu toimija (Substitute Decision Maker), joka voi olla esim. puoliso tai huoltaja. Potilas (Patient) on asiakas, joka vastaanottaa terveydenhuollon palveluita. Privacy Policy Author voi olla esim. alueellinen tai paikallinen viranomainen, joka määrittelee yksityisyyden suojaan liittyvät käytännöt lakien ja asetusten perusteella tai se voi olla organisaation ylläpitäjä, jos organisaatiolle on määritelty omat yksityisyyden suojaan liittyvät käytännöt.

2.4 Käyttötapaukset

2.4.1 Yksityisyyden hallinta

Alla olevassa kuvassa esitetään käyttötapaukset, joilla suojataan potilastietojen yksityisyyttä ja hallitaan niiden yksityisyyttä hätätilanteissa.



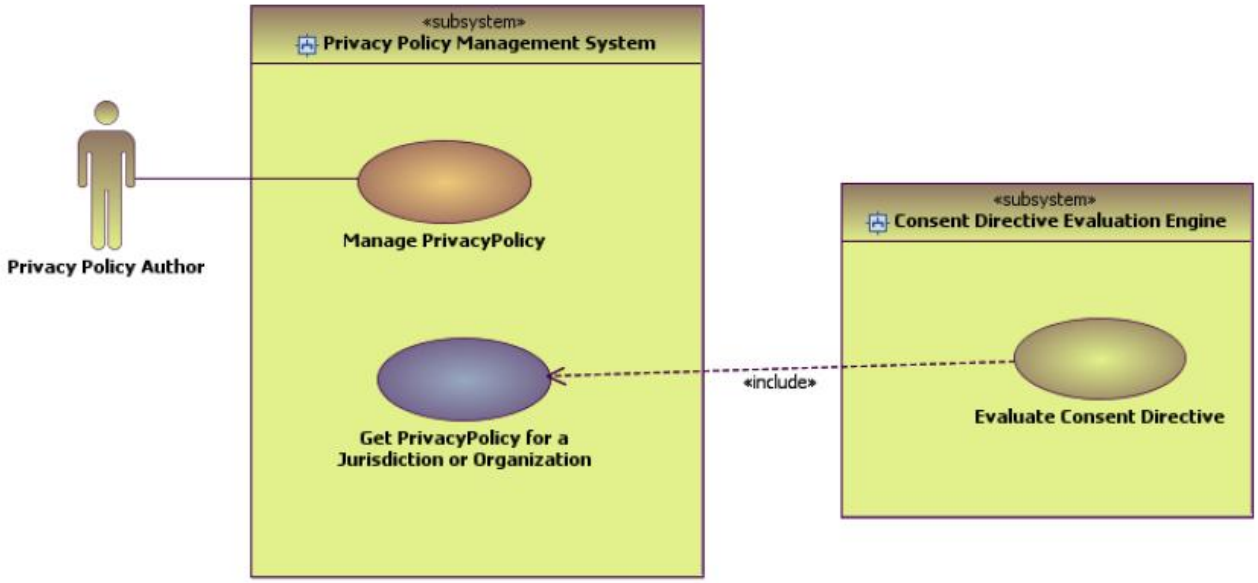
Kuva 2 Yksityisyyden hallinta

Evaluate Consent Directive –käyttötapauksessa tutkitaan suostumus, mitä tietoja suostumuksen antaja (Consenter) haluaa luovuttaa. Jos hän on kieltänyt joidenkin tietojen luovutuksen, niin järjestelmä voi näyttää, että tästä potilaasta on piilotettuja tietoja, jotka voi saada näkyville, jos suostumuksen antaja haluaa antaa palveluntuottajalle ”jaetun salaisuutensa” (Shared Secret), joka on salasana tai PIN-koodi. Palveluntuottaja voi hätätapauksessa (esim. akuutti hengenvaara) ohittaa suostumuksen järjestelmän ominaisuudella. Tästä käytöstä jää tieto järjestelmään ja tieto menee myös valvovalle viranomaiselle.

Esimerkki:
Potilas hakeutuu hoitoon toiselle palveluntarjoajalle, missä ei yleensä käy (esim. ollessaan sukulaisvirailulla toisella paikkakunnalla). Palveluntarjoaja hakee potilaan hoitotiedot sen mukaan, miten suostumuksessa on määritelty. Jos niistä näkyy, että potilaalla on jotain piilotettuja tietoja, niin palveluntarjoaja voi pyytää potilaalta niitä käyttöönsä, jos epäilee niiden olevan oleellisia tämän sairauden hoitamisen kannalta.

2.4.2 Yksityisyyden suojan käytäntöjen hallinta ja kyselyt

Alla oleva kuva esittää käyttötapaukset, jotka liittyvät yksityisyyden suojan käytäntöjen hallintaan ja kyselyihin.



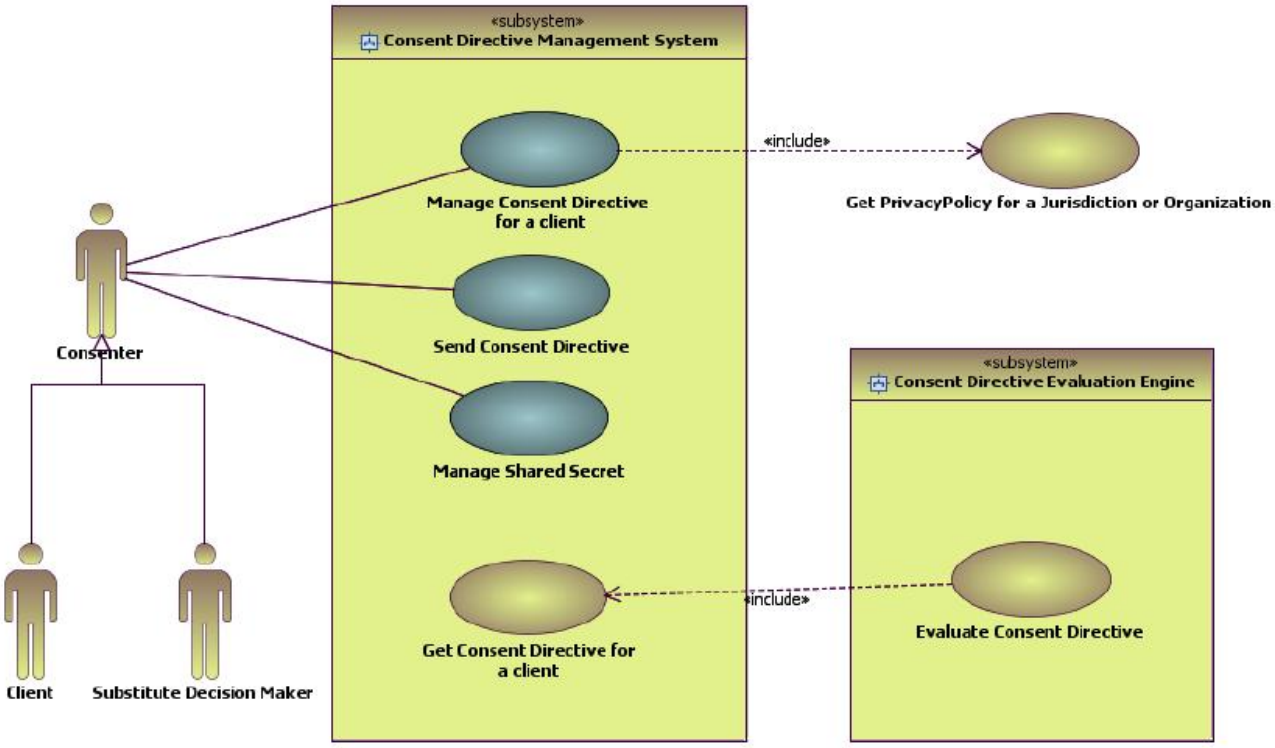
Kuva 3 Yksityisyyden suojan käytäntöjen hallinta ja kyselyt

Viranomaisen tehtävänä on pitää yllä yleisiä yksityisyyden suojaan liittyviä käytäntöjä. Suostumus sisältää yksityisyyden suojaan liittyvät käytännöt.

Esimerkki:
Yksityisyyden suojaan liittyviin käytäntöihin voidaan määritellä kulloinkin voimassa olevie lakien asettamat rajoitteet tietojen käytölle. Näiden lakien muuttuessa viranomainen muuttaa käytäntöjä vastaaman voimassaolevia lakeja.

2.4.3 Suostumuksen hallinta ja toimeenpano

Suostumusten hallintaan ja niiden toimeenpanoon liittyvät käyttötapaukset on kuvattuna alla olevassa kuvassa.



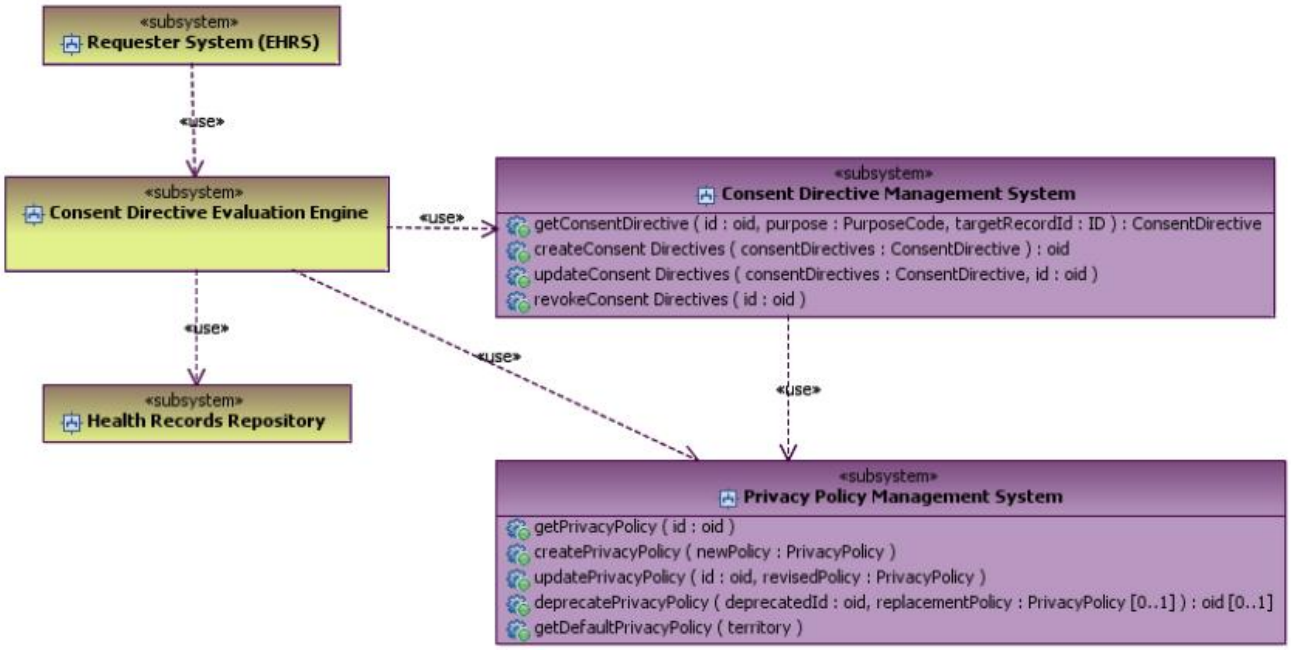
Kuva 4 Suostumuksen hallinta ja toimeenpano

Suostuja voi itse luoda ja hallinnoida omia suostumuksiaan, lähettää/ottaa käyttöön suostumuksensa ja hallinnoida ”jaettua salaisuuttaan” (salasana tai PIN-koodi). Suostumukset on aina johdettu yksityisyyden suojan käytännöistä, joita ei voi ohittaa.

Esimerkki:
Suostuja päättää ottaa käyttöönsä suostumuksen hallinnan. Hän kirjautuu palveluun ja rakentaa suostumuskäytäntönsä, joka jää palveluun saataville. Tällöin jonkun tarvitessa suostujan tietoja järjestelmästä tarkistetaan, minkälaiset suostumukset kyseisellä henkilöllä ovat voimassa.

2.4.4 Käyttötapausten toteutus

Alla olevassa kuvassa on käsitteellisellä tasolla kuvattu käyttötapauksien toteuttamiseen tarvittavat tietojärjestelmät ja niiden väliset riippuvuudet.



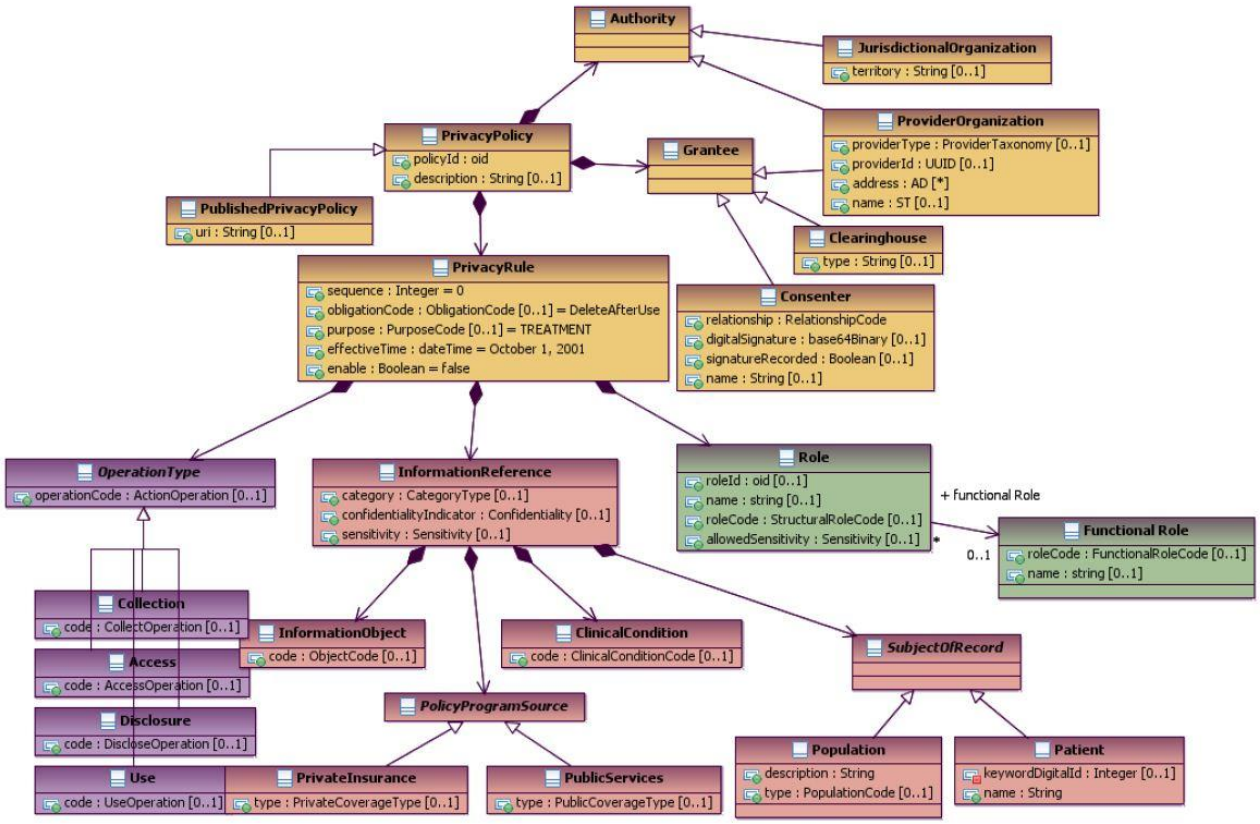
Kuva 5 Käyttötapausten toteutus

Tiedon pyytäjän potilastietojärjestelmä käyttää ”suostumuksen tutkimuskonetta”, joka käyttää suostumuksenhallinta- ja yksityisyydenhallintajärjestelmiä, joiden perusteella se saa tiedon, mitä tietoja se voi saada käyttöönsä toisesta tai keskitetystä tietovarannosta.

2.5 Yksityisyyden suojan käytäntöjen tietoanalyysi

Yksityisyyden suojan käytäntöjen (Privacy Policy) rakenne ja attribuutit, joita voidaan siirtää järjestelmien välillä on esitelty alla olevassa tietomallissa. Sama kuva on esitetty isommassa koossa liitteessä 1.

1. Yksityisyyden suojan käytännöt on ilmaistava alustariippumattomasti, koska tietoja joudutaan vaihtamaan hyvin erilaisten järjestelmien välillä.
2. Yksityisyyden suojan käytäntöjen on perustuttava standardeihin rakenteisiin ja terminologioihin, jotta ne voivat toimia eri organisaatioissa ja eri järjestelmissä.



Kuva 6 Yksityisyyden suojan yleiskuva

Authority on organisaatio, jolla on päätäntävalta määritellä yksityisyydensuojakäytäntö. Kyse voi olla viranomaisesta (JurisdictionalOrganization) tai palveluntuottajasta (ProviderOrganization).

PrivacyPolicy on pääluokka, joka sisältää säännöt (PrivacyRule), joita turvajärjestelmät valvovat. Ne toimivat pohjana suostumuksille. PublishedPrivacyPolicy ilmaiseen sen, mistä ihmisen luettavassa muodossa oleva yksityisyydensuojakäytäntö löytyy.

Grantee ilmaisee sen, kenellä on valtuuksia sallia tai rajoittaa tietoja, joita suostumus voi koskea. Näitä tahoja voivat olla suostuja (Consenter), palveluntuottaja (ProviderOrganization) tai välittäjä (Clearinghouse).

OperationType määrittelee käyttöoikeudet, jotka suostuja on myöntänyt tietyllä käyttäjälle asiakkaan terveystietoja varten.

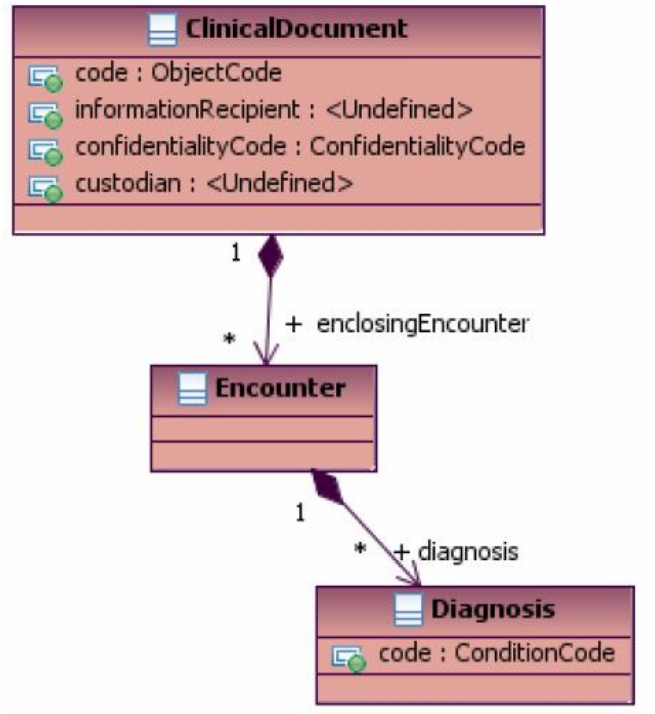
InformationReference määrittelee ne tietoelementit henkilökohtaisesta terveystiedosta, jotka ovat yksityisyydensuojakäytännön ja suostumuksen kohteina.

- InformationObject esittää viittaukset tietyntyppiisiin kohteisiin (esim. asiakirjat, tilaukset)
- ClinicalCondition tarkoittaa terveydentilaa, joka liittyy yksityisyydensuojakäytäntöön. Tila voidaan ilmaista standardin sanaston (esim. LOINC, SNOMED CT) mukaan koodattuna. Tällaisia voivat olle esim. (päihdyttävien) aineiden väärinkäyttö tai HIV-statukseen liittyvät tiedot.
- PolicyProgramSource määrittää terveyspalveluiden maksajan, joka voi olla yksityinen (PrivateInsurance) tai julkinen (PublicServices). Se voi vaikuttaa yksityisyydensuojakäytäntöön
- SubjectOfRecord luokkaa ei määritellä tarkemmin. Population-luokan avulla tietty käytäntö voidaan kohdistaa johonkin haluttuun väestön osaan.

Role määrittää tietojärjestelmän käyttäjän (tyypillisesti tiedon pyytäjästä). FunctionalRole määrittää esim. sen, että Organisaatiot A ja B voivat käyttää toistensa potilastietoja, jos heillä on olemassa sopimus siitä.

2.5.1 Yksityisyyden suojan käytäntöjen soveltaminen henkilökohtaisiin terveystietoihin

Oheisessa kuvassa esitetään kuinka järjestelmä voi käyttää ClinicalDocumentin koodattuja attribuutteja yksityisyyden suojan käytäntöjen valvontaan. Koodatut attribuutit voivat olla ClinicalDocumentin headerissa tai bodyssa. Koodauksen rakenteessa ja prosessissa tulee ottaa huomioon myös se, että tutkitaan onko kyseinen dokumentti jo koodattu vai ei. Tämän jälkeen koodauksesta voidaan tulkita, onko siinä haettaavaa koodia vai ei.



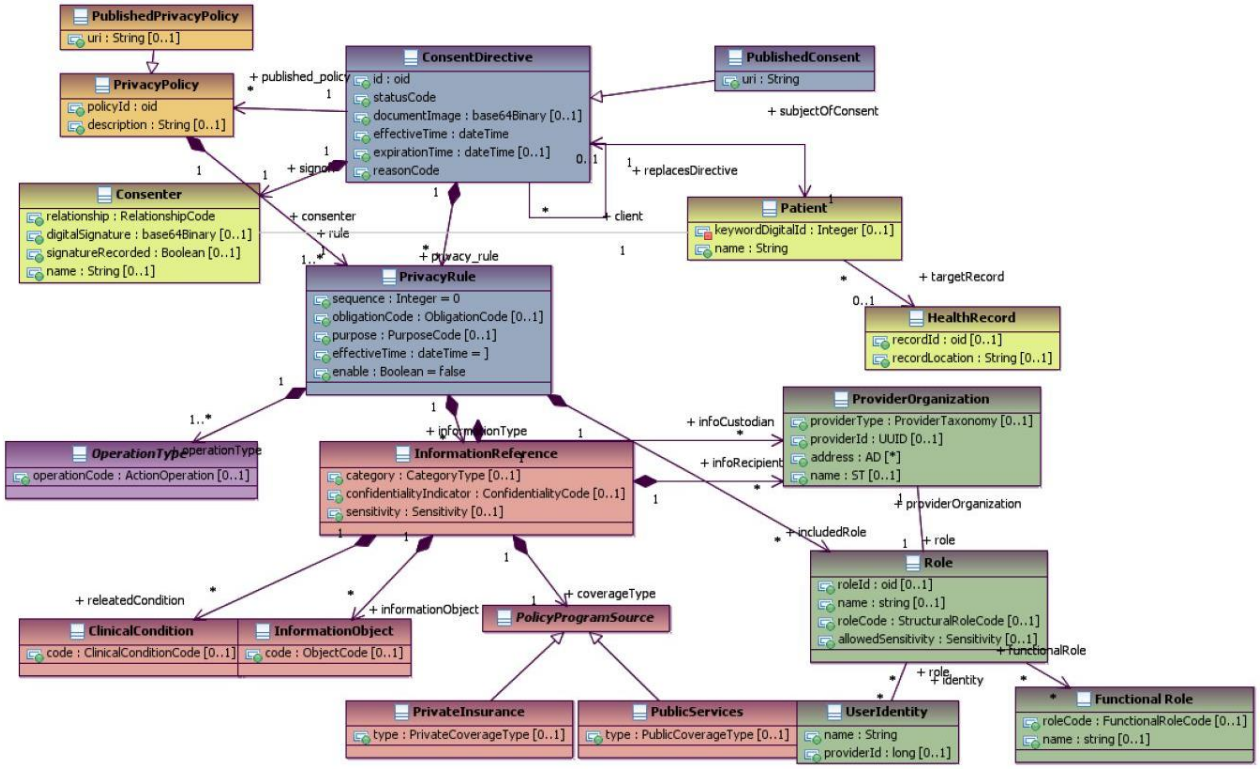
Kuva 7 Yksityisyyden suojan käytäntöjen koodaus

Riippuen siitä, onko asiakirja rakenteisessa vai rakenteistamattomassa muodossa, voidaan tiedot suojata joko asiakirjan (document) tai asiakirjan osan (document section) tasolla. Rakenteinen ja koodattu tieto voidaan suojata jopa tietoelementin (data element) tasolla. Rakenteistamaton tieto voidaan suojata vain asiakirjan (document) tai asiakirjan osan (document section) tasolla.

2.6 Suostumuksen toimintaohjeen tietoanalyysi

Suostumuksen toimintaohjeen (Consent Directive) rakenne ja attribuutit on esitetty alla olevassa tietomallissa. Tietomalli on esitetty isommassa koossa liitteessä 2.

Tietomallissa kuvataan yksittäisen asiakkaan suostumuksia olettaen, että käytössä ovat myös yksityisyyden suojan käytännöt.



Kuva 8 Suostumuksen yleiskuva

ConsentDirective on pääluokka, joka ilmaisee kokoelman niistä suostumukseen liittyvistä ohjeista, joita suostuja on julkaissut, joko itsestään tai jostakusta muusta. PublishedConsent ilmaisee paikan, josta suostumuksen kohteena olevan henkilön suostumus löytyy.

Consenter ilmaisee suostujan tai valtuutetun henkilön (Substitute Decision Maker) ominaisuuksia (sukulaisuussuhde, sähköinen allekirjoitus, tieto allekirjoituksesta paperilla, suostujan nimi)

Client-luokkaa voidaan käyttää asiakkaan/suostujan ominaisuuksiin (esim. ”jaettu salaisuus” eli salasana tai PIN-koodi rajoitettuun tietoon)

PrivacyRule määrittää suostujan käyttöoikeudet tietyntyyppiseen informaatioon tietyille käyttäjille.

HealthRecord määrittää suostumuksissa määriteltyjen tietojen kohteet (OID, sijainti)

2.7 Järjestelmien välinen vuorovaikutus

Analyysimallissa on kuvattuna käsitteellisellä tasolla myös järjestelmien välinen vuorovaikutus. Sekvenssikaavioilla on kuvattuna:

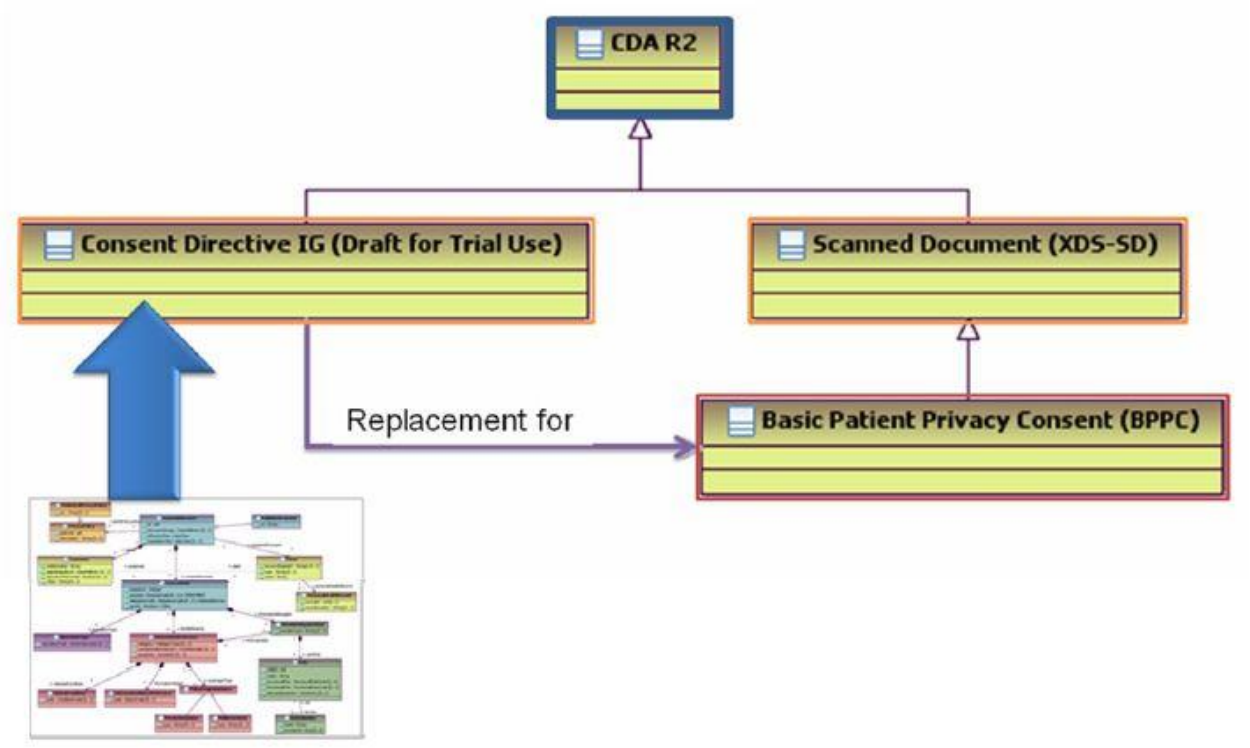
- Suostumusohjeiden hallinta
- Yksityisyyden suojan käytäntöjen hallinta
- Kaksi erilaista tapaa pyytää potilastietoja

2.8 Aiheeseen liittyvän sanaston analyysi

Analyysimallissa on myös analysoituna aihealueeseen liittyvät termit ja käsitteet

2.9 Toteutus CDA R2:ssa

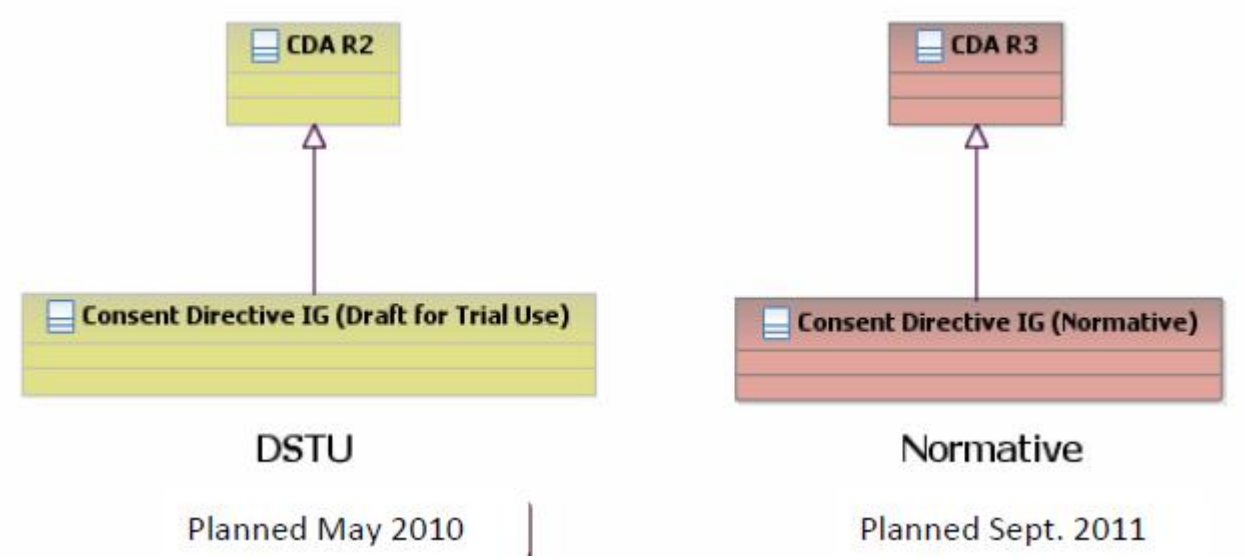
Analyysimallin pohjalta on laadittu toteutusohje CDA R2:sta varten. Toteutusohjeen lähestymistapana oleva yhteensopivuus taaksepäin on kuvattuna alla olevassa kuvassa.



Kuva 9 CDA R2 toteutusohjeen lähestymistapa

Toteutusohjeessa kuvataan CDA R2 headerin rajoitteet ja toteutus structuredBody-rakenteeseen.

Tavoitteena on, että toteutusohje otetaan käyttöön myös tulevassa CDA R3 –standardissa.

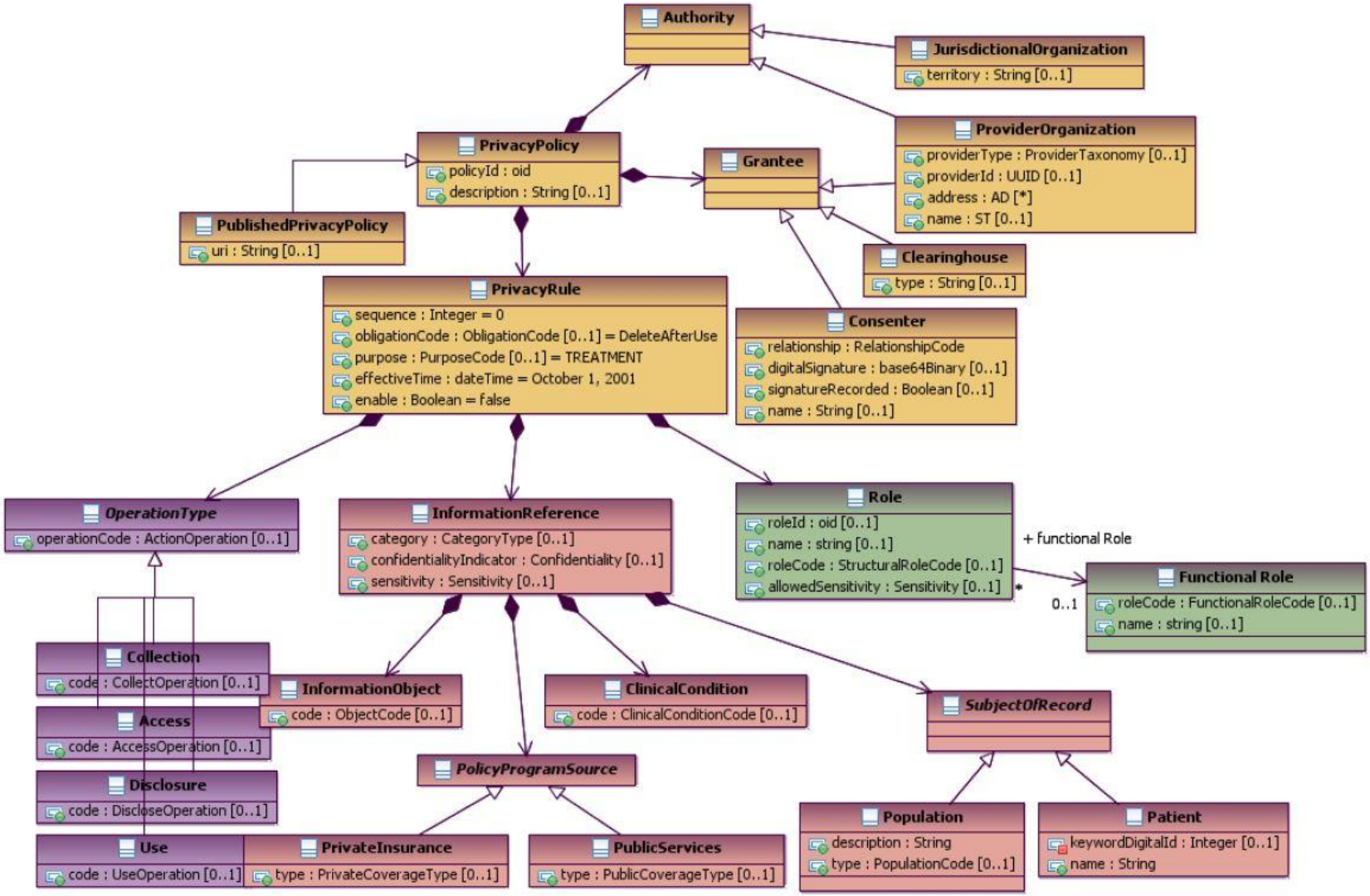


Kuva 10 Suostumuksen toteutusohjeen aikataulusuunnitelma

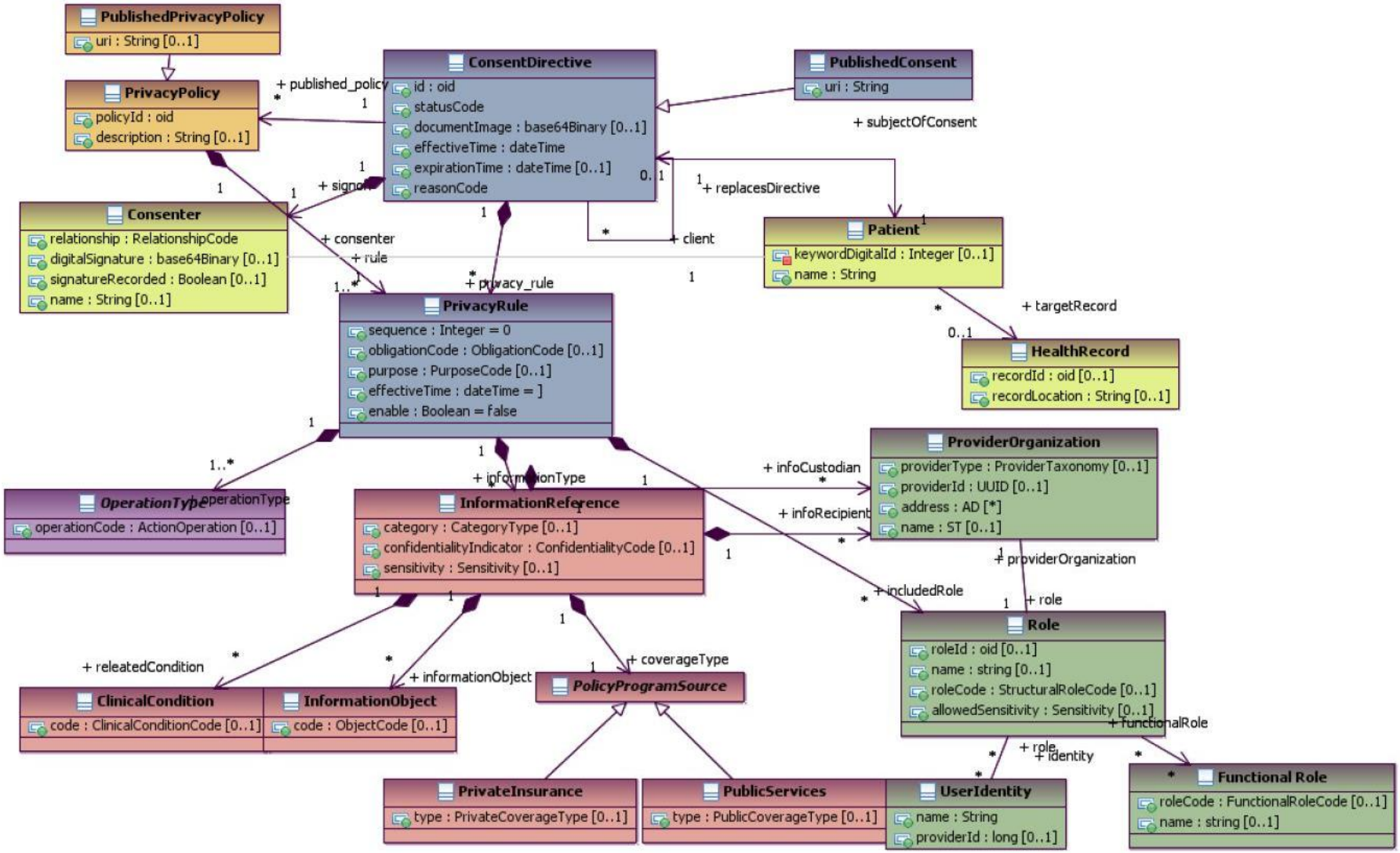
3. YHTEENVETO

CDA R3:een yksityisyyden suojaan ja suostumuksiin liittyvät asiat on periaatteellisella tasolla kuvattuna aihealueen analyysimallissa. Analyysimallin pohjalta on laadittu toteutusohje CDA R2:sta varten, jossa kuvataan CDA R2:n headerin ja bodyn rajoitteet analyysimallin mukaisen suostumuksien hallinnan toteuttamisessa. Kummastakin standardiluonnoksesta kerätään kokemuksia ja kommentteja, joiden perusteella suostumusten hallinta tulevassa CDA R3:ssa tulee tarkentumaan.

Liite 1


Authority
JurisdictionalOrganization
territory : String [0..1]
ProviderOrganization
providerType : ProviderTaxonomy [0..1]
providerId : UUID [0..1]
address : AD [*]
name : ST [0..1]
PrivacyPolicy
policyId : oid
description : String [0..1]
Grantee
PublishedPrivacyPolicy
uri : String [0..1]
Clearinghouse
type : String [0..1]
PrivacyRule
sequence : Integer = 0
obligationCode : ObligationCode [0..1] = DeleteAfterUse
purpose : PurposeCode [0..1] = TREATMENT
effectiveTime : dateTime = October 1, 2001
enable : Boolean = false
Consenter
relationship : RelationshipCode
digitalSignature : base64Binary [0..1]
signatureRecorded : Boolean [0..1]
name : String [0..1]
OperationType
operationCode : ActionOperation [0..1]
InformationReference
category : CategoryType [0..1]
confidentialityIndicator : Confidentiality [0..1]
sensitivity : Sensitivity [0..1]
Role
roleId : oid [0..1]
name : string [0..1]
roleCode : StructuralRoleCode [0..1]
allowedSensitivity : Sensitivity [0..1]
+ functional Role
*
0..1
Functional Role
roleCode : FunctionalRoleCode [0..1]
name : string [0..1]
Collection
code : CollectOperation [0..1]
InformationObject
code : ObjectCode [0..1]
ClinicalCondition
code : ClinicalConditionCode [0..1]
SubjectOfRecord
Access
code : AccessOperation [0..1]
Disclosure
code : DiscloseOperation [0..1]
PolicyProgramSource
Population
description : String
type : PopulationCode [0..1]
Patient
keywordDigitalId : Integer [0..1]
name : String
Use
code : UseOperation [0..1]
PrivateInsurance
type : PrivateCoverageType [0..1]
PublicServices
type : PublicCoverageType [0..1]

Liite 2


PublishedPrivacyPolicy
uri : String [0..1]
PrivacyPolicy
policyId : oid
description : String [0..1]
+ published_policy
ConsentDirective
id : oid
statusCode
documentImage : base64Binary [0..1]
effectiveTime : dateTime
expirationTime : dateTime [0..1]
reasonCode
PublishedConsent
uri : String
+ subjectOfConsent
+ signer
+ replacesDirective
Consenter
relationship : RelationshipCode
digitalSignature : base64Binary [0..1]
signatureRecorded : Boolean [0..1]
name : String [0..1]
+ consenter
+ rule
+ client
Patient
keywordDigitalId : Integer [0..1]
name : String
+ privacy_rule
+ targetRecord
PrivacyRule
sequence : Integer = 0
obligationCode : ObligationCode [0..1]
purpose : PurposeCode [0..1]
effectiveTime : dateTime =]
enable : Boolean = false
HealthRecord
recordId : oid [0..1]
recordLocation : String [0..1]
ProviderOrganization
providerType : ProviderTaxonomy [0..1]
providerId : UUID [0..1]
address : AD [*]
name : ST [0..1]
+ infoCustodian
+ infoRecipient
+ providerOrganization
OperationType
operationCode : ActionOperation [0..1]
+ operationType
InformationReference
category : CategoryType [0..1]
confidentialityIndicator : ConfidentialityCode [0..1]
sensitivity : Sensitivity [0..1]
+ includedRole
+ role
Role
roleId : oid [0..1]
name : string [0..1]
roleCode : StructuralRoleCode [0..1]
allowedSensitivity : Sensitivity [0..1]
+releatedCondition
+ informationObject
+ coverageType
ClinicalCondition
code : ClinicalConditionCode [0..1]
InformationObject
code : ObjectCode [0..1]
PolicyProgramSource
+ functionalRole
+ identity
PrivateInsurance
type : PrivateCoverageType [0..1]
PublicServices
type : PublicCoverageType [0..1]
UserIdentity
name : String
providerId : long [0..1]
Functional Role
roleCode : FunctionalRoleCode [0..1]
name : string [0..1]