



**Specifiche tecniche Infrastruttura  
di Gestione consenso e privacy  
FSEr**

*GDL-O Sicurezza*



**Arsenà.IT**

*Centro Veneto  
Ricerca e  
Innovazione per la  
Sanità Digitale*



## Informazioni preliminari

### Contatti

Per ulteriori informazioni, si prega di contattare:

5                    *Ing Oriella Pallottino*  
  
                      *Project Engineer*  
  
                      *Viale Oberdan, 5 – 31100 Treviso*  
  
                      *cell. +393669239759*  
  
                      *e-mail opallottino@consorzioarsenal.it*

10

### Controllo del documento

N. documento:    Specifiche tecniche: Infrastruttura di Gestione consenso e privacy FSEr 2.6.3

Stato di avanzamento:                    Public Comment

Data di prima emissione:                    20/01/15

15                    Ultimo Aggiornamento:                    10/06/16

Revisione:                                    versione 2.6.3

Numero di pagine:                            72

Responsabile del documento:            *Claudio Saccavini*

Coordinatore della stesura:              *Mauro Zanardini*

20                    Autore:                                        *Oriella Pallottino*  
  
   *Mauro Zanardini*



## Status del documento

Versione	Status	Data	Descrizione Modifica
<b>0.1</b>	<b>BOZZA</b>	<b>09/05/2013</b>	Condivisione interna
<b>0.2</b>	<b>BOZZA</b>	<b>22/10/2014</b>	Condivisione GDL-O Sicurezza
<b>0.3</b>	<b>BOZZA</b>	<b>03/11/2014</b>	Review post GDL-O Sicurezza
<b>1.0</b>	<b>PUBLIC COMMENT</b>	<b>20/01/2015</b>	Versione per il Public Comment
<b>2.0</b>	<b>UNITA' DI REGIA</b>	<b>26/06/2015</b>	Versione per Unità di regia
<b>2.1</b>	<b>UNITA' DI REGIA</b>	<b>01/07/2015</b>	Modifiche editoriali
<b>2.5</b>	<b>UNITA' DI REGIA</b>	<b>22/03/2016</b>	Introdotta Consenso Advanced per Care-Giver e Guarantor.  Introdotti requisiti per rilevare i Consensi FSEr.
<b>2.6</b>	<b>UNITA' DI REGIA</b>	<b>25/03/2016</b>	Modifica dell'elemento PID-13 (Phone Number – Home / XTN )  Modifica della strutturazione del tutore legale per il CDA2
<b>2.6.1</b>	<b>UNITA' DI REGIA</b>	<b>29/03/2016</b>	Correzione refuso esempio "sourcePatientInfo"  Correzione refuso attributo use per l'elemento <telecom>
<b>2.6.2</b>	<b>UNITA' DI REGIA</b>	<b>20/04/2016</b>	Correzione refuso esempio "consensi Advanced"
<b>2.6.3</b>	<b>UNITA' DI</b>	<b>26/04/2016</b>	Sezione 5.3: Precisazione sul consenso alla consultazione FSEr



	REGIA		<p>"advanced" in caso di care giver / tutore legale.</p> <p>Appendice B.1.1: precisazione sul CDA2 nel caso di rifiuto di fornire i dati di contatto (email e telefono) da parte del tutore legale</p>
--	-------	--	--



## Indice

	<b>Glossario.....</b>	<b>7</b>
	<b>Introduzione .....</b>	<b>8</b>
	<b>Iter di approvazione documentale .....</b>	<b>9</b>
5	<b>Open Issues.....</b>	<b>10</b>
	<b>Summary .....</b>	<b>11</b>
	<b>1 Il consenso all'interno del progetto FSE.....</b>	<b>14</b>
	<b>2 Infrastruttura Privacy .....</b>	<b>17</b>
	<b>2.1 Casi d'uso .....</b>	<b>19</b>
10	2.1.1 Creazione del consenso all'alimentazione FSEr .....	19
	2.1.2 Documenti coperti da privacy (a maggiore tutela di anonimato con riferimento al documento "casi d'uso e gestione delle policy") .....	20
	2.1.3 Creazione di policy di visibilità ad hoc per documenti coperti da privacy ...	21
	2.1.4 Creazione di documenti che descrivono prestazioni effettuate in anonimato	
15	22	
	2.1.5 Creazione di un documento clinico a cui si applicano le policy di visibilità definite dal documento di Consenso alla consultazione FSEr.....	22
	2.1.6 Creazione di un consenso alla consultazione ad evento .....	23
	2.1.7 Modifica di un consenso alla consultazione ad evento .....	24
20	2.1.8 Revoca del Consenso all'alimentazione del proprio FSEr .....	25
	2.1.9 Consenso all'alimentazione del FSEr con i documenti clinici prodotti prima della sottoscrizione del consenso all'alimentazione del FSEr.....	26
	2.1.10 Creazione del consenso alla consultazione FSEr.....	26
	2.1.11 Consultazione dei documenti clinici in caso di emergenza .....	27
25	2.1.12 Raccolta del consenso da parte del mmg/pls .....	28
	2.1.14 Creazione di un documento di consenso advanced: delega per minore o persona sottoposta a tutela .....	30
	2.1.15 Creazione di un documento di consenso advanced: delega per un caregiver	31
30	<b>3 Classificazione dei documenti di Consenso.....</b>	<b>32</b>
	<b>4 Valutazione dei consensi: Policy Manager.....</b>	<b>34</b>
	<b>4.1 Policy di Accessibilità.....</b>	<b>34</b>
	4.1.1 Processo di valutazione delle Policy di Accessibilità.....	35
	4.1.2 Dettaglio tecnico del Processo di valutazione delle policy.....	39



5	<b>5 Creazione documenti di Consenso .....</b>	<b>41</b>
	5.1 Consenso all'alimentazione del FSEr .....	41
	5.2 <i>Consenso all'alimentazione del FSEr con il pregresso</i> .....	43
5	5.2.1 Transazioni correlate alla sottoscrizione del consenso all'alimentazione FSEr con il pregresso .....	43
	5.3 <b>Creazione e gestione del Consenso alla consultazione .....</b>	<b>44</b>
	5.4 <b>Consenso ad evento .....</b>	<b>46</b>
	5.4.1 Creazione e gestione del documento di Consenso ad evento .....	46
	5.4.2 Aggiornamento Documento di Consenso ad Evento.....	49
10	5.5 <b>Livello di Confidenzialità dei Documenti Clinici .....</b>	<b>50</b>
	5.5.1 Processo di definizione del livello di confidenzialità.....	51
	5.6 <b>Revoca di un Consenso (alimentazione, consultazione o ad evento) .....</b>	<b>55</b>
	5.7 <b>Dichiarazione di consultazione in emergenza .....</b>	<b>55</b>
	5.8 <b>Struttura Consenso basic .....</b>	<b>57</b>
15	5.9 <b>Struttura Consenso Advanced.....</b>	<b>57</b>
	<b>Appendice A: OID consensi basic e advanced .....</b>	<b>58</b>
	A.1. PPPI Consensi basic .....	58
	A.2. PPPI Consensi Advanced .....	60
	<b>Appendice B: Aggiunte alle linee guida BPPC per la strutturazione del CDA R.2.</b>	
20	.....	61
	B.1 ClinicalDocument/RecordTarget .....	61
	B.1.1 Numero di telefono e mail del paziente .....	61
	B.1.2 Tutore Legale .....	62
	<b>Appendice C: Dati a maggior tutela dell'anonimato .....</b>	<b>66</b>
25	<b>Appendice D: Requisiti Interfaccia Raccolta Consenso FSEr .....</b>	<b>67</b>
	<b>Bibliografia .....</b>	<b>72</b>



## Glossario

<b>AO</b>	Aziende Ospedaliere
<b>ACC</b>	Applicazioni Cartelle Cliniche
<b>AO</b>	Azienda Ospedaliera
<b>APSS</b>	Azienda Provinciale Socio Sanitaria
<b>AR</b>	Anagrafe Regionale
<b>ASL</b>	Azienda Sanitaria Locale
<b>AUSL</b>	Azienda Unità Sanitaria Locale
<b>BPPC</b>	Basic Patient Privacy Consents
<b>CDA</b>	Clinical Document Architecture
<b>CF</b>	Codice Fiscale
<b>CIE</b>	Carta di identità Elettronica
<b>CNS</b>	Carta Nazionale dei Servizi
<b>CUP</b>	Centro Unificato di Prenotazione
<b>DCE</b>	Documento Clinico Elettronico
<b>FSE</b>	Fascicolo Sanitario Elettronico
<b>HL7</b>	Health Level Seven
<b>ICT</b>	Information and Communication Technology
<b>IHE</b>	Integrating The Healthcare Enterprise
<b>LIS</b>	Laboratory Information System
<b>MEF</b>	Ministero dell'Economia e delle Finanze
<b>MMG</b>	Medico di Medicina Generale / Medici di Medicina Generale
<b>PDTA</b>	Percorso Diagnostico Terapeutico Assistenziale
<b>PLS</b>	Pediatri di Libera Scelta
<b>PPPI</b>	Patient Privacy Policy Identifier: identificatore di una policy sottoscritta dal paziente
<b>PM</b>	Project Management
<b>Repository di riferimento</b>	Repository documentale utilizzato dal source documentale in oggetto per memorizzare i documenti
<b>OID</b>	ISO Object Identifiers
<b>SIA</b>	Sistema Informativo Aziendale
<b>SPCoop</b>	Sistema Pubblico di Connettività e Cooperazione
<b>SSN</b>	Servizio Sanitario Nazionale
<b>TS</b>	Tessera Sanitaria
<b>XDS</b>	Cross-Enterprise Document Sharing
<b>XML</b>	eXtensible Mark-up Language



## Introduzione

Il presente documento di linee guida è stato redatto all'interno del GDL-O "Sicurezza", gruppo di lavoro operativo del progetto Fascicolo Sanitario Elettronico Regionale.

5 Viene affrontato il tema relativo all'infrastruttura tecnologica che consentirà l'applicazione delle policy di visibilità e le regole di privacy associate ai dati contenuti all'interno del FSEr. Queste policy potranno essere sottoscritte dal titolare dei dati clinici, o saranno applicate di default in funzione delle regole di accessibilità definite a livello regionale.

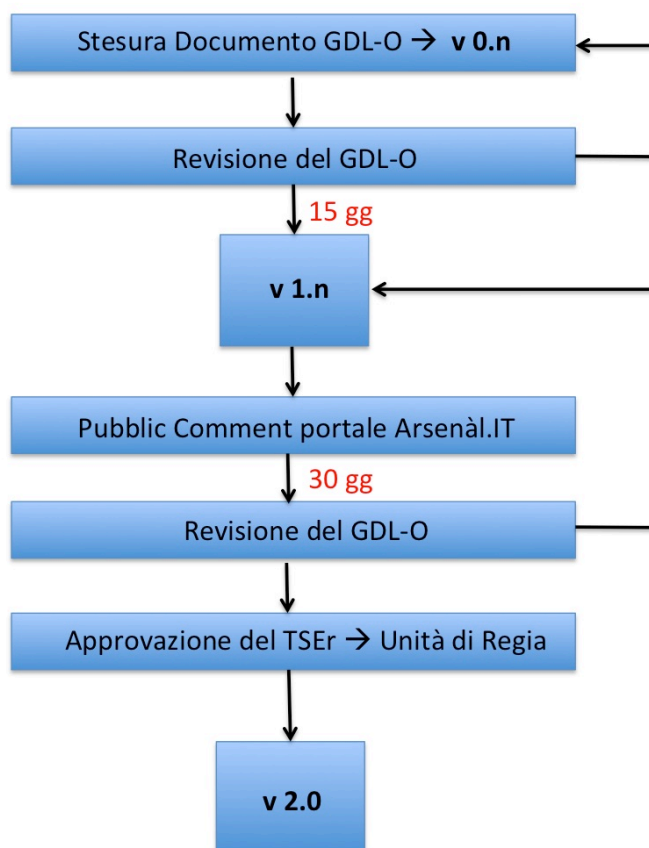
10 L'infrastruttura definita in questo documento è sviluppata in accordo alle direttive del GDL-O Privacy e formalizzate all'interno delle linee guida redatte dal gruppo stesso.

15 Il modello tecnologico si basa su un'infrastruttura di tipo XDS (descritta nelle specifiche di riferimento relative all'Infrastruttura di condivisione Documentale FSEr, "Specifiche tecniche di Infrastruttura per il FSEr"), e prevede la creazione e la condivisione di documenti di Consenso (prodotti in formato CDA R.2) che permettono la definizione delle policy di visibilità dei documenti clinici presente nel FSEr.

20 Viene presentato di seguito l'iter di approvazione documentale a cui la documentazione redatta da Arsenà.IT all'interno del progetto FSEr dovrà essere sottoposta.



## Iter di approvazione documentale



**v 0.n → STATUS BOZZA** → il documento è stato redatto all'interno del GDL-O di competenza, le modifiche e i commenti devono essere inviati all'indirizzo e-mail del coordinatore alla stesura del presente documento (riferimento paragrafo Informazioni generali – Contatti in incipit al presente documento) integrati i commenti e/o le eventuali modifiche del GDL-O vengono redatte le varie versioni v 0.n.

Una volta definita una v 0.n definitiva all'interno del GDL-O, questo ha **15 gg** per apportare ulteriori modifiche sempre inviandole all'indirizzo e-mail del coordinatore alla stesura.

**v 1.n → STATUS PUBLIC COMMENT** → il documento in formato PDF viene pubblicato sul sito di Arsenàl.IT e attraverso lo strumento del FORUM tutta la comunità di Arsenàl.IT può lasciare un proprio commento al documento



pubblicato. I commenti saranno rilasciati seguendo delle specifiche istruzioni, disponibili sul sito di Arsenàl.IT.

Il periodo di *public comment* durerà **30 gg.**

5 Durante il periodo di public comment Arsenàl.IT analizzerà i commenti rilasciati, proponendo una possibile soluzione. Ogni commento e la relativa risposta rimarranno visibili all'intera comunità che potrà intervenire nella discussione.

Alla fine del periodo di public comment tutti i commenti analizzati da Arsenàl.IT verranno sottoposti al GDL-O di competenza. In caso di approvazione i cambiamenti verranno integrati al documento di riferimento.

10 Il GDL-O di competenza valuterà la rilevanza dei cambiamenti apportati al documento e deciderà l'eventuale pubblicazione dello stesso per un ulteriore periodo di *public comment* (pubblicazione v 1.n).

15 L'iter di pubblicazione e revisione si conclude nel momento in cui non sono apportati cambiamenti sostanziali al documento secondo decisione del GDL-O di competenza.

La versione definitiva andrà quindi in approvazione al TSE-R e all'Unità di Regia.

**v 2.0 → APPROVATO →** il documento in formato PDF approvato dall'Unità di Regia sarà reso pubblico.

## 20 Open Issues

1. Si chiede al GDL-O Anagrafe di individuare la posizione all'interno dei tracciati HL7 dei nuovi servizi anagrafici per il consenso all'alimentazione del FSEr.
- 25 2. Al termine della refertazione, su scelta del medico refertatore la pubblicazione del documento all'interno del FSEr può essere sospesa (es. esito positivo biopsia), fino al momento in cui il paziente non è stato contattato verbalmente per la comunicazione del risultato. Problema aperto da discutere con le DMO.



3. Si deve discutere la terza tipologia di consenso relativa all'inserimento all'interno del proprio FSEr di tutti i documenti clinici prodotti prima del rilascio del consenso all'alimentazione dello stesso.
- 5 4. Decidere con il GDL-O Privacy e le DMO se la dichiarazione di emergenza ha una valenza temporale specificata dal medico che ne sta facendo richiesta.
- 10 5. Se il paziente decide di sottoscrivere delle specifiche policy di visibilità associandole ad un determinato evento / prestazione (richiedendo la creazione di un Documento di Consenso ad Evento prima della refertazione), le stesse policy di visibilità si applicheranno ad ogni referto prodotto a seguito di tale prestazione / evento.
- 15 6. Ad ora non è definita una modalità per creare il consenso alla consultazione ad evento a livello di cartella MMG che produce la ricetta per le cui prestazioni deve essere applicata una specifica policy di visibilità. Ad ora è gestita tale possibilità solo in fase di prenotazione / accettazione.
- 20 7. In attesa delle indicazioni di Invitalia riguardo alla dichiarazione di emergenza si chiede di iniziare ad analizzare i seguenti aspetti:
  - le motivazioni della consultazione del medico ai dati saranno codificate e potranno essere selezionate da una lista? Oppure sarà presente un campo note dove ognuno potrà inserire la propria motivazione?
  - le dichiarazioni dovranno essere "taggate" per poter essere ricercate in seguito?
  - potranno essere visualizzate solo dal paziente, o anche da eventuali altri operatori, come l'MMG?

## Summary

- 25 L'obiettivo di queste specifiche tecniche è quello di tradurre le linee guida teoriche definite dal GDL-O Privacy in un sistema applicativo automatico in grado di raccogliere i consensi sottoscritti dal Paziente in relazione al trattamento dei dati dello stesso ai fini di cura nell'ambito del Progetto FSEr.



È prerequisite fondamentale per la comprensione di tali specifiche tecniche, la conoscenza di base delle funzionalità di un environment XDS e la conoscenza delle linee guida emanate dal GDL-O Privacy "Casi d'uso e gestione delle policy".

In questo documento viene descritta l'infrastruttura per la creazione e la gestione di quattro tipologie di Consenso:

- Consenso all'alimentazione del FSEr: permette di iniziare l'indicizzazione dei documenti del paziente nel Registry regionale. Questo consenso non prevede ulteriori dettagli di specializzazione (dal momento della sottoscrizione tutti i documenti creati per il paziente devono entrare a far parte del FSEr)
- Consenso alla consultazione FSEr: è un documento di consenso che regola le policy di visibilità dei documenti che alimentano il FSEr per fini di cura. Queste policy si applicano di default a tutti i documenti per i quali NON è stato sottoscritto un documento di consenso ad hoc
- Consenso alla consultazione ad evento: un documento di consenso che viene associato ad uno specifico evento/documento. Questo documento definisce le policy di visibilità che sovrascrivono le policy identificate dal consenso alla consultazione FSEr. Questa tipologia di consenso, se sottoscritto prima della produzione del documento clinico a cui si riferisce, comporta un flusso informativo dal sistema che raccoglie il consenso al sistema che produrrà il referto (si faccia riferimento alla sezione 5.5 e alla sezione 5.4.1)
- Consenso per il popolamento del FSEr con tutti i documenti precedentemente prodotti per il paziente: *(questa tipologia di consenso non è gestita nella versione 1.0 delle specifiche)*

Ogni documento di consenso è raccolto in modo puramente digitale e senza la necessità di firma digitale. Gli attori e gli applicativi coinvolti in tale infrastruttura e che quindi possono essere coinvolti nella raccolta di ogni tipologia di Consenso sopra-citati sono:

- Portale del cittadino;
- Cartella elettronica MMG/PLS;
- Sistema gestionale ULSS (o altro sistema aziendale deputato alla raccolta del consenso);



- Sistemi gestionali di farmacia;
- Sistemi gestionali di reparti e/o verticali in accettazione diretta

5 Questo documento definisce inoltre le modalità per la sottoscrizione della Dichiarazione di Consultazione in Emergenza, che permette ad un operatore di visualizzare dei documenti resi consultabili ad altri operatori sanitari, nei casi di reale e conclamata necessità. Questo processo richiede la creazione da parte dell'operatore di un'autocertificazione digitale che non deve essere firmata digitalmente.

10 Questo documento definisce le modalità che devono essere attuate dal Policy Manager per verificare le policy di visibilità di un determinato documento a seguito di una richiesta eseguita da uno specifico operatore (si veda sezione 4.1)

L'Appendice A di questo documento definisce tutte le policy di dominio che possono essere sottoscritte da un paziente.

15 L'Appendice B definisce tutti i set di prestazioni, risultati, informazioni cliniche che sono considerate a maggior tutela dell'anonimato (referti HIV, malattie sessualmente trasmissibili, ecc.) e che quindi necessitano di una maggior tutela nei confronti della loro consultazione.

### **To do Aziendali**

20 L'azienda ULSS/Ospedaliera deve individuare il sistema preposto alla raccolta dei consensi FSEr. Questo sistema dovrà essere integrato con i servizi FSEr, mediante la creazione di un documento CDA R2 di consenso, in grado di tradurre in formato strutturato le policy di consenso selezionate.

25 L'azienda ULSS/Ospedaliera deve predisporre un processo tecnico/organizzativo che permetta di raccogliere in fase di prenotazione/accettazione/ospedalizzazione del paziente uno specifico consenso ad evento applicabile a tutti i documenti che verranno prodotti a seguito di tale evento (si veda sezione 5.5).

Il Sistema XDS Document Repository + Embedded XDS Document Repository and Source aziendale deve rispettare i requisiti funzionali definiti all'interno delle seguenti specifiche.

## 1 Il consenso all'interno del progetto FSE

Le attività connesse alla costituzione del FSEr danno luogo ad un trattamento dei dati personali ulteriore e distinto rispetto all'insieme dei trattamenti derivanti dall'erogazione delle prestazioni sanitarie, in base ai quali i dati sono stati prodotti ed acquisiti.

- 5 La distinzione e le diversità consistono nell'attività di ricomposizione e condivisione informatica di tutte le informazioni, relative alla storia clinica e socio-assistenziale del paziente, prodotte dai diversi soggetti all'interno della Regione del Veneto.

- L'informativa al trattamento dei dati attraverso il Fascicolo Sanitario Elettronico regionale, spiega in modo semplice le opportunità che offre questo tipo di strumento e  
10 che il diniego alla prestazione del consenso all'alimentazione del FSEr del paziente non ha alcuna conseguenza sul diritto alla prestazione di cura richiesta. Il trattamento dei dati personali infatti deve rispettare pienamente la libera volontà del paziente, che con il proprio consenso ha la facoltà di permettere o meno la costituzione del proprio FSEr, di far confluire in esso dati relativi al suo stato di salute e di esercitare il potere di  
15 controllo su chi può accedere al suo fascicolo e a quali informazioni.

Le tipologie di consenso che sono state definite dal GDL-O Privacy sono nel totale rispetto di quanto stabilito dalla normativa di riferimento.

In tale contesto al paziente verranno richieste tre tipologie di consenso:

- [1] il consenso all'alimentazione del proprio FSEr;
- 20 [2] il consenso alla consultazione del proprio FSEr (che può essere generico o relativo ad un singolo evento/documento clinico);
- [3] il consenso all'inserimento nel fascicolo sanitario elettronico regionale dei documenti relativi ad eventi precedenti al rilascio del consenso all'alimentazione (quest'ultimo aspetto gestito autonomamente dalle singole  
25 ULSS/AO).

- Il consenso all'alimentazione del proprio FSEr da parte del paziente deve essere esplicito, quindi non intuito o desunto da un comportamento, pertanto l'espressione della volontà del paziente per un accesso modulare al suo FSEr si manifesta attraverso un consenso a carattere generale che viene prestato on line tramite il portale  
30 regionale o in situazioni particolari presso il proprio MMG/PLS, il farmacista territoriale, il

personale di reparto o altro in base alle specificità di ciascuna ULSS/AO. Questa tipologia di consenso può essere in qualsiasi momento revocato. La revoca del consenso determina che il FSEr non sia più alimentato.

- 5 Il consenso in caso di persona minorenni o sottoposta a tutela, può essere espresso da un genitore o da un tutore con un valido documento di identità e con una specifica dichiarazione. Nel momento in cui il minore raggiunge la maggiore età è necessario che esprima il proprio consenso.

Il consenso alla consultazione permette al paziente un diverso livello di visibilità dei propri dati socio-sanitari, mediante una specifica profilatura degli attori coinvolti.

- 10 L'attività di profilatura si basa su un sistema di gestione dei privilegi a livello regionale. Questo sistema è il Policy Manager, che attribuisce diritti di accesso ed autorizza alla visualizzazione degli specifici documenti clinici solo gli attori abilitati.

Sono state definite dal GDL-O Privacy le categorie di attori che possono essere abilitate alla consultazione dei documenti clinici all'interno del FSEr. Tali categorie sono state  
15 riprese dal Disciplinare Tecnico allegato al DPCM FSE.

RUOLI
Farmacista
Operatore amministrativo
Direttore sanitario
Medico di Medicina Generale/Pediatra di Libera Scelta
Direttore amministrativo
Medico
Medico Residenza Sanitaria Assistenziale (RSA)
Infermiere
Medico rete di patologia
Operatore socio sanitario

**Figura 1: Categorie di attori abilitate al Consenso FSEr**



Il consenso all'inserimento di dati clinici relativi ad eventi precedenti al rilascio del consenso all'alimentazione può essere espresso dal paziente sul portale mediante l'accesso con le proprie credenziali di autenticazione o presso il proprio MMG/PLS/operatore sanitario. La sottoscrizione di questo consenso comporta  
5 l'indicizzazione di uno specifico documento di consenso a livello regionale. L'indicizzazione di tale documento comporta l'innescio di una serie di operazioni che comportano l'indicizzazione a livello regionale di tutti i documenti prodotti per quel determinato paziente in ogni ULSS/AO.

Ulteriore garanzia per il paziente è la facoltà di non consentire la visibilità di alcune  
10 informazioni sanitarie relative a singoli eventi clinici a soggetti diversi da chi ha prodotto il dato. Questo è realizzato mediante la sottoscrizione di un documento di consenso puntuale relativo all'evento e/o documento.

Il GDL-O Privacy ha deciso che sarà possibile effettuare un oscuramento del dato per le categorie di soggetti definiti dal paziente, che comporta sia la non visibilità del  
15 documento, sia la circostanza che l'oscuramento è stato effettuato. L'oscuramento dell'evento clinico è comunque revocabile nel tempo.



## 2 Infrastruttura Privacy

L'infrastruttura definita per la gestione e la raccolta dei consensi è basata sui seguenti profili di integrazione IHE:

- XDS (Cross-Enterprise Document Sharing)
- BPPC (Basic Patient Privacy Consent)

Versione Technical Framework v10.1

([http://ihe.net/uploadedFiles/Documents/ITI/IHE\\_ITI\\_TF\\_Vol1.pdf](http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf)).

Vengono identificati tre diversi domini:

- quello di un MMG/PLS, portale per il cittadino, dipartimentale ospedaliero o un qualsiasi attore che può creare un documento di consenso;
- quello della Ulss/AO;
- quello della Regione.

Il primo dominio è costituito da un BPPC Content Creator, che crea il contenuto di un documento di consenso (in formato CDA R.2), e da un XDS Document Source, che crea i metadati associati a quel dato documento e invia tale documento ad un attore XDS Document Repository.

Il dominio Ulss/AO è costituito da un XDS Document Repository associato ad un Embedded XDS Document Source and Repository (vedere specifiche di riferimento dell'Infrastruttura di condivisione documentale per ulteriori dettagli sulla specifica implementazione XDS definita per il progetto FSEr) e da un XDS Document Registry.

L'embedded XDS Document Source and XDS Document Repository, attraverso la transazione [ITI-42] Register Document set-b, indicizza il documento nel dominio regionale nell'XDS Document Registry.

Il dominio regionale implementa, oltre alle funzionalità di indicizzazione supportate dall'attore XDS Document Registry, anche le funzionalità di Policy Manager (che logicamente raggruppa i ruoli di "PIP" Policy Information Point, "PAP" Policy Administration Point e "PDP" Policy Decision Point. Si faccia riferimento all'Access Control White Paper per ulteriori dettagli relativi a questi concetti



[http://ihe.net/Technical\\_Framework/upload/IHE\\_ITI\\_TF\\_WhitePaper\\_AccessControl\\_2009-09-28.pdf](http://ihe.net/Technical_Framework/upload/IHE_ITI_TF_WhitePaper_AccessControl_2009-09-28.pdf)) che valuta tutte le policy di consenso associate ad un dato documento e garantisce l'accessibilità ai soli documenti autorizzati (fare riferimento alle specifiche tecniche relative all'infrastruttura di condivisione documentale per ulteriori dettagli relativi al sistema di Autorizzazione degli accessi in un ambiente federato XDS).

Il Registry regionale comunica (utilizzando una transazione legacy) le informazioni relative al consenso all'alimentazione del FSEr a livello di Anagrafe Regionale (AUR). In questo modo, l'informazione relativa ai consensi di creazione e alimentazione è fruibile da ogni attore in grado di interrogare il sistema anagrafico regionale. Si veda la sezione

**Errore. L'origine riferimento non è stata trovata.** per l'individuazione dello specifico campo dell'anagrafica che veicola l'informazione relativa a tali consensi.

Nel dominio del MMG/PLS, CUP, etc. il BPPC Content Creator crea il documento di consenso e il Document Source crea i metadati associati ed è responsabile dell'invio del documento all'XDS Document Repository mediante la transazione [ITI-41] Provide And Register Document Set-b. L'attore XDS Document Repository indicizza il documento di consenso attraverso una transazione [ITI-42] Register Document Set-b verso l'attore XDS Document Registry aziendale.

La stessa transazione (secondo le specifiche tecniche definite nel documento "Infrastruttura di condivisione Documentale FSEr") viene inizializzata anche dall'Embedded XDS Document Source per indicizzare il documento di consenso nell'XDS Document Registry regionale.

Nel dominio regionale l'XDS Document Registry è integrato con il sistema di Anagrafe Regionale (AUR), dove il paziente è identificato in base all'MPI regionale. Nel momento in cui c'è una modifica del consenso all'alimentazione del FSEr questa informazione viene automaticamente comunicata a livello di Anagrafe Regionale.

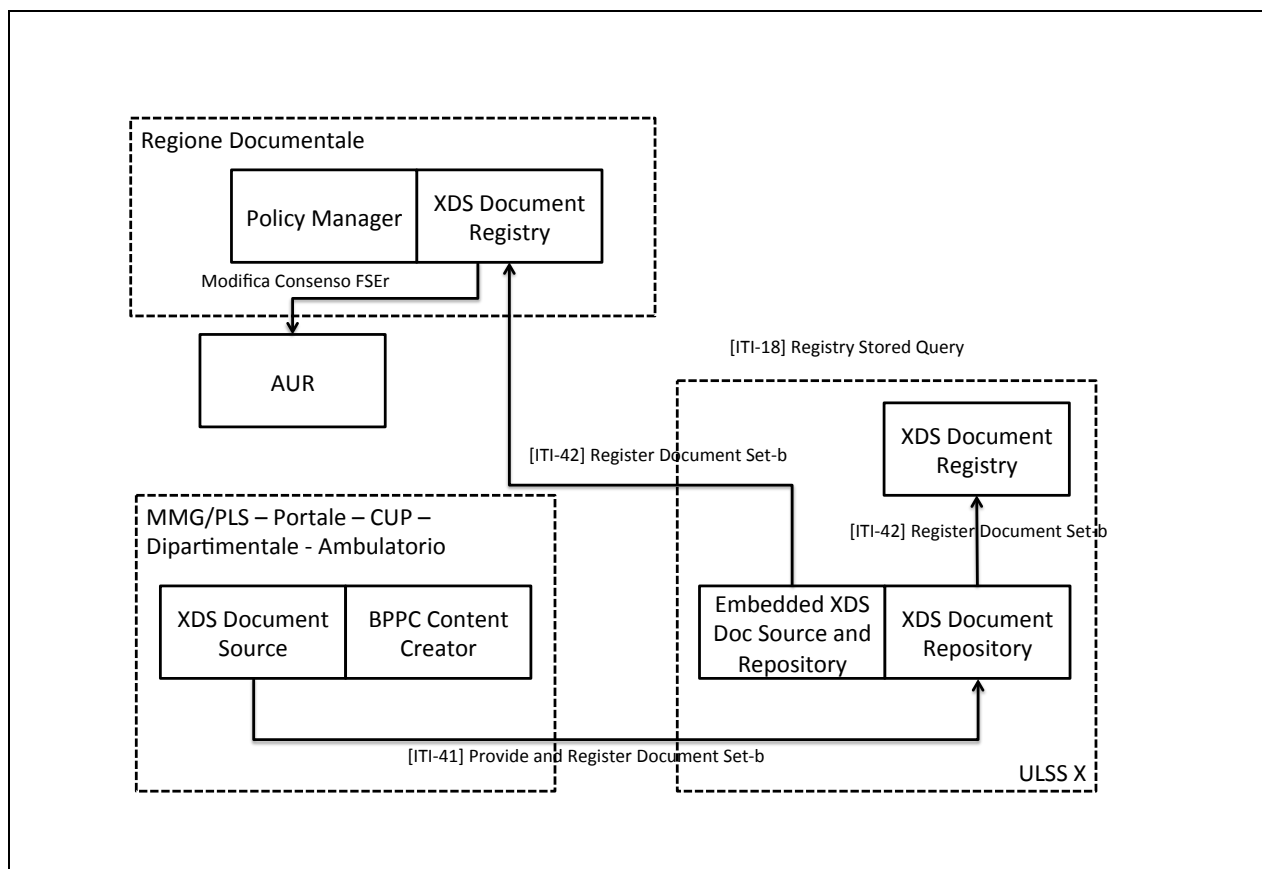


Figura 2: Infrastruttura Raccolta Consenso FSEr

## 2.1 Casi d'uso

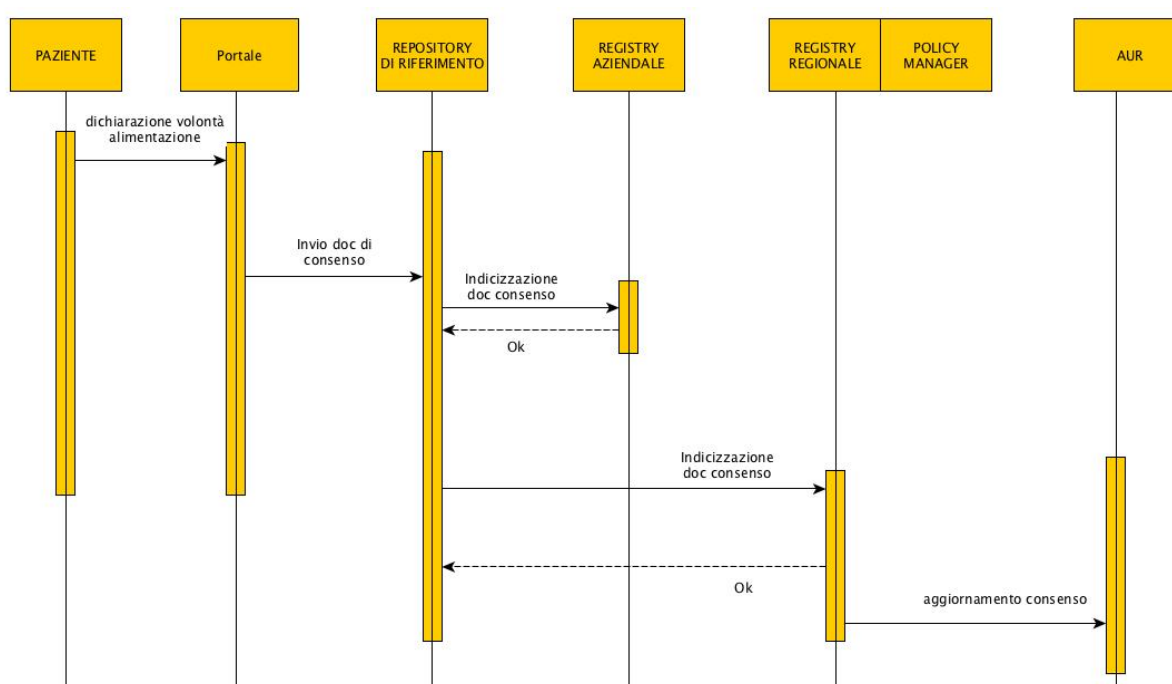
### 2.1.1 Creazione del consenso all'alimentazione FSEr

Il primo caso d'uso descrive la gestione del consenso all'alimentazione del FSEr.

- 5 Il consenso all'alimentazione del FSEr può essere rilasciato dal paziente on line tramite portale del cittadino o in casi residuali presso il proprio MMG/PLS o direttamente in ULSS (sportello ritiro referti, CUP, o altra struttura preposta).

10 Il paziente si autentica correttamente nel portale e crea un documento di consenso digitale; questo documento di consenso viene inviato al Repository di riferimento.

- Il Policy Manager individua che un documento di consenso all'alimentazione del FSEr è stato sottoscritto e comunica tale informazione all'Anagrafe Regionale. L'informazione relativa al consenso all'alimentazione del fascicolo sanitario elettronico è un'informazione permanentemente presente in Anagrafe regionale.
- 5 Un paziente che acconsente all'alimentazione del proprio FSEr ad esempio in Ulss 3 non dovrà rinnovare il proprio consenso in un'altra Ulss qualora si recasse in quest'ultima per effettuare una prestazione.



10

Figura 3: Sequence Diagram raccolta Consenso all'alimentazione FSEr

### 2.1.2 Documenti coperti da privacy (a maggiore tutela di anonimato con riferimento al documento "casi d'uso e gestione delle policy")

15

Il secondo caso d'uso riguarda le policy di visibilità dei documenti coperti da privacy (le tipologie di documenti sono state definite dal GDL-O Privacy nel documento "Casi d'uso e gestione delle policy"). Se il paziente ha sottoscritto il consenso all'alimentazione FSEr, anche questa tipologia di documenti entrano a far

parte del Fascicolo Sanitario Elettronico del paziente ma, di default, sono visibili al solo paziente stesso.

In questo caso il confidentiality code del documento sarà di tipo "V" (Very Restricted).

### 5 2.1.3 Creazione di policy di visibilità ad hoc per documenti coperti da privacy

Il terzo caso d'uso presentato riguarda la gestione di quei documenti clinici che risultano coperti da privacy (confidentiality code= "V") e per i quali il paziente sceglie delle policy di visibilità ad hoc. Il documento clinico in oggetto avrà quindi associato uno specifico documento di consenso alla consultazione.

10 Ad esempio il paziente può decidere di rendere visibile un test HIV solo al suo MMG. Il documento clinico relativo al test HIV entrerà a far parte del FSEr e sarà visibile al solo MMG.

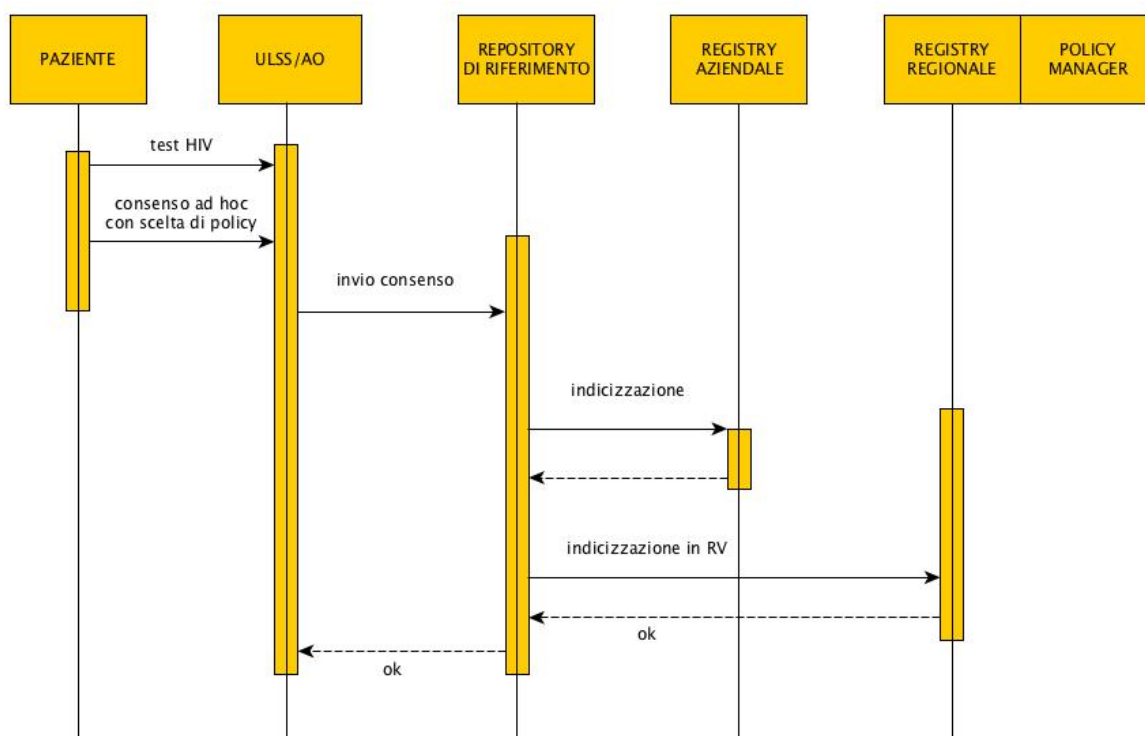


Figura 4: Creazione consenso alla consultazione ad evento



#### **2.1.4 Creazione di documenti che descrivono prestazioni effettuate in anonimato**

Il quarto caso d'uso considera la condizione in cui il paziente decide di eseguire la prestazione in anonimato. In questo caso il documento clinico relativo ad esempio al test dell'HIV non andrà ad alimentare il FSEr.

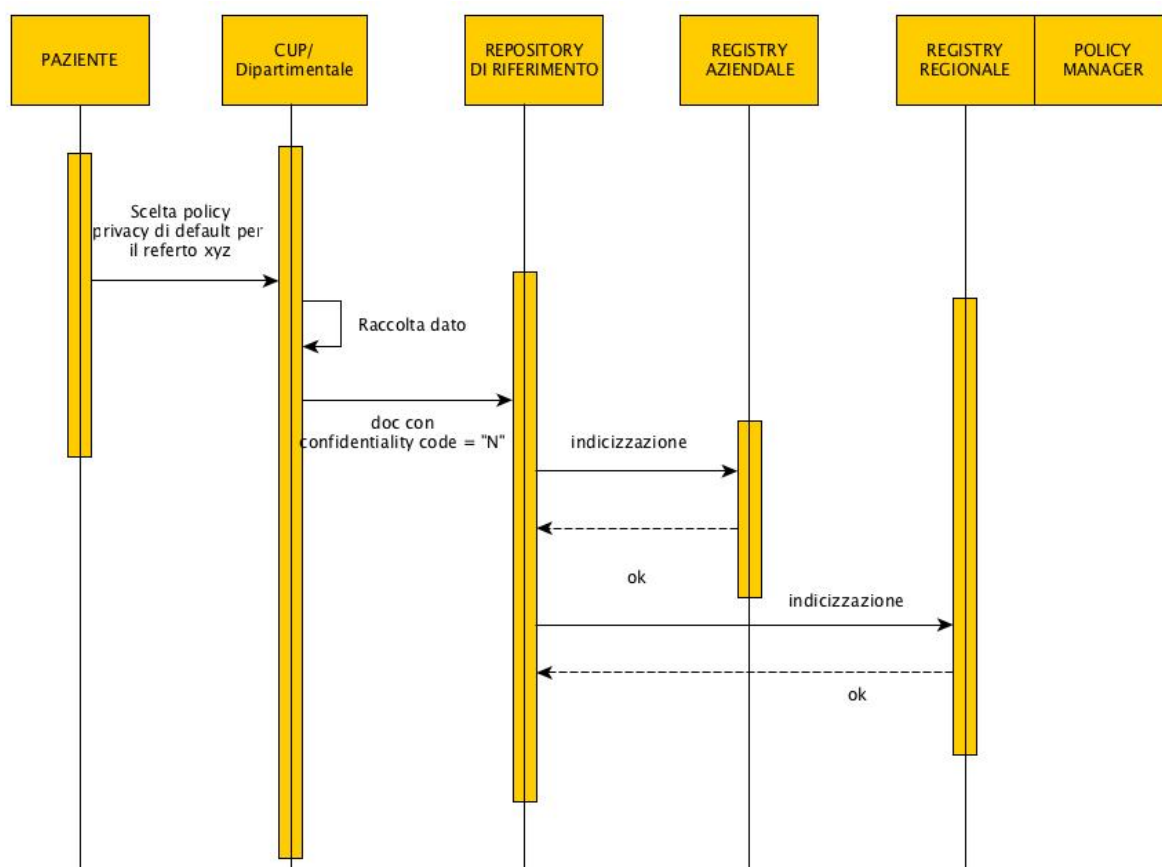
#### **2.1.5 Creazione di un documento clinico a cui si applicano le policy di visibilità definite dal documento di Consenso alla consultazione FSEr**

Il quinto caso d'uso presenta la situazione in cui il paziente decida di non modificare le sue policy di privacy e di adeguarle per quel documento clinico, a quelle di tutti i documenti contenuti nel suo FSEr.

In questo caso non viene sottoscritto dal paziente un documento di consenso alla consultazione ad evento.

Il metadato associato a questo documento clinico sarà "N" (Normal).

Una volta completata la prestazione il documento digitale può essere indicizzato a livello aziendale e a livello Regionale. Non esistono specifici documenti di consenso associati a questo documento clinico. Si applicano le policy di default e le policy definite in modo generico per i documenti contenuti nel Fascicolo Sanitario Elettronico regionale.



**Figura 5: Sequence Diagram creazione di un documento secondo le policy FSEr di default**

### 2.1.6 Creazione di un consenso alla consultazione ad evento

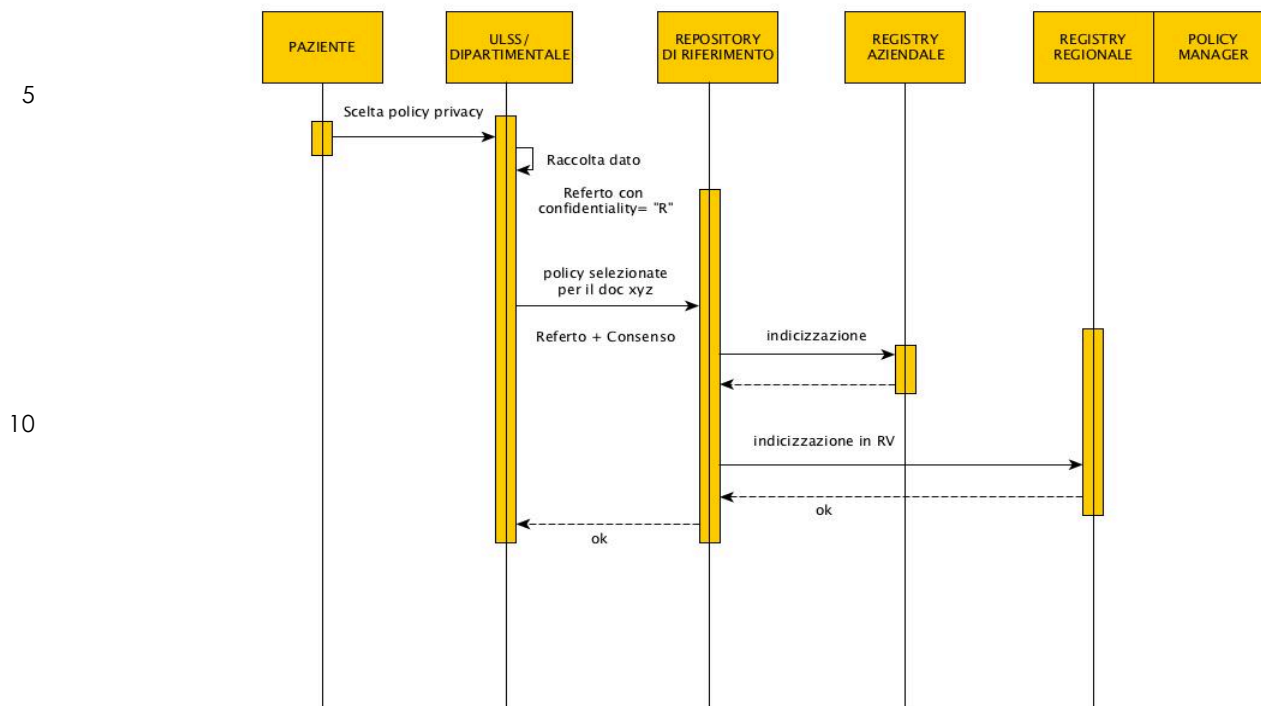
- 5 Il sesto caso d'uso descrive come rendere possibile la scelta di criteri di visibilità ad hoc per un dato documento clinico.

Il paziente può decidere che quel documento clinico può essere visto ad esempio solo dal suo MMG. Viene generato un documento di consenso che conterrà le policy di privacy definite dal paziente. Viene mantenuta un'associazione tra il documento clinico che verrà prodotto ed il consenso sottoscritto mediante l'utilizzo di uno specifico metadato del consenso stesso, che identifica il documento clinico per il quale si applicano le specifiche regole di accessibilità.

10

In questo caso il confidentiality code = "R"

I documenti vengono indicizzati a livello di Registry aziendale e successivamente a livello regionale qualora il paziente abbia precedentemente acconsentito all'alimentazione del proprio FSEr.



**Figura 6: Sequence Diagram sottoscrizione consenso ad-hoc per un documento (prima della creazione del documento stesso)**

### 2.1.7 Modifica di un consenso alla consultazione ad evento

Questo caso d'uso prevede che un paziente utilizzi l'apposito portale per cambiare le policy di privacy per un certo documento clinico.

La modifica delle policy di visibilità si traduce nella creazione di un nuovo documento di consenso, che va a sostituire (Replacement) il precedente documento di consenso.



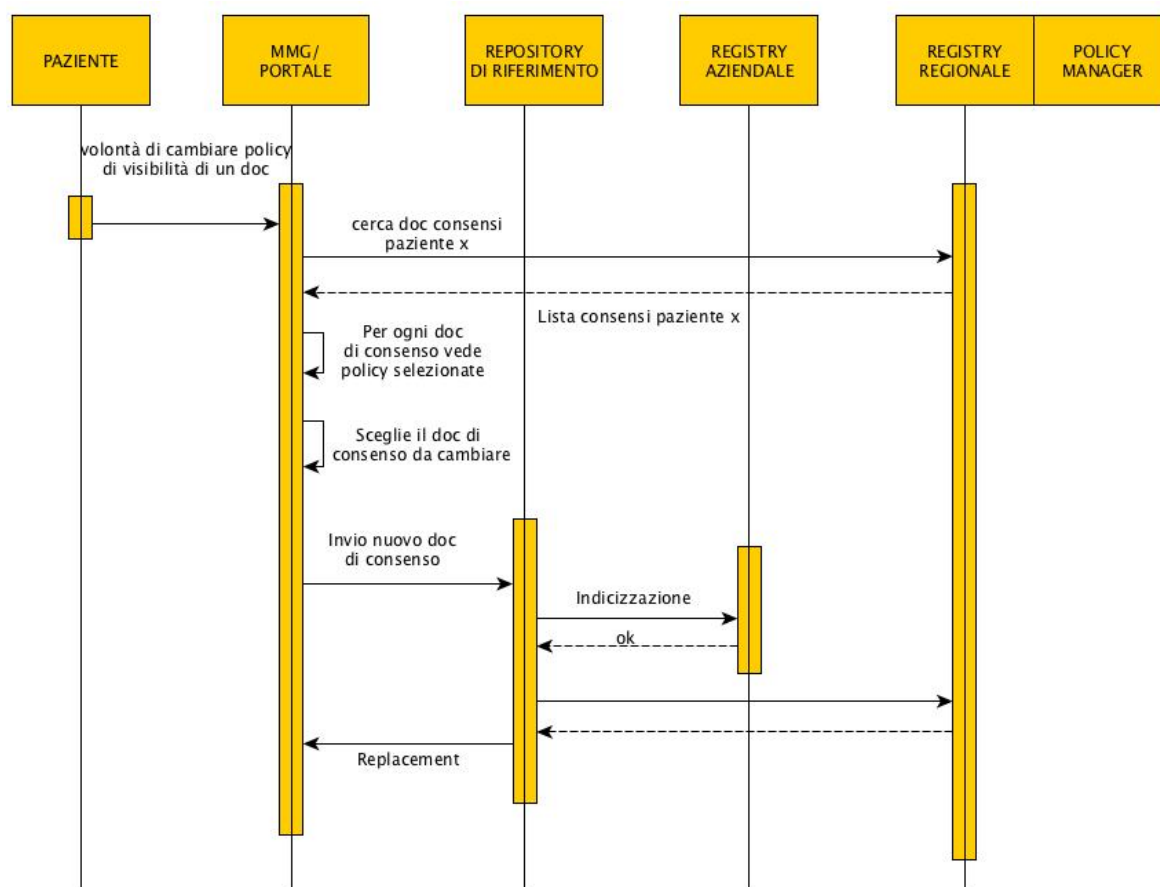


Figura 7: Sequence Diagram sottoscrizione consenso ad-hoc per un documento esistente

### 2.1.8 Revoca del Consenso all'alimentazione del proprio FSEr

- 5 Il caso d'uso che viene descritto, evidenzia la possibilità per il paziente di revocare il consenso all'alimentazione del proprio FSEr.

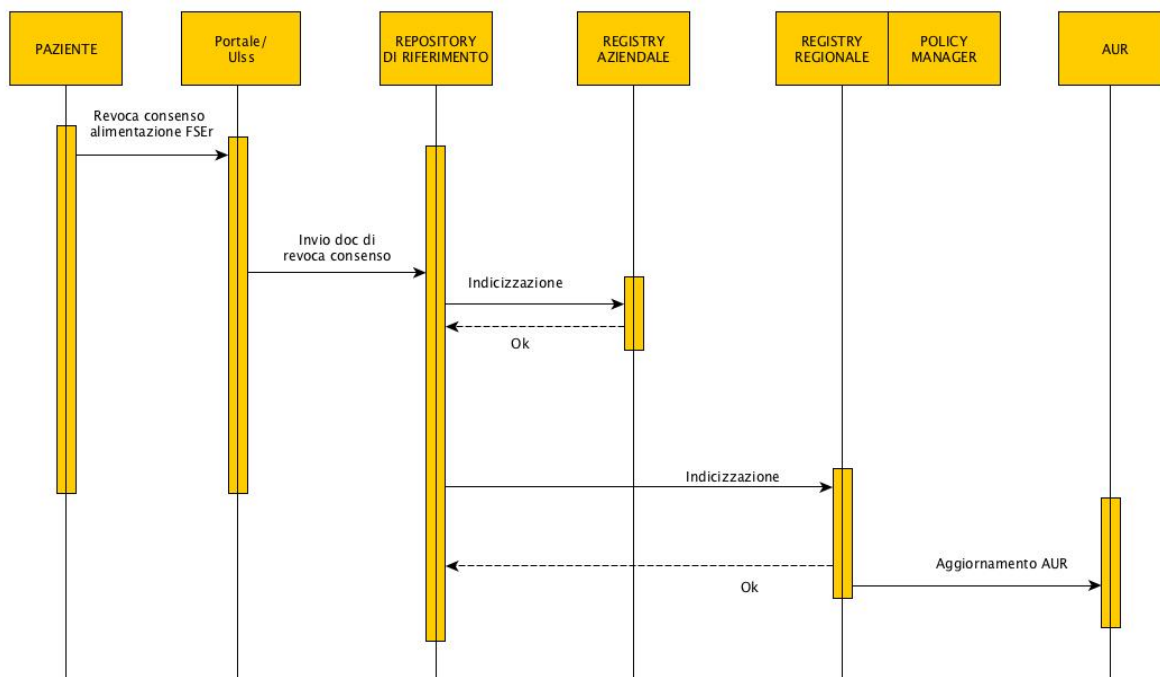
La revoca del consenso all'alimentazione può essere fatta dal paziente tramite portale o presso la Ulss/AO.

- 10 In questo caso il paziente può ad esempio recarsi in Ulss/AO e comunicare all'operatore di voler revocare il consenso all'alimentazione per il proprio FSEr.

L'operatore si autentica sul portale con le proprie credenziali e trasferisce l'informazione di revoca del consenso del paziente.

Viene creato un documento di revoca del consenso digitale che attesta la volontà del paziente. Questo documento di revoca sarà inviato al Repository di riferimento che a sua volta lo indicizzerà in Regione e in Ulss/AO.

L'informazione sarà quindi inviata all'Anagrafe Regionale.



**Figura 8: Sequencen Diagram revoca consenso all'alimentazione del FSEr**

### **2.1.9 Consenso all'alimentazione del FSEr con i documenti clinici prodotti prima della sottoscrizione del consenso all'alimentazione del FSEr**

10 Da definire

### **2.1.10 Creazione del consenso alla consultazione FSEr**

15 Il caso d'uso descrive la situazione in cui i documenti clinici di un paziente possano essere visualizzati dai medici che hanno in cura il paziente in quel momento, ovvero quelli che rientrano nel percorso diagnostico terapeutico assistenziale in atto e necessitano di visualizzare i documenti clinici del paziente.



In questo caso il paziente può decidere di rendere visibile i documenti ai soli medici che rientrano nel PDTA o decidere di renderli visibili ad esempio al solo MMG.

Nella prima situazione si tratta di consenso generico che il paziente può sottoscrivere senza dare ulteriore dettaglio.

- 5 Ad esempio il paziente nel momento in cui decide di alimentare il proprio FSEr sottoscrive il consenso generico di visualizzazione dei propri documenti clinici a tutti i medici che rientrano nel proprio PDTA. A questo punto sarà incluso il MMG e, ad esempio in caso di ricovero, tutti i medici di reparto. In questo caso il documento di consenso avrà un OID del tipo:

10 urn:oid:2.16.840.1.113883.2.9.2.50.4.13.2

Se al contrario, il paziente decide di non prestare questo tipo di consenso, avrà la possibilità di prestare un consenso alla consultazione più specifico. Può quindi scegliere a quale categoria di persone (definite nella sezione 1.1) vuole rendere visibile i propri referti. Ad esempio può decidere di renderli visibili al solo MMG. In questo caso il documento di consenso avrà un OID del tipo:

15 urn:oid:2.16.840.1.113883.2.9.2.50.4.13.3

urn:oid:2.16.840.1.113883.2.9.2.50.4.13.3

Se il paziente decide di concedere la consultazione ad un caregiver oppure ad un tutore legale alle normali PPI deve essere sommata quella che identifica il consenso come "Advanced". In questo caso il documento di consenso avrà anche un OID del tipo:

20 urn:oid:2.16.840.1.113883.2.9.2.50.4.13.14

urn:oid:2.16.840.1.113883.2.9.2.50.4.13.14

Al momento della prestazione di un consenso alla consultazione più restrittivo, una notifica di *alarm* lo avvisa delle conseguenze che la mancata visibilità dei suoi dati e documenti ai soggetti del sistema sanitario e socio-sanitario può comportare.

25

### **2.1.11 Consultazione dei documenti clinici in caso di emergenza**

Il presente caso d'uso riguarda la possibilità per un operatore sanitario di consultare i documenti clinici di un paziente nel caso in cui quest'ultimo si trovi in situazioni di emergenza.

Nello specifico pertanto, un operatore sanitario o socio-sanitario potrà avere accesso al FSEr di un determinato paziente, benché privo del consenso alla consultazione da parte dello stesso. Le condizioni che legittimano tale accesso "straordinario" sono riportate nel testo della norma (DPCM FSE).

- 5 L'operatore sanitario che richiederà di avere accesso al FSEr dell'assistito dovrà obbligatoriamente sottoscrivere una dichiarazione in cui attesterà che l'accesso al FSEr dell'assistito è avvenuto ai sensi dell'articolo 15 del DPCM FSEr.

Sarà creato uno specifico documento di consenso che verrà inviato al repository regionale ed indicizzato a livello di Registry.

- 10 XSDDocumentEntry.typeCode="Dichiarazione Consultazione Emergenza FSEr"
- XSDDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12"

### **2.1.12 Raccolta del consenso da parte del mmg/pls**

- 15 Il caso d'uso seguente descrive la possibilità del mmg o pls di raccogliere il consenso all'alimentazione, consultazione e alimentazione con il pregresso del FSEr di un paziente.

Un paziente si reca dal proprio mmg e decide di sottoscrivere il consenso per l'alimentazione e consultazione del proprio FSEr.

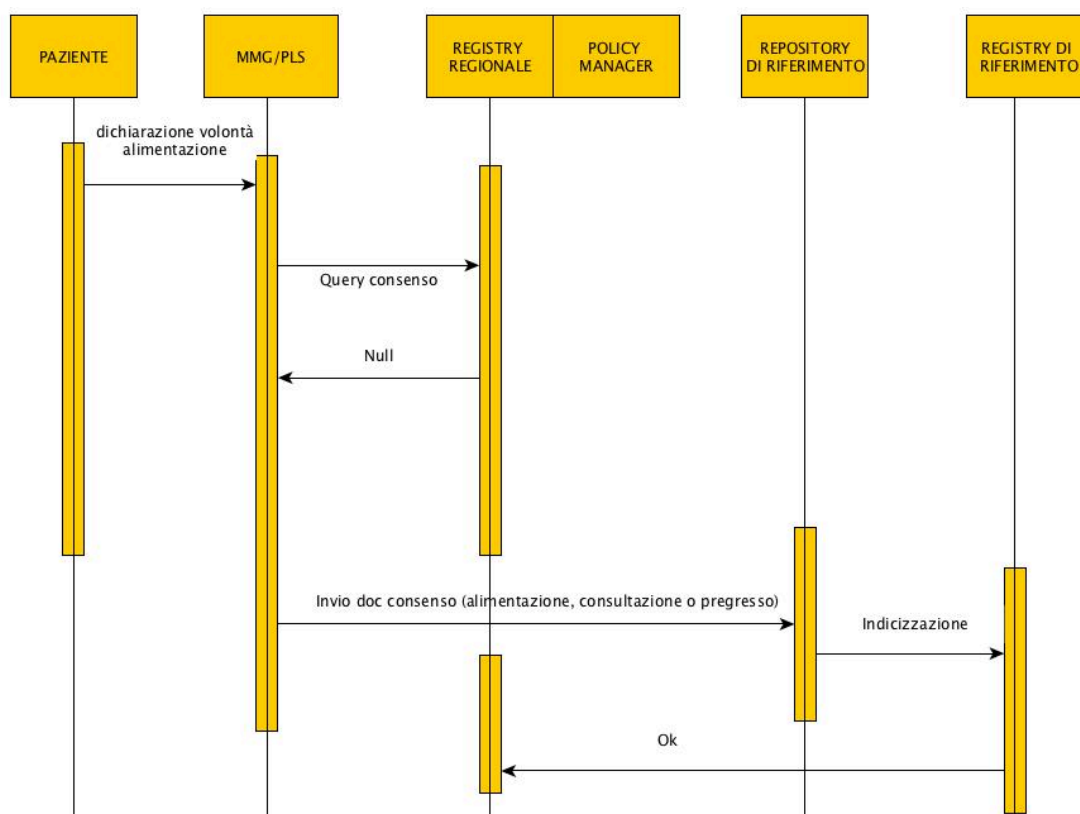
- 20 Il mmg verifica se il paziente ha già fornito qualche tipo di consenso in precedenza, autenticandosi in un particolare contesto applicativo (C.6.5) che gli permette di visualizzare tutti i consensi sottoscritti da quel paziente e facendo una query al Registry regionale.

- 25 Se la query non gli restituisce nessun risultato può proporre al paziente di raccogliere il consenso in quel momento. Al contrario, se il documento di Consenso è già presente, il sistema di cartella del mmg deve fornire la possibilità al medico stesso di recuperare il documento di consenso sottoscritto. Tale documento dovrà essere visualizzato in modalità HTML utilizzando l'apposito foglio di stile regionale accessibile attraverso rete pubblica.

Nel caso in cui la query non restituisce nessun tipo di consenso per quel paziente, il mmg può raccogliermo in quel momento. Non è possibile sottoscrivere più consensi dello stesso tipo (ad eccezione dei consensi alla Consultazione ad Evento).

5 Per ogni tipologia di consenso raccolto (Consenso Consultazione, Consenso all'alimentazione, Consenso all'alimentazione del FSEr con il pregresso), verrà creato uno specifico documento e tale documento verrà inviato al Repository di riferimento.

10 Se il paziente decide di affinare il proprio consenso alla consultazione, permettendo ad esempio la visualizzazione dei propri documenti clinici al solo mmg deve recarsi all'ufficio preposto all'interno della ULSS di appartenenza o Distretto della propria ULSS o accedendo al portale con le proprie credenziali.



**Figura 9: Sequence Diagram raccolta consenso del FSEr MMG/PLS**

#### **2.1.14 Creazione di un documento di consenso advanced: delega per minore o persona sottoposta a tutela**

- 5 Il consenso alla alimentazione e consultazione al FSEr in caso di persona minorenni o sottoposta a tutela può essere espresso da un genitore o da un tutore con un valido documento di identità e con una specifica dichiarazione. Nel momento in cui il minore raggiunge la maggiore età è necessario che esprima il proprio consenso.
- 10 Come caso d'uso consideriamo un genitore che decide di aprire il FSEr per suo figlio minorenni presso il PLS. Il PLS sottoscrive un consenso alla alimentazione e consultazione del FSEr per il paziente minorenni che riporta gli identificativi del paziente (CF ed MPI) all'interno del <recordTarget>/<patientRole>. Il documento di consenso dovrà contenere inoltre gli identificativi del tutore (CF ed MPI) che
- 15 dovranno essere specificati all'interno di <recordTarget>/<patientRole>/<patient>/<guardian> come definito in Appendice B.

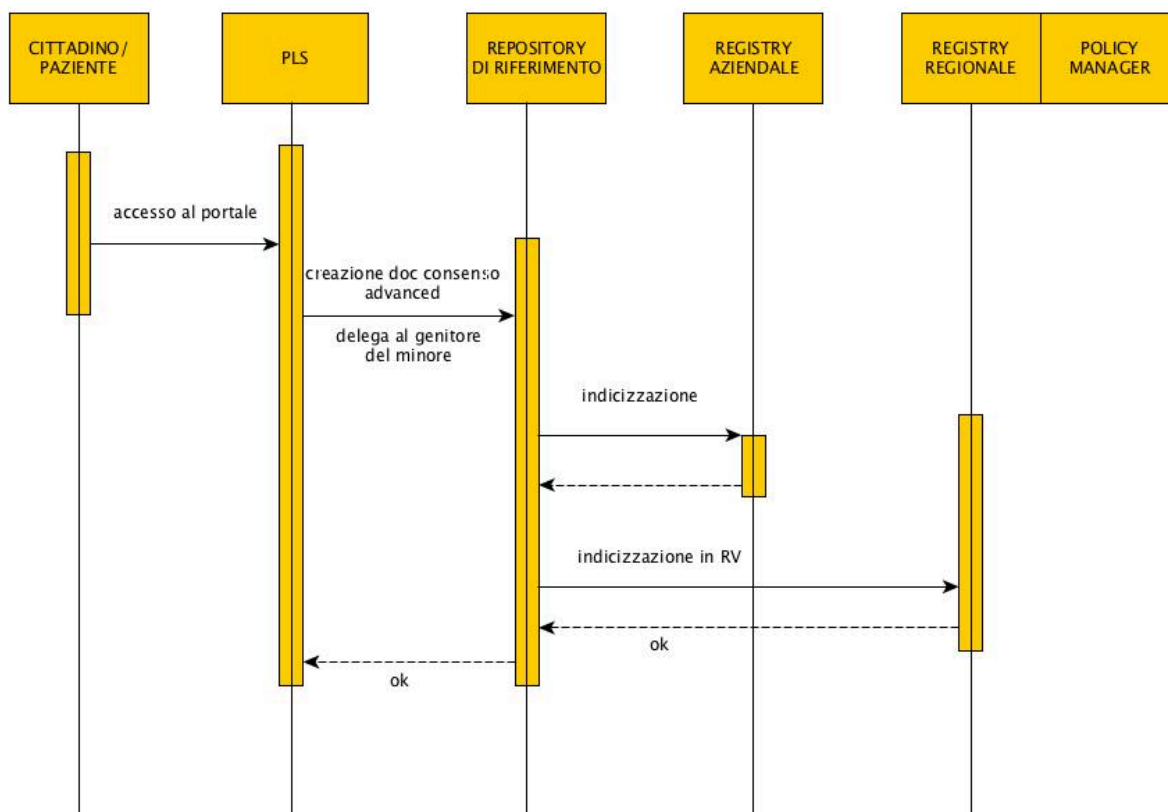


Figura 11: Sequence Diagram consenso advanced: delega minore

### 5 2.1.15 Creazione di un documento di consenso advanced: delega per un care giver

Il caso d'uso descrive la situazione di un paziente che vuole affidare la gestione del proprio FSEr ad un care giver.

10 Ad esempio si considera il caso di una persona anziana che decide di delegare il figlio alla gestione del proprio FSEr.

Tramite portale il cittadino crea un documento di consenso di tipo advanced mediante il quale esprime la sua volontà di delegare il figlio alla gestione del proprio FSEr.

All'interno del body del documento di consenso verranno specificati i care giver come definito in Appendice B.

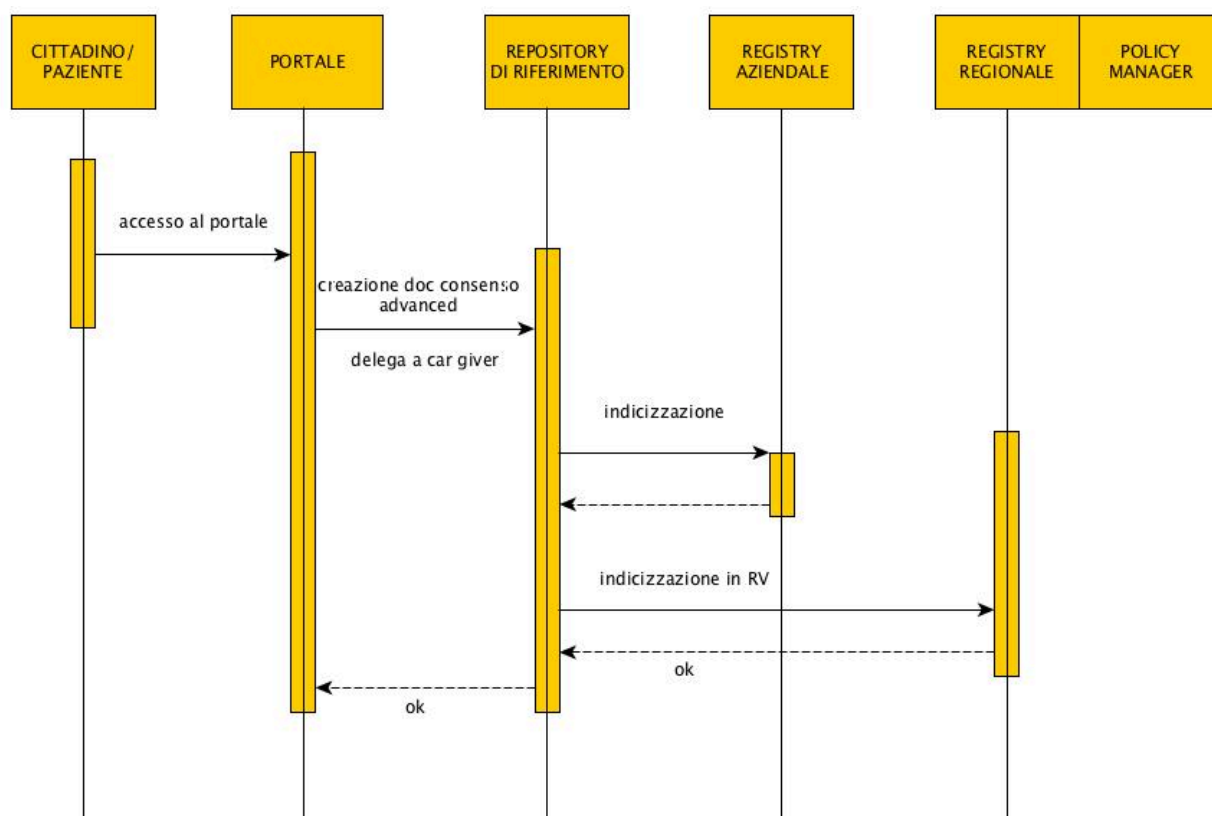


Figura 12: Sequence Diagram consenso advanced: delega care giver

### 3 Classificazione dei documenti di Consenso

Il presente paragrafo ha l'obiettivo di analizzare e classificare le tipologie di consenso e le policy di visibilità consentite all'interno dell'infrastruttura privacy del FSEr.





In questo contesto vengono definiti le seguenti tipologie di consenso in funzione dei dati/documenti clinici a cui le policy sottoscritte vengono applicate:

- **Consenso all'alimentazione del FSEr:** viene prestato dal paziente in modo volontario e permette al paziente di avere tutti i documenti clinici nominali (cioè non prodotti in regime di anonimato) presenti nel proprio Fascicolo Sanitario Elettronico regionale.
- **Consenso alla consultazione FSEr:** esiste un unico documento di consenso alla consultazione per ogni paziente. Questo documento definisce le policy di visibilità di contesto applicabili a tutti i documenti contenuti nel FSEr (a meno di specifiche policy sottoscritte ad hoc mediante un Consenso alla consultazione ad evento).
- **Consenso alla Alimentazione del FSEr pregresso:** viene prestato dal paziente in modo volontario e gli permette di avere nel proprio FSEr i propri documenti clinici pregressi, ovvero prodotti prima della data in cui ha prestato il consenso alla alimentazione.
- **Consenso alla consultazione ad evento:** è un documento di consenso alla consultazione che si applica solo ad uno specifico documento clinico (individuato nei metadati del documento di consenso stesso).

Di seguito viene presentata la classificazione dei documenti di Consenso in funzione della tipologia di policy sottoscritte:

- **Consenso alla consultazione FSEr basic:** si tratta di un consenso alla consultazione (che può essere anche ad evento) che si traduce in policy di visibilità che l'attore Policy Manager può applicare solo sulla base del valore dei metadati associati ai documenti richiesti (ed eventuali documenti di consenso associati) e sulla base dei parametri di contesto della richiesta, desumibili dall'asserzione di identità dell'operatore. Ad esempio un documento di consenso basic è quello che traduce la volontà del paziente di non far visualizzare i propri documenti ad una categoria di operatori sanitari. Ad esempio a tutti i MMG.
- **Consenso alla consultazione FSEr advanced:** si tratta di un consenso alla consultazione (che può essere anche ad evento) che si traduce in policy di visibilità che per essere valutate dal Policy Manager necessitano dell'interpretazione del contenuto strutturato del CDA R.2 del documento di



consenso stesso, memorizzato nel Repository Aziendale. Un esempio di consenso advanced è quello che permetterebbe al paziente di non rendere visibile i propri documenti ad esempio al Dott. Mario Rossi.

In aggiunta ai documenti di consenso, queste specifiche tecniche descrivono le modalità di raccolta della Dichiarazione di consultazione in emergenza FSEr.

- **Dichiarazione di consultazione in emergenza FSEr:** è un documento di consenso, sottoscritto da un operatore sanitario che necessita, per ragioni di emergenza, di vedere tutti i documenti contenuti nel FSEr di un paziente e resi visibili dallo stesso, a prescindere dalle policy di visibilità applicabili.

## 4 Valutazione dei consensi: Policy Manager

In questa sezione sono descritte le logiche funzionali dell'attore Policy Manager. Questo attore valuta le policy di visibilità applicabili alle richieste ricevute (transazione [ITI-18] Registry Stored Query) in funzione della presenza o meno dei documenti di consenso / dichiarazioni di consultazione in emergenza sottoscritti.

Un XDSDocumentEntry non autorizzato per l'utente che esegue la richiesta, NON deve essere inserita all'interno del messaggio di response creato dall'XDS Document Registry.

Per ogni XDSDocumentEntry autorizzato, l'attore XDS Document Registry deve creare un'autorizzazione gestita dal raggruppato attore SeR Authorization Decisions Manager in accordo alle specifiche tecniche di riferimento IHE e di progetto FSEr:

- [http://ihe.net/uploadedFiles/Documents/ITI/IHE\\_ITI\\_Suppl\\_SeR.pdf](http://ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_SeR.pdf)
- "Specifiche tecniche Infrastruttura XDS per il FSEr"

### 4.1 Policy di Accessibilità

In questa sezione è descritto il processo di valutazione delle policy di visibilità associato ad ogni documento indicizzato nel Registry regionale che presenta un match con i parametri di query specificati.



Il processo descritto di seguito (Figura 9) deve essere applicato in modo indipendente ad ogni documento che rispetta i parametri di filtro della query.

#### 4.1.1 Processo di valutazione delle Policy di Accessibilità

5 In questa sezione viene descritto l'activity diagram rappresentato in Figura 9.

Una volta individuato un XDSDocumentEntry che rispetta i parametri di filtro della query contenuta nel messaggio di richiesta della transazione [ITI-18] Registry Sotred Query, il Policy Manager deve valutare se lo specifico operatore che sta eseguendo la richiesta ha diritto o meno di visualizzare tale documento. In caso  
10 negativo, l'esistenza di tale documento è totalmente oscurata al richiedente (concetto di oscuramento dell'oscuramento).

Il Policy Manager ha a disposizione per eseguire la propria valutazione:

1. Metadati relativi al documento che corrisponde ai parametri di query;
2. Asserzione di identità del richiedente;

15 La prima verifica che deve essere effettuata riguarda l'identità del richiedente. Se il richiedente coincide con il titolare del documento clinico (paziente) o il creatore del documento clinico (author), il documento può essere rivelato al richiedente. Questa verifica viene effettuata sulla base del confronto del valore dei metadati XDSDocumentEntry.patientId e XDSDocumentEntry.author con il valore  
20 dell'attributo NameID dell'asserzione di identità.

Se entrambi i controlli hanno esito negativo viene verificato il livello di confidenzialità del documento con metadati corrispondenti ai parametri di query. Si possono verificare tre condizioni:

- 25 1. XDSDocumentEntry.confidentialityCode="N": in questo caso il documento clinico non nasce con un consenso ad evento nativamente associato (si veda sezione 5.5.1 per i dettagli), ma potrebbe esistere un documento di consenso ad evento creato a posteriori dal paziente. Per questo il policy Manager deve verificare l'esistenza di un documento di consenso ad evento attivo associato al documento clinico in esame (XDSDocumentEntry.typeCode="Consenso ad  
30 Evento" e XDSDocumentEntry.eventCodeList!="Consenso Revocato" e XDSDocumentEntry.referenceIdList coincidente con il valore del



XDSDocumentEntry.uniqueId del documento clinico in esame, a meno della codifica descritta in sezione 5.4.1).

a. Se tale documento di consenso esiste il policy Manager deve procedere come descritto nel punto 2.a di seguito;

5 b. Se tale documento di consenso NON esiste, al documento clinico in oggetto possono essere applicate solo le policy di visibilità di default definite dal documento di "Consenso alla Consultazione FSEr" (come descritto in sezione 5.2).

10 i. Se il Consenso alla consultazione FSEr non esiste o non è attivo (XDSDocumentEntry.eventCodeList="Consenso Revocato"), il documento non può essere rivelato.

15 ii. Se il Consenso alla consultazione FSEr è attivo, a seconda delle policy di visibilità sottoscritte (elenco di PPPI all'interno del metadato XDSDocumentEntry.eventCodeList) e dei parametri di asserzione (contesto, ruolo, metodo di autenticazione dell'operatore), viene valutato se lo specifico richiedente può visualizzare il documento.

1. Se il documento è visibile, il corrispondente XDSDocumentEntry viene inserito nel messaggio di response della query effettuata;

20 2. Se il documento non è visibile è necessario verificare se la richiesta è effettuata in condizione di emergenza. Il processo prosegue al punto X

2. XDSDocumentEntry.confidentialityCode="R": in questo caso un documento di Consenso ad evento deve esistere ed è caratterizzato da XDSDocumentEntry.referenceIdList identico al XDSDocumentEntry.referenceIdList del documento clinico in esame. Questo consenso può essere attivo o meno:

a. Se il documento di Consenso ad evento è attivo vengono verificate le policy di visibilità associate al documento di Consenso ad evento.

30 i. Se si tratta di PPPI basic, il Policy Manager può valutare l'accessibilità del documento in esame semplicemente analizzando il contenuto dell'asserzione di identità del richiedente.



1. Se il documento è visibile, il corrispondente XDSDocumentEntry viene inserito nel messaggio di response della query effettuata;
  2. Se il documento non è visibile è necessario verificare se la richiesta è effettuata in condizione di emergenza. Il processo prosegue al punto X
- 5
- ii. Se si tratta di PPPI advanced, il Policy Manager deve recuperare il documento di Consenso dal XDS Document Repository in cui è memorizzato, mediante una transazione [ITI-43] Retrieve Document Set. Il contenuto di questo documento di consenso, strutturato in accordo allo standard CDA R.2 deve essere interpretato per valutare l'accessibilità del documento stesso:
- 10
1. Se il documento è visibile, il corrispondente XDSDocumentEntry viene inserito nel messaggio di response della query effettuata;
  2. Se il documento non è visibile è necessario verificare se la richiesta è effettuata in condizione di emergenza. Il processo prosegue al punto X
- 15
- iii. Se la policy sottoscritta è di oscuramento del documento (XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.99"), il documento non può essere visualizzato.
- 20
- b. Se il documento di Consenso ad evento non è attivo , al documento in oggetto si applicano le sole policy di visibilità relative al Consenso alla consultazione FSEr partendo dal punto 1.b.
3. XDSDocumentEntry.confidentialityCode="V": in questo caso un documento di consenso ad evento potrebbe esistere o meno e potrebbe essere stato creato nativamente con il documento clinico oppure successivamente. Se il documento clinico nativamente ha associato un documento di consenso, il documento di consenso e il documento clinico stesso saranno caratterizzati dallo stesso valore del metatato XDSDocumentEntry.referenceIdList. Se il documento di consenso è creato a posteriori (rispetto alla creazione del documento clinico), il documento di consenso sarà caratterizzato da XDSDocumentEntry.referenceIdList coincidente con il valore del
- 25
- 30



XDSDocumentEntry.uniqueId del documento clinico in esame, a meno della codifica descritta in sezione 5.4.1.

a. Se il documento di consenso NON esiste o esiste ma è revocato (XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.100") il documento NON è visibile

b. In tutti gli altri casi il processo prosegue dal punto 2.a, con la verifica delle policy di visibilità associate al documento di consenso ad evento.

X. se il documento clinico è visibile a taluni operatori sanitari ma non allo specifico operatore richiedente, il Policy Manager verifica l'esistenza di una Dichiarazione di consultazione in emergenza (descritta in sezione 5.7) sottoscritta dallo stesso richiedente e temporalmente valida (XDSDocumentEntry.typeCode="Dichiarazione Consultazione Emergenza FSEr", XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12" XDSDocumentEntry.serviceStopTime < NOW, XDSDocumentEntry.author = NameID dell'asserzione del richiedente).

a. Se esiste ed è valida il documento è visibile, il corrispondente XDSDocumentEntry viene inserito nel messaggio di response della query effettuata;

b. Se non esiste o non è valida, il documento non può essere visualizzato.

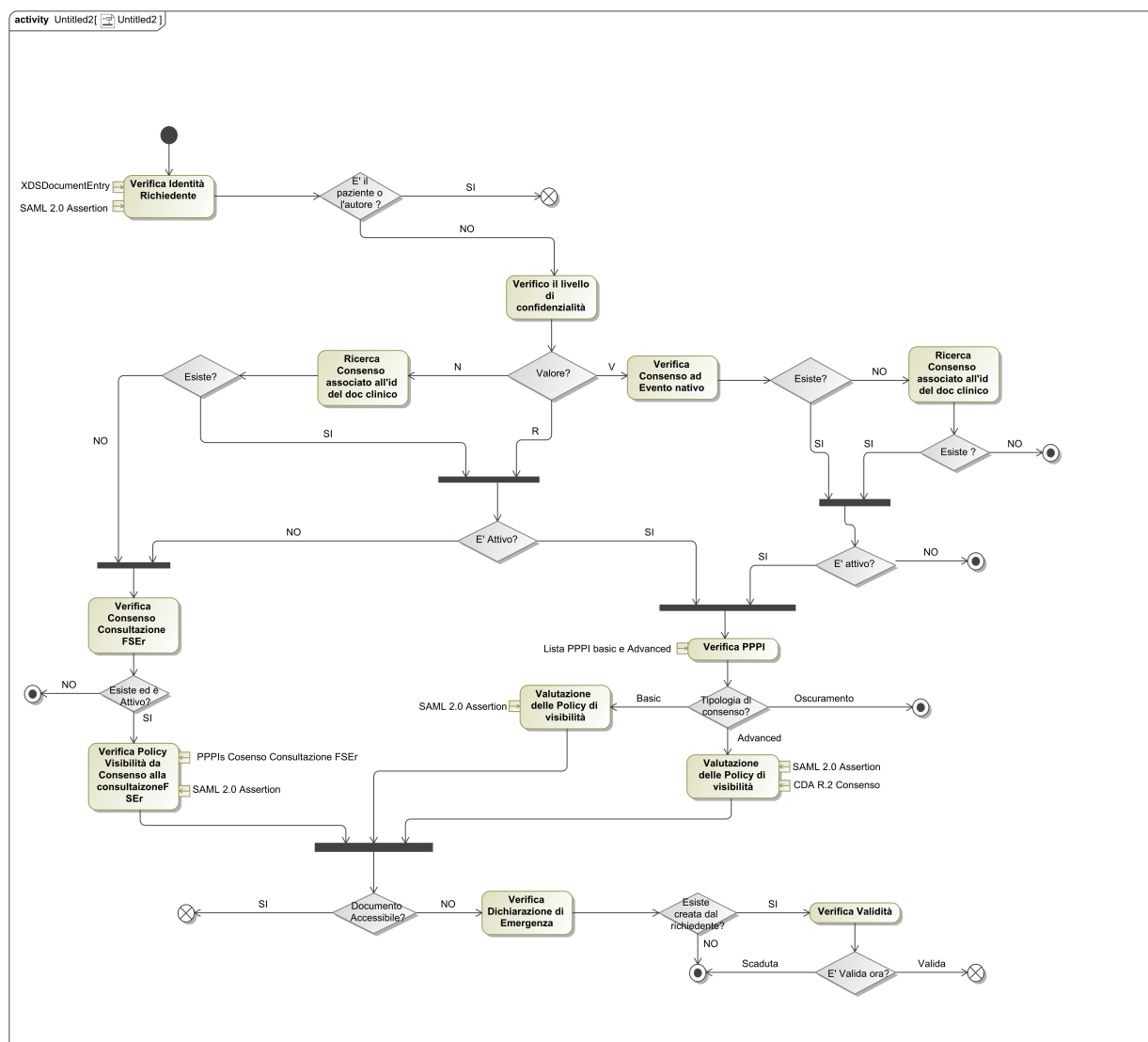


Figura 13: Processo di applicazione policy di visibilità

#### 4.1.2 Dettaglio tecnico del Processo di valutazione delle policy

- 5 Per ogni nodo decisionale viene descritta l'operazione eseguita dall'attore Policy Manager.
- “È il paziente?” → Assertion/@Role == “R.0”;



- “Che valore assume il livello di confidenzialità?” →  
XDSDocumentEntry.confidentialityCode == “N” | “R” | “V”
- 5   ▪ Esiste un documento di consenso associato ad un documento nativamente  
senza Consenso ad evento associato (“N” o “V”) ? →  
FindDocumentByReferenceID: \$XDSDocumentEntryReferenceIDList==  
XDSDocumentEntry.uniqueId (documento clinico);
- Recupero di un Consenso ad evento nativo → FindDocumentByReferenceID:  
\$XDSDocumentEntryReferenceIDList==  
XDSDocumentEntry.referenceIdList(documento clinico)
- 10   ▪ Il documento di consenso è attivo ? → XDSDocumentEntry.referenceIdList !=  
“Consenso Revocato”;
- Quale è la tipologia del documento di consenso ? →
  - Basic se XDSDocumentEntry.eventCodeList ∈ tabella A.1 -  
“urn:oid:2.16.840.1.113883.2.9.2.50.4.13.99”;
  - 15   ○ Oscuramento se XDSDocumentEntry.eventCodeList=  
“urn:oid:2.16.840.1.113883.2.9.2.50.4.13.99”;
  - Advanced se XDSDocumentEntry.eventCodeList ∈ tabella A.1.
- Valutazione delle policy di visibilità → (come definito in appendice A);
- 20   ▪ Esiste il documento di Consenso alla consultazione FSEr → FindDocuments:  
\$XDSDocumentEntryTypeCode == “Consenso Consultazione”;
- Verifica della Dichiarazione di emergenza → FindDocuments:  
\$XDSDocumentEntryTypeCode == “Dichiarazione Consultazione di Emergenza  
FSEr” ; \$XDSDocumentEntryeventCodeList ==  
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12; \$XDSDocumentEntry.author ==  
25   Assertion/Subject/NameID ; XDSDocumentEntryServiceStopTime <= now.



## 5 Creazione documenti di Consenso

### 5.1 Consenso all'alimentazione del FSEr

Il consenso all'alimentazione del FSEr può essere registrato dal paziente tramite portale o de visu dal personale Ulss, dal MMG/PLS o dal farmacista.

- 5 Il documento di raccolta del consenso in formato CDA R.2 viene creato dal portale web o dall'applicativo software del MMG/PLS/operatore Ulss/farmacista e reso disponibile nel Fascicolo Sanitario Elettronico.

Il consenso all'alimentazione del FSEr (come ogni altro consenso) deve essere compliant con le linee guida definite all'interno del profilo di integrazione BPPC (Basic Privacy Patient Consent).

10

Queste specifiche definiscono dei dettagli tecnici aggiuntivi rispetto alle linee guida IHE BPPC. I metadati associati ad un documento di consenso devono essere valorizzati in accordo a quanto definito nel documento ITI TF:3 5.1.2.1.1 "XDS DocumentEntry Metadata" e in accordo alle linee guida definite nel documento "XDS Affinity Domain FSEr".

15

Ulteriori requisiti per la definizione dei metadati nel caso di consenso all'alimentazione del FSEr sono definiti di seguito:

`XDSDocumentEntry.typeCode="Consenso FSEr"`

`XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.1"`

- 20 Gli identificativi del paziente saranno riportati come definito da ITI TF:3 5.1.2.1.1 con l'obbligatorietà della presenza del PID-13 (Phone Number - Home / XTN ) contenente il numero di telefono del paziente e la mail. I campi definiti per l'elemento PID-13 sono i seguenti:

- XTN.2 (telecommunication use code): OPZIONALE; rappresenta l'utilizzo del dato trasmesso (ad esempio "numero di casa", "telefono in caso assenza"). Per i possibili valori fare riferimento alla tabella [HL7 Table 0201];
  - XTN.3 (telecommunication equipment type): OPZIONALE; identifica il tipo di apparecchio (ad esempio telefono fisso, cellulare, fax). Per i possibili valori fare riferimento alla tabella [HL7 Table 0202];
- 25



- XTN.4 (email address): OBBLIGATORIO; contiene l'indirizzo email.
- XTN.12 (Unformatted Telephone number): OBBLIGATORIO; contiene il numero completo di prefisso;

5 Nel caso di più Tutori, deve essere presente un solo indirizzo mail ed un solo numero di telefono. Questi due valori devono essere presi dall'elemento <guardian> presente sul CDA2 marcato dall'attributo *classCode*="GUARD"

10 Nel caso in cui il numero di telefono e la mail non siano disponibili all'interno del sistema che procede alla creazione del documento di consenso il sistema DEVE permettere l'inserimento di questi dati. Nel caso in cui il paziente rifiutasse l'inserimento dovrà essere mostrato a video un warning che segnala il fatto che non verranno rilasciate credenziali d'accesso al cittadino per il proprio FSEr. In questo caso l'elemento PID-13 non sarà presente.

15 Nel caso in cui il paziente sia di minore età o sottoposto a tutela, o comunque non abbia la capacità legale d'agire, il consenso viene espresso dai soggetti che ne hanno la potestà legale. In questo caso il campo PID-13 conterrà i recapiti del tutore legale.

Esempio:

```
<rim:Slot name="sourcePatientInfo">
  <rim:ValueList>
    <rim:Value>PID-3|DTP-
1^^^&1.3.6.1.4.1.21367.2005.3.7&ISO</rim:Value>
    <rim:Value>PID-5|DICTAPHONE^ONE^^^</rim:Value>
    <rim:Value>PID-7|19650120</rim:Value>
    <rim:Value>PID-8|M</rim:Value>
    <rim:Value>PID-
11|100MainSt^^BURLINGTON^MA^01803^USA</rim:Value>
    <rim:Value>PID-
13|^^^paziente@paziente.it^5^6^7^8^9^10^11^3471234567</rim:Value>
  </rim:ValueList>
</rim:Slot>
```

Questa tipologia di consenso è un Consenso basic in quanto non è relativo ad uno specifico evento e non richiede la valutazione del contenuto del CDA R.2 per prendere decisioni di accessibilità. Si faccia riferimento alle linee guida BPPC per la strutturazione di tale CDA R.2: ITI TF:3 5.1.2.2 con la sola eccezione delle modifiche previste dall'appendice B.

## **5.2 Consenso all'alimentazione del FSEr con il pregresso**

### **5.2.1 Transazioni correlate alla sottoscrizione del consenso all'alimentazione FSEr con il pregresso**

Il consenso all'alimentazione del FSEr pregresso può essere registrato dal paziente tramite portale o de visu dal personale Ulss, dal MMG/PLS o dal farmacista, così come avviene per tutti gli altri tipi di consenso.

Il documento di consenso all'alimentazione del pregresso in formato CDA R.2 viene creato dal portale web o dall'applicativo software del MMG/PLS/operatore Ulss/farmacista e reso disponibile nel Fascicolo Sanitario Elettronico.

Questo tipo di consenso (come ogni altro consenso) deve essere compliant con le linee guida definite all'interno del profilo di integrazione BPPC (Basic Privacy Patient Consent).

Queste specifiche definiscono dei dettagli tecnici aggiuntivi rispetto alle linee guida IHE BPPC. I metadati associati ad un documento di consenso devono essere valorizzati in accordo a quanto definito nel documento ITI TF:3 5.1.2.1.1 "XDS DocumentEntry Metadata" e in accordo alle linee guida definite nel documento "XDS Affinity Domain FSEr".

Ulteriori requisiti per la definizione dei metadati nel caso di consenso all'alimentazione del FSEr sono definiti di seguito:

XDSDocumentEntry.typeCode="Consenso Alimentazione Pregresso FSEr"

XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.13"

Questa tipologia di consenso è un Consenso basic in quanto non è relativo ad uno specifico evento e non richiede la valutazione del contenuto del CDA R.2 per



prendere decisioni di accessibilità. Si faccia riferimento alle linee guida BPPC per la strutturazione di tale CDA R.2: ITI TF:3 5.1.2.2.

### 5.3 Creazione e gestione del Consenso alla consultazione

5 Il consenso alla consultazione è una tipologia di consenso che può essere applicato a tutti i documenti contenuti nel FSEr. Il paziente può quindi sottoscrivere un consenso alla consultazione non associato a specifici documenti clinici.

Le policy di visibilità ricavabili da questa tipologia di consenso alla consultazione sono applicabili in funzione dell'analisi di ruolo e contesto dell'operatore che cerca di visualizzare un dato documento clinico.

10 Si faccia riferimento alle specifiche tecniche per la generazione delle asserzioni d'identità per i dettagli relativi alla valorizzazione di tali attributi ("Infrastruttura di Sicurezza GDL-O Sicurezza").

Ad esempio il paziente può decidere di rendere visibili i propri documenti clinici contenuti (o che saranno contenuti) nel proprio FSEr solo a particolari categorie di  
15 persone, come quella degli MMG o degli specialisti in contesto di ricovero.

Vengono pertanto specificati dei veri e propri contesti di visualizzazione dei documenti che sono svincolati dal singolo documento. Il set di possibili consensi relativi a ruoli e contesti è definito in sezione A.1.

Il paziente potrebbe decidere di concedere la consultazione del proprio FSEr ad un  
20 "care giver" oppure ad un tutore legale. In questi casi, il consenso alla consultazione FSEr sarebbe di tipo "advanced".

Di seguito vengono definiti alcuni dettagli tecnici aggiuntivi rispetto alle linee guida IHE BPPC. I metadati associati ad un documento di consenso devono essere valorizzati in  
accordo a quanto definito nel documento ITI TF:3 5.1.2.1.1 "XDS DocumentEntry  
25 Metadata" e in accordo alle linee guida definite nel documento "XDS Affinity Domain FSEr".

Ulteriori requisiti per la definizione dei metadati nel caso di Consenso alla consultazione sono definiti di seguito:

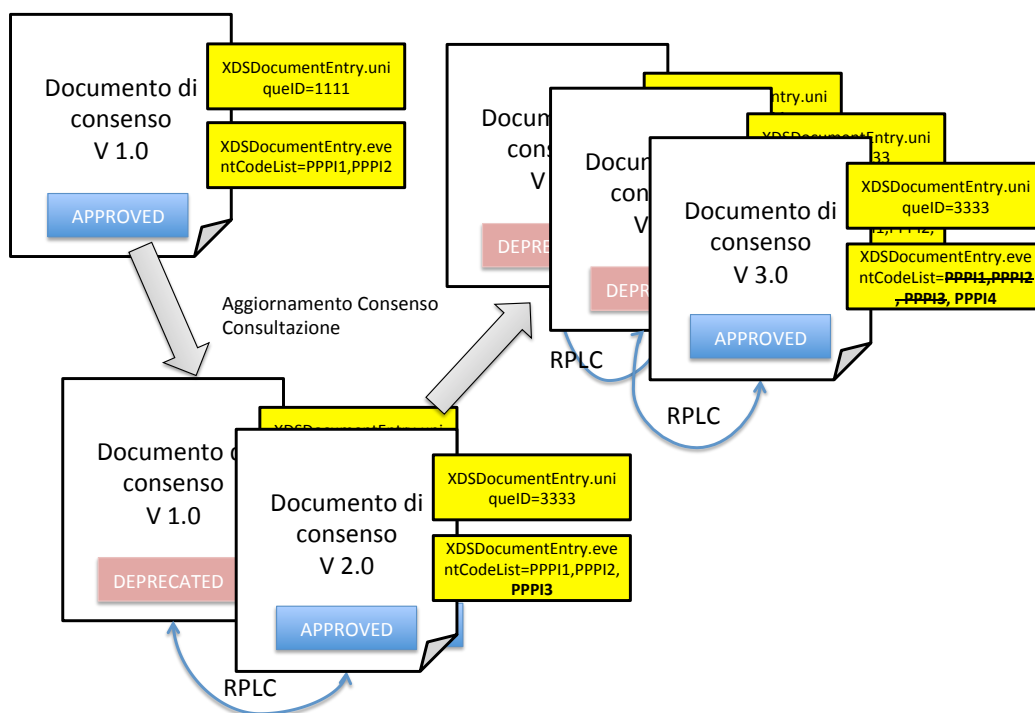
XDSDocumentEntry.typeCode="Consenso Consultazione"



XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.n"

Il metadato eventCodeList identifica il Patient Policy Privacy Identifier. Per un elenco di tutti i PPPI utilizzabili per i documenti di Consenso alla consultazione si veda sezione A.1. Tra questi riveste un ruolo particolare il PPPI: urn:oid:2.16.840.1.113883.2.9.2.50.4.13.2 che

- 5 rappresenta il consenso alla Consultazione del FSEr per "tutti i soggetti dei Servizi Socio Sanitari Regionali che prendono in cura l'assistito, presso cui sono redatti i dati e documenti sanitari che alimentano il FSE". Il consenso alla consultazione può essere aggiornato in qualsiasi momento dal paziente sul portale o dal medico/farmacista/operatore ulss tramite i propri applicativi.
- 10 Il Consenso alla consultazione viene aggiornato mediante un'azione di Replace XDS come descritto di seguito. In questo modo può esistere in ogni momento per ogni paziente un unico documento di Consenso alla consultazione in stato "APPROVED". In un'azione di Replace, possono essere aggiunte nuove PPPI rispetto alla versione precedente, oppure possono esserne selezionate di nuove. L'attore BPPC Content
- 15 Creator deve verificare che le PPPI selezionate non siano tra loro contrastanti. Di seguito è presentato il processo di aggiornamento per un Consenso alla consultazione FSEr.

**CREAZIONE e AGGIORNAMENTO DOCUMENTO CONSENSO ALLA CONSULTAZIONE****Figura 16: Processo di aggiornamento consenso alla consultazione**

## 5.4 Consenso ad evento

### 5.4.1 Creazione e gestione del documento di Consenso ad evento

- 5 Il consenso ad evento permette al paziente di dare uno specifico set di regole di visibilità di un dato documento clinico.

Nel caso in cui il paziente decida di non modificare le sue policy di privacy e di adeguarle alle policy relative a tutti i documenti contenuti nel suo FSER, verrà associato al documento clinico un metadato con confidentiality code= "N". Un documento creato con confidentialityCode "N" non ha consensi ad hoc (Consensi ad evento) associati al documento stesso e le policy di visibilità possono essere valutate solo sulla base del Consenso alla consultazione in stato "APPROVED". In

10

questo caso non è necessario creare nessun tipo di documento di consenso aggiuntivo.

Se il paziente decide invece di oscurare il referto per una o più categorie di professionisti o di estendere le policy di visibilità ad altre categorie di professionisti (modificando per lo specifico documento clinico le policy di visibilità definite nel documento di Consenso alla consultazione), il documento sarà creato con confidentialityCode= "R" (Restricted) e identificherà per il Policy Manager che il documento clinico è stato creato in modo nativo con un documento di consenso ad evento associato. Il sistema responsabile della raccolta del consenso ad evento (CUP, sportello di accettazione diretta, portale cittadino), crea un documento di consenso ad evento caratterizzato dai parametri descritti di seguito:

```
XSDDocumentEntry.typeCode="Consenso ad Evento"
```

```
XSDDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.n"
```

Il metadato typeCode identifica che il documento di consenso si applica solo ad uno specifico documento clinico. La lista di PPPI selezionati per lo specifico documento clinico sono individuate nel metadato eventCodeList.

Il metadato XSDDocumentEntry.referenceIdList del documento di consenso, deve essere utilizzato per creare il link tra documento clinico e documento di consenso come descritto di seguito. Il documento di consenso ad evento può essere aggiornato mediante un azione di XDS Replace. Per questo motivo, è necessario mantenere un identificativo fisso che viene mantenuto tra le varie versioni dello stesso documento di consenso, che si riferirà sempre allo stesso documento clinico.

- **Se il documento di Consenso ad evento viene creato prima della creazione del documento clinico associato:** (es. dichiarazione, in fase di accettazione, di voler modificare le policy di visibilità di ogni output prodotto a seguito di una determinata prestazione sanitaria) il documento clinico stesso verrà creato con un metadato XSDDocumentEntry.referenceIdList che conterrà lo stesso valore del metadato XSDDocumentEntry.referenceIdList del documento di consenso. Questo id deve essere coincidente con il valore del metadato XSDDocumentEntry.uniqueId della prima versione del documento di consenso. Questo Id è strutturato come di seguito:

```
XSDDocumentEntry.referenceIdList="[XSDDocumentEntry.uniqueId_Conse  
nso_primaVersione]^urn:rve:2014:bppcDoc"
```



Es.:

```
<rim:Slot name="urn:ihe:iti:xds:2013:referenceIdList ">
<rim:ValueList>
<rim:Value>2013001^^^1.2.3.4.5.6&ISO^urn:rve:2014:bppcDoc</r
im:Value>
</rim:ValueList>
</rim:Slot>
```

Il metadato confidentialityCode deve essere valorizzato come di seguito:

XDSDocumentEntry.confidentialityCode="R"

5 Le specifiche policy di visibilità possono essere state raccolte da un attore diverso dal Source documentale e/o il documento clinico può non esistere nel momento di creazione del consenso ad evento (es. nel caso di raccolta di tale consenso al momento dell'accettazione). In questi casi, l'integrazione tra sistema di raccolta del consenso e sistema di creazione del documento clinico  
10 deve garantire il trasferimento dell'identificativo univoco (XDSDocumentEntry.referenceIdList) del documento di consenso.

• **Se il documento di Consenso ad evento è creato dopo il documento clinico a cui si riferisce:** il documento clinico sarà stato creato con livello di confidenzialità Normal:

15 XDSDocumentEntry.confidentialityCode="N"

Il documento di consenso ad evento tratterà la relazione con il documento clinico mediante il metadato XDSDocumentEntry.referenceIdList. Questo metadato del documento di consenso deve essere valorizzato con il XDSDocumentEntry.uniqueId del documento clinico a cui si riferisce. Questo id  
20 deve essere strutturato come di seguito:

XDSDocumentEntry.referenceIdList="[XDSDocumentEntry.uniqueId\_doc\_clinico]^urn:rve:2014:bppcDoc".

Esiste una specifica policy di visibilità che può essere sottoscritta da un paziente per uno specifico documento, l'oscuramento. In questo caso il documento entra a far parte del FSEr ma non è consultabile da nessun operatore diverso dal paziente  
25



stesso. Questa tipologia di consenso, è caratterizzata dal seguente Patient Privacy Policy Identifier:

XDSDocumentEntry.eventCodeList= urn:oid:2.16.840.1.113883.2.9.2.50.4.13.99

#### 5 5.4.2 Aggiornamento Documento di Consenso ad Evento

Le policy di visibilità selezionate ad hoc per un documento clinico possono essere cambiate a discrezione del paziente. Questa modifica è eseguita mediante una operazione di Replace XDS che deve mantenere, per la nuova versione del documento di consenso, lo stesso valore di metadatao XDSDocumentEntry.referenceIdList della versione deprecata.

È illustrato di seguito il legame concettuale realizzato tra documenti clinici (nel caso di documento di consenso creato prima del documento clinico associato) e documenti di consenso ad evento.

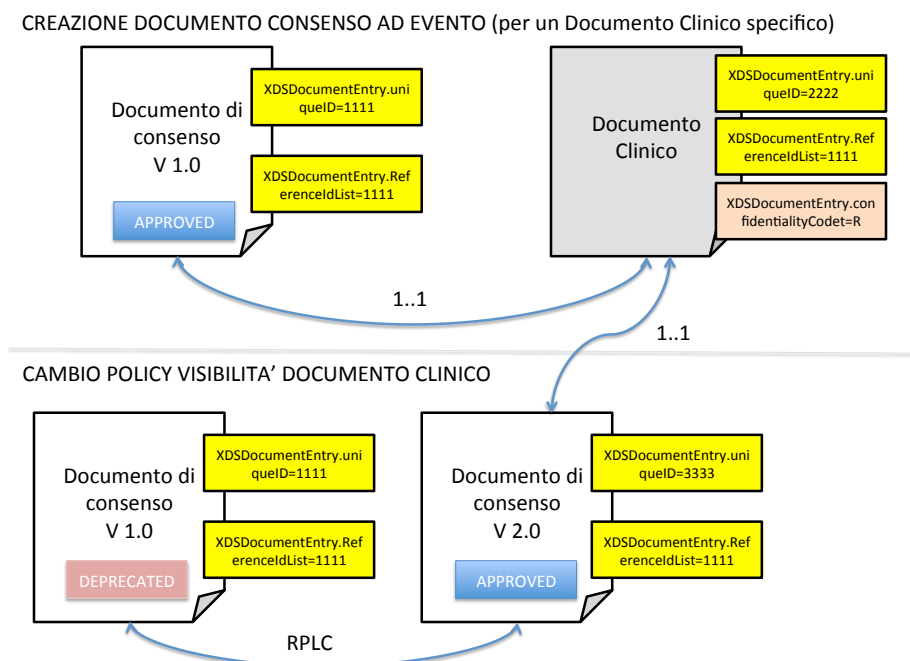


Figura 17: Processo di creazione Consenso ad evento

## 5.5 Livello di Confidenzialità dei Documenti Clinici

Ad ogni documento clinico è associato uno specifico livello di confidenzialità che identifica le policy di visibilità native del documento stesso.

- 5            ➤ N (Normal): documento clinico per il quale, nativamente, valgono le policy di visibilità di default del FSEr. Questo documento potrebbe non avere documenti di consenso ad evento associati. Un documento con questa tipologia di confidenzialità non contiene dati a maggior tutela dell'anonimato.
- 10          ➤ R (Restricted): documento per il quale, nativamente, è stato creato un consenso alla consultazione ad evento. Un documento con questa tipologia di confidenzialità non contiene dati a maggior tutela di anonimato. Il documento stesso (metadati) contiene il riferimento al documento di Consenso ad evento associato.
- 15          ➤ V (Very Restricted): un documento clinico caratterizzato da questo livello di confidenzialità contiene dati a maggior tutela di anonimato. Il documento può avere dei documenti di consenso ad evento associati.

Di seguito (e in figura 14 ) è descritto il processo mediante cui viene associato un determinato livello di confidenzialità ad un documento clinico prodotto.

- 20          Si sottolinea che le policy di visibilità possono essere create ed applicate con massima granularità possibile al massimo ad un documento, che costituisce quindi l'unità atomica che può essere rivelata o meno ad un richiedente.

La granularità (numero di referti prodotti) con cui verranno strutturati i dati clinici prodotti da una struttura sanitaria NON è ipotizzabile prima dell'effettiva esecuzione della prestazione stessa (per esempio, una determinata prestazione potrebbe comportare la produzione di uno o più referti in funzione del risultato di una o più osservazioni).

- 30          Se il paziente decide di sottoscrivere delle specifiche policy di visibilità associandole ad un determinato evento/prestazione (richiedendo la creazione di un documento di Consenso ad evento prima della refertazione), le stesse policy di visibilità si applicheranno ad ogni referto prodotto a seguito di tale prestazione/evento.

Questo legame tra N referti e 1 documento di Consenso alla consultazione ad evento è definitivo (non può essere modificato nel tempo), in quanto il documento clinico sarà caratterizzato sempre dallo stesso riferimento (XDSDocumentEntry.referenceIdList) al documento di consenso. Ogni successivo aggiornamento delle policy di visibilità si applicherà obbligatoriamente a tutti i referti prodotti a seguito della medesima prestazione. Questo approccio semplifica notevolmente il processo di sottoscrizione di consensi alla consultazione ad evento prima dell'effettiva refertazione e garantisce la copertura con le medesime policy di visibilità di documenti che potrebbero essere correlati non solo dal punto di vista organizzativo ma anche contenutistico.

### 5.5.1 Processo di definizione del livello di confidenzialità

L'obiettivo di questa sezione è descrivere in modo sintetico il flusso informativo che regola l'assegnazione del livello di confidenzialità ad un documento clinico prodotto da un'azienda sanitaria.

Non viene definito in questa sezione con che livello di granularità può essere raccolto il consenso alla consultazione ad evento prima del processo di refertazione stesso. Si ricorda che questa modalità di sottoscrizione è l'unica che garantisce l'ingresso dei documenti clinici nel FSEr in modo nativo con policy di visibilità assegnate ad hoc.

Il Consenso alla consultazione ad evento può essere raccolto ed associato:

- Ad una ricetta/ordine: il paziente può sottoscrivere delle policy di visibilità ad hoc che si applicheranno a tutti i documenti di referto prodotti a seguito della erogazione dell'intera ricetta. Questo caso si applica, per esempio, in regime di accettazione diretta nel caso in cui il paziente usufruisca di tutte le prestazioni prescritte durante lo stesso evento. Questa atomicità dell'evento può comportare la produzione di più referti. Ad ogni referto verranno applicate le policy di visibilità sottoscritte.
- Ad ogni prestazione prenotata/eseguita: il paziente potrà sottoscrivere delle policy di visibilità ad hoc per ogni prestazione prenotata. In questo caso le prestazioni comporteranno la produzione di un numero di referti maggiore o uguale al numero di prestazioni

prenotate. Referti afferenti alla stessa prestazione ereditano le stesse policy di visibilità.

Se il paziente decide di sottoscrivere un documento di Consenso alla consultazione ad evento, vengono identificate le policy di visibilità e viene creato un documento di consenso alla consultazione ad evento. **L'identificativo univoco del documento di consenso DEVE essere trasferito insieme alle informazioni di prenotazione/accettazione al sistema ambulatoriale o dipartimentale responsabile della refertazione e della pubblicazione del documento.** Un documento clinico che ha nativamente un documento di consenso alla consultazione ad evento associato, può essere caratterizzato da livello di confidenzialità "R" oppure "V" se la prestazione richiesta comporta la produzione di dati a maggior tutela dell'anonimato.

La valutazione di quale livello di confidenzialità è necessario applicare alla prestazione è legato al contenuto della Appendice B di questo documento. Se la prestazione (o la ricetta nel caso in cui non sia possibile gestire in modo atomico le prestazioni richieste) ricade nel set di prestazioni a maggior tutela dell'anonimato, il livello di confidenzialità dei documenti che verranno prodotti deve essere "V".

Questa valutazione DEVE essere ripetuta in fase di refertazione. Se, in fase di refertazione, vengono associati al documento clinico di referto dei risultati clinici che possono ricadere nel set di dati a maggior tutela dell'anonimato, il documento clinico deve essere prodotto con livello di confidenzialità "V". È quindi possibile che una prestazione che una prestazione non considerata a maggior tutela dell'anonimato comporti la produzione di un referto con livello di confidenzialità più restrittivo.

Se il paziente decide di non sottoscrivere un documento di Consenso ad evento per il documento clinico, esso potrà essere creato con livello di confidenzialità "N" o "V". Anche in questo caso, se la prestazione richiesta, o i risultati refertati, veicolano informazioni a maggior tutela dell'anonimato, il documento verrà prodotto con livello di confidenzialità "V".

Se dalla medesima prestazione sono prodotti più referti clinici, il processo di analisi della confidenzialità del contenuto del documento deve essere ripetuto per tutti i documenti prodotti. È lasciato alle logiche applicative/organizzative aziendali, la possibilità di raggruppare all'interno dei referti prodotti le prestazioni e i risultati in funzione del livello di confidenzialità (Es. un LIS particolarmente avanzato potrebbe raggruppare nello stesso referto tutti i risultati a maggior tutela dell'anonimato,



producendo un referto con livello di confidenzialità "V", in modo da rendere accessibili e fruibili in modo più immediato i restanti dati, che potrebbero essere raggruppati in un referto con livello di confidenzialità "R").

- 5 Il medico refertatore può ritenere opportuna l'interruzione del processo di pubblicazione di un referto. In questo caso, se le modalità organizzative dell'azienda sanitaria di riferimento lo permettono, il processo è sospeso fino alla conferma di avvenuto contatto con il paziente.

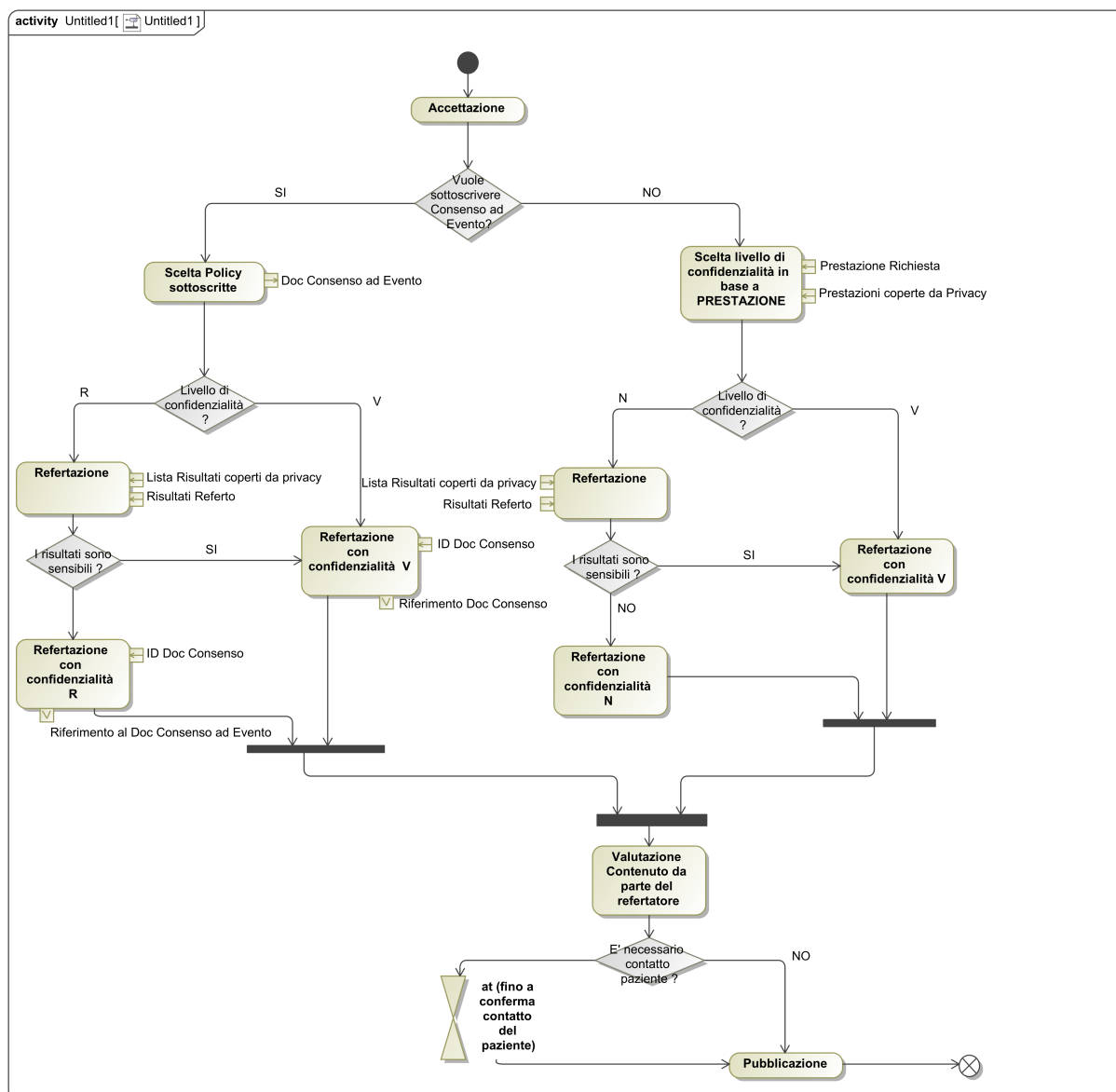


Figura 18: Processo di Refertazione e Pubblicazione

## 5.6 Revoca di un Consenso (alimentazione, consultazione o ad evento)

La revoca del consenso all'alimentazione o del consenso alla consultazione del FSEr è possibile in qualsiasi momento e può essere eseguita ad opera degli stessi attori in grado di sottoscrivere questi documenti di consenso (sistema aziendale, cartella del medico di medicina generale, portale paziente). Nel momento in cui il paziente decide di revocare il Consenso all'alimentazione FSEr non è più possibile indicizzare documenti associati al determinato paziente all'interno del XDS Document Registry regionale. Se viene revocato il Consenso alla consultazione del FSEr, nessun operatore sarà in grado di recuperare documenti dal FSEr per quel determinato paziente. Lo stesso approccio deve essere adottato per un documento di Consenso ad evento. Nel caso in cui il paziente desideri revocare il consenso ad hoc sottoscritto per un determinato documento clinico, il documento di consenso ad evento deve essere sostituito con una nuova versione, mediante un'azione di replacement. In questo caso, restano applicabili le sole policy ricavabili dal documento di Consenso alla consultazione FSEr.

L'azione di revoca di uno dei tre consensi consiste nel replacement del documento di consenso con un nuovo documento caratterizzato dai seguenti metadati:

- XDSDocumentEntry.typeCode="Consenso Consultazione" (o "Consenso FSEr" o "Consenso ad Evento");
- XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.100";

## 5.7 Dichiarazione di consultazione in emergenza

Un operatore sanitario o socio-sanitario potrà avere accesso al FSEr di un determinato paziente, benché privo del consenso alla consultazione da parte dello stesso. Le condizioni che legittimano tale accesso "straordinario" sono riportate nel testo della norma (DPCM FSE).

L'operatore, dopo aver sottoscritto un'esplicita Dichiarazione di consultazione in emergenza, potrà accedere, per un limitato periodo di tempo, ai documenti clinici del paziente contenuti nel FSEr e resi consultabili almeno ad un operatore/classe di operatori.

La Dichiarazione di consultazione in emergenza è uno specifico documento di consenso (sempre strutturato in accordo alle linee guida IHE BPPC) strutturato in

formato CDA R2. L'operatore che sottoscrive la dichiarazione deve definire la durata di tale sottoscrizione. All'interno del CDA R2 la durata della dichiarazione deve essere strutturata come di seguito. All'interno dell'elemento <documentationOf>/<serviceEvent>/<effectiveTime> viene riportata la durata temporale della dichiarazione di emergenza. All'interno dell'attributo value del sotto-elemento <effectiveTime>/<low> viene riportato la data dell'inizio della validità della dichiarazione, mentre nell'attributo value del sotto-elemento <effectiveTime>/<high> viene riportata la data di fine validità della dichiarazione. Entrambi gli elementi sono caratterizzati da un tipo di dato TS, e devono contenere la data con anno, mese, giorno, ora, minuti, secondi: YYYYMMddhhmmss+|-ZZzz. Le ore devono essere riportate nell'intervallo 00:00:00 - 23:59:59. ZZzz rappresenta l'offset rispetto al tempo di Greenwich (GMT-Greenwich Mean Time). Il valore dell'offset dipenderà dalle impostazioni di ora legale; per l'Italia potrà variare fra ZZzz valorizzato con +0100 oppure +0200 (nel caso di ora legale). Di seguito viene riportato un frammento di CDA di esempio:

```
<documentationOf>
  <serviceEvent>
    <code code="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12"
      displayName="Dichiarazione Consultazione in Emergenza"
      codeSystem="2.16.840.1.113883.2.9.2.50.6.30"
      codeSystemName="PPPI_Regione_Veneto"/>
    <!-- durata temporale dichiarazione di consultazione in
    emergenza> -->
    <effectiveTime>
      <low value="20070510093000+0100"/>
      <high value="20070511093000+0100"/>
    </effectiveTime>
  </serviceEvent>
</documentationOf>
```

I metadati del documento di Dichiarazione di consultazione in emergenza devono essere caratterizzati dalle seguenti specificità:

XDSDocumentEntry.typeCode="Dichiarazione Consultazione Emergenza FSEr"

20 XDSDocumentEntry.eventCodeList="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12"



XDSDocumentEntry.serviceStartTime= data/ora sottoscrizione dichiarazione;

XDSDocumentEntry.serviceStopTime= data/ora scadenza della sottoscrizione.

## 5.8 Struttura Consenso basic

5 Un Consenso basic è un documento di consenso per il quale l'attore Policy Manager può valutare le policy di accessibilità ad un determinato documento solamente interpretando i metadati associati al documento di consenso stesso. Queste tipologie di consensi sono caratterizzati dalle PPPI definite in sezione A.1.

10 Il consenso Basic viene creato da un attore BPPC Content Creator in accordo alle linee guida definite nel profilo di integrazione IHE BPPC con la sola eccezione delle modifiche previste dall'appendice B. Le specifiche tecniche per la strutturazione del documento in formato CDA R.2 sono definite in sezione 5.1.2 Patient Privacy Consent Acknowledgment Document Specification 1.3.6.1.4.1.19376.1.5.3.1.1.7 – With no Scanned Document Part.

15 Non è previsto di inserire all'interno del documento di Consenso un oggetto PDF contenente la Wet Signature del paziente che sottoscrive lo specifico documento di Consenso.

## 5.9 Struttura Consenso Advanced

20 Un Consenso Advanced è un documento di consenso per il quale l'attore Policy Manager può valutare le policy di accessibilità ad un determinato documento valutando il contenuto del documento di consenso. Queste tipologie di consensi sono caratterizzati dalle PPPI definite in sezione A.2.

Il Consenso Advanced viene creato da un attore BPPC Content Creator in accordo alle linee guida definite nel profilo di integrazione IHE BPPC con la sola eccezione delle modifiche previste dall'appendice B.

25 Non è previsto di inserire all'interno del documento di Consenso un oggetto PDF contenente la Wet Signature del paziente che sottoscrive lo specifico documento di Consenso.

## Appendice A: OID consensi basic e advanced

In questa sezione vengono definiti i Patient Privacy Policy Identifiers (PPPIs) selezionabili dal paziente ed associabili ai documenti di consenso che condizionano visibilità dei documenti. Questi identificativi vengono utilizzati per codificare il metadatao

5 XDSDocumentEntry.eventCodeList.

### A.1. PPPI Consensi basic

OID PPPI	Descrizione PPPI	Note (Verifiche Policy Manager)
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.1	Consenso alla alimentazione del FSEr	
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.2	Consenso alla consultazione per tutti gli operatori coinvolti nel PDTA del paziente	*Contesti ammessi: (Assertion/Request Context="C.1.1", "C.1.2", "C.1.3", "C.2.1", "C.2.2", "C.2.3", "C.3.1",)
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.3	Consenso alla consultazione per MMG/PLS	Verificata da policy Manager per Assertion/Request Context="C.1.1" o "C.1.2"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.4	Consenso alla consultazione per farmacista	Verificata da policy Manager per Assertion/Request



		Context="C.5.1" o "C.4.2"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.5	Consenso alla consultazione per operatore amministrativo	Verificata da policy Manager per Assertion/Request Context="C.6.1", "C.6.2", "C.6.3", "C.6.4"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.6	Consenso alla consultazione per direttore sanitario	Verificata da policy Manager per Assertion/Role="R. 1.9"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.7	Consenso alla consultazione per direttore amministrativo	Verificata da policy Manager per Assertion/Role="R. 4.2"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.8	Consenso alla consultazione per Medico (RSA)	Verificata da policy Manager per Assertion/Request Context="C.8"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.9	Consenso alla consultazione per Infermiere	Verificata da policy Manager per Assertion/Role="R. 1.10" o "R.1.11"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.10	Consenso alla consultazione per Medico rete di patologia	Verificata da policyManager per Assertion/Request



		Context="C.9"
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.11	Consenso alla consultazione per Operatore socio sanitario	Verificata da Policy Manager per Assertion/role R.1.34
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.12	Dichiarazione Consultazione in Emergenza	
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.13	Consenso Alimentazione Pregresso FSEr	
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.99	Oscuramento del documento	
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.100	Consenso Revocato	

\* Per i dettagli relativi ai Contesti e Ruoli si faccia riferimento al documento "Infrastruttura di sicurezza" redatto dal GDL-O Sicurezza

## A.2. PPPI Consensi Advanced

5

OID PPPI	Descrizione PPPI	Note (Verifiche Policy Manager)
urn:oid:2.16.840.1.113883.2.9.2.50.4.13.14	Consenso di tipo advanced: esclusione tipologia referti, delega minore,	



	care giver	
--	------------	--

## Appendice B: Aggiunte alle linee guida BPPC per la strutturazione del CDA R.2.

### B.1 ClinicalDocument/RecordTarget

- 5 All'interno della sezione relativa al paziente vengono aggiunte le obbligatorioità riportate nelle sezioni sottostanti rispetto alla guida BPPC.

#### B.1.1 Numero di telefono e mail del paziente

Il numero di telefono e la mail del paziente DEVONO essere riportati all'interno di almeno due elementi <recordTarget>/<patientRole>/<telecom>

- 10
- Deve essere presente almeno 1 elemento <telecom> con attributo use = "MC" e attributo value="tel:(\$Pref)\$Num"/> (dove \$Pref= prefisso telefonico e \$Num= numero telefonico)
  - Deve essere presente almeno 1 elemento <telecom> con attributo value="mailto:\$mail" (dove \$mail= mail paziente)
- 15

Nel caso in cui l'interessato è di minore età o sottoposto a tutela, o comunque non ha la capacità legale d'agire ed il consenso viene espresso dai soggetti che ne hanno la potestà legale, DEVE essere riportato il numero di telefono all'interno dell'elemento <guardian>. In questo caso l'elemento <telecom> all'interno

20 <recordTarget>/<patientRole> può essere non presente.

Ad Esempio:

```
<guardian>  
...  
25 <telecom use="MC" value="tel:(0039)334334334334"/>  
    <telecom value="mailto:tutore1.e-mail@example.com"/>  
    <guardianPerson>
```

```
...  
</guardianPerson>  
...  
</guardian>
```

5

10

Nel caso in cui il numero di telefono e la mail non siano disponibili all'interno del sistema che procede alla creazione del documento di consenso il sistema DEVE permettere l'inserimento di questi dati. Nel caso in cui il paziente o il tutore legale rifiutasse l'inserimento di uno dei due dati o entrambi dovrà essere mostrato a video un warning che segnala il fatto che non verranno rilasciate credenziali d'accesso al cittadino per il proprio FSEr.

In questo caso, l'elemento <telecom> figlio dell'elemento <patientRole> e l'elemento <telecom> figlio dell'eventuale elemento <guardian> dovranno avere un solo attributo nullFlavor="ASKU" (asked but unknown).

15

Ad esempio:

```
<telecom nullFlavor="ASKU"/>.
```

### B.1.2 Tutore Legale

20

Nei casi previsti dalla legge è OBBLIGATORIO che all'interno della sezione recordTarget sia presente un elemento <recordTarget>/<patientRole>/<patient>/<guardian> contenente tutte le informazioni relative al tutore legale del paziente.

Nel caso di un solo tutore legale l'elemento <guardian> DEVE avere attributo classCode="GUARD".

25

Nel caso di più tutori legali, uno solo dei tutori presenti e specializzati dall'elemento <guardian> DEVE avere attributo classCode="GUARD" ( il tutore a cui verranno inviate le credenziali di accesso FSEr mediante mail/numero telefono ), mentre per gli altri NON l'attributo NON deve essere presente.

Per il CDA di consultazione nel caso di Tutore Legale, all'interno dell'Header, DEVE essere presente un documentationOf/serviceEvent di tipo Advanced.

30

*Fare riferimento alle Specifiche Tecniche per la creazione del documento informatico del Progetto "Riuso Veneto-ESCAPE" [REF1].*



## Esempio Sezione RecordTarget

```
<recordTarget>
  <patientRole classCode="PAT">
    <id assigningAuthorityName="Ministero Economia e Finanze" extension="CF"
5      root="2.16.840.1.113883.2.9.4.3.2"/>
    <!-- CF -->
    <id assigningAuthorityName="Regione Veneto" extension="MPI"
      root="2.16.840.1.113883.2.9.2.50.4.1.2"/>
    <!-- MPI -->
10    <addr use="HP">
      <houseNumber>NUMERO CIVICO</houseNumber>
      <streetName>VIA</streetName>
      <postalCode>CAP</postalCode>
      <city>CITTA</city>
15
    </addr>
    <!-- aggiungere per consenso alla consultazione 18/02/16 -->
    <telecom use="MC" value="tel:(0039)0422216129"/>
    <telecom value="mailto:patient.e-mail@example.com"/>
20    <patient>
      <name>
        <family>COGNOME</family>
        <given>NOME</given>
      </name>
25    <administrativeGenderCode code="F" codeSystem="2.16.840.1.113883.5.1"/>
    <birthTime value="19590527"/>
    <!-- Tutore Legale -->
    <guardian classCode="GUARD">
      <id assigningAuthorityName="Ministero Economia e Finanze" extension="CFtutore"
30      root="2.16.840.1.113883.2.9.4.3.2"/>
      <!-- CF -->
      <id assigningAuthorityName="Regione Veneto" extension="MPItutore"
        root="2.16.840.1.113883.2.9.2.50.4.1.2"/>
      <guardianPerson>
35        <name>
          <family>COGNOME Tutore</family>
          <given>NOME Tutore</given>
        </name>
40
      </guardianPerson>
      </guardian>
45    </patient>
  </patientRole>
</recordTarget>
```

### B.1.3 Consensi Advanced: Care-giver

Nei casi previsti dalla legge è **OBBLIGATORIO** che sia presente all'interno del Body del CDA2 sezione "Patient Consent" (codice LOINC "59284-0") contenente le informazioni riguardanti il consenso "Advanced". La sezione DEVE avere un elemento <code> valorizzato come da tabella seguente: essere strutturata come di seguito:

5

Attributo	R/O	Tipo	Valore	Descrizione
code	R	ST	59284-0	LOINC Code for Patient Consent
codeSystem	R	OID	2.16.840.1.113883.6.1	OID del sistema di codifica delle regole
codeSystemName	O	ST	LOINC	Tipo Codifica
displayName	O	ST	Patient Consent	Descrizione Regola

Per il CDA di consultazione, nel caso in cui si voglia delegare anche il Care Giver alla consultazione, all'interno dell'Header DEVE essere presente un documentationOf/serviceEvent di tipo Advanced.

### 10 **B.1.3.1 Specifica tipo di consenso avanzato <entry>/<act>**

All'interno della <section> DEVE essere presente un elemento <entry>/<act> con attributi classCode="CONS" moodCode="EVN che specifica la tipologia di consenso avanzato definita nella sezione. La tipologia di consenso avanzato viene specificata all'interno di un elemento <act>/<code> che deve essere popolato come da tabella seguente:

15

Attributo	R/O	Tipo	Valore	Descrizione
code	R	ST	OID del sistema di identificazione (es. urn:oid:2.16.840.1.113883.2.9.2.50.4.13.14)	Code per consenso Advanced
codeSystem	R	OID	2.16.840.1.113883.2.9.2.50.6.30	OID del sistema di codifica delle



				regole
displayName	O	ST	Advanced	Descrizione Regola

#### B.1.3.1.1 Care Giver <act>/<participant>

Il "Care Giver" viene specificato mediante l'elemento <act>/<participant typeCode="CON">/<participantRole classCode="NOK">. Sarà presente un elemento <participant> per ogni "care giver".

Gli identificativi per il "care giver" sono:

- MPI (OBBLIGATORIO); l'MPI regionale deve essere recuperato puntualmente dall'applicativo mediante una Query Paziente.
- Codice Fiscale / STP / ENI

Queste informazioni devono essere specificate in un elemento <id> contenuto all'interno di <participantRole>. L'elemento <id> viene popolato come da tabella seguente:

Attributo	R/O	Tipo	Valore	Descrizione
root	R	OID	OID del sistema di identificazione (es. "2.16.840.1.113883.2.9.4.3.2")	OID del sistema di identificazione
extension	R	ST	Identificativo del "care giver"	Identificativo del soggetto

Gli OID utilizzabili per gli identificativi sono:

OID del documento	Tipologia Identificativo
2.16.840.1.113883.2.9.4.3.2	Codice Fiscale
2.16.840.1.113883.2.9.2.50.4.1.1	STP_RVE
2.16.840.1.113883.2.9.2.50.4.1.4	ENI_RVE
2.16.840.1.113883.2.9.2.50.4.1.2	MPI Regione Veneto



## Esempio sezione "Consensi Advanced"

```
<component>
  <section>
5    <code code="59284-0" codeSystem="2.16.840.1.113883.6.1" codeSystemName="LOINC"
      codeSystemVersion="2.19" displayName="Patient Consent"></code>
    <entry>
      <act classCode="CONS" moodCode="EVN">
10        <code code="urn:oid:2.16.840.1.113883.2.9.2.50.4.13.14"
            displayName="Advanced"
            codeSystem="2.16.840.1.113883.2.9.2.50.6.30"/>
        <participant typeCode="CON">
          <participantRole classCode="NOK">
15            <id assigningAuthorityName="Ministero Economia e Finanze" extension="CF"
                root="2.16.840.1.113883.2.9.4.3.2"/>
            <!-- CF -->
            <id assigningAuthorityName="Regione Veneto" extension="MPI"
                root="2.16.840.1.113883.2.9.2.50.4.1.2"/>
          </participantRole>
20        </participant>
        <participant typeCode="CON">
          <participantRole classCode="NOK">
25            <id assigningAuthorityName="Ministero Economia e Finanze" extension="CF"
                root="2.16.840.1.113883.2.9.4.3.2"/>
            <!-- CF -->
            <id assigningAuthorityName="Regione Veneto" extension="MPI"
                root="2.16.840.1.113883.2.9.2.50.4.1.2"/>
          </participantRole>
30        </participant>
      </act>
    </entry>
  </section>
35 </component>
```

## Appendice C: Dati a maggior tutela dell'anonimato

To be defined



## Appendice D: Requisiti Interfaccia Raccolta Consenso FSEr

### D.1 FSEr - Gestione consenso alimentazione, consultazione ed alimentazione del pregresso.

5 L'alimentazione del Fascicolo Sanitario Elettronico con informazioni, dati e documenti sia futuri che pregressi e la loro consultazione attraverso il FSEr da parte dei soggetti autorizzati, implica un trattamento di dati. Al fine di ottemperare alla norma, è necessario acquisire preventivamente il consenso dell'interessato.

10 Il consenso per il FSEr viene prestato soltanto dall'interessato al quale si riferiscono i dati sanitari, purché maggiorenne, nel pieno possesso delle capacità giuridiche.

Si ricorda che contestualmente al rilascio del consenso alla alimentazione del FSEr, la cartella del MMG/PLS richiederà l'inserimento del numero di cellulare e l'indirizzo e-mail al fine di attivare la visibilità dei documenti clinici e/o dei figli di minore età.

15 Nel caso in cui il numero di telefono e la mail non siano disponibili all'interno del sistema che procede alla creazione del documento di consenso il sistema DEVE permettere l'inserimento di questi dati. Nel caso in cui il paziente rifiutasse l'inserimento dovrà essere mostrato a video un warning che segnala il fatto che non verranno rilasciate credenziali d'accesso al cittadino per il proprio FSEr.

20 Se l'interessato è di minore età o sottoposto a tutela, o comunque non ha la capacità legale d'agire, il consenso viene espresso dai soggetti che ne hanno la potestà legale.

Nel caso sia il genitore che presti il consenso per il figlio minore, il MMG/PLS dovrà acquisire le seguenti informazioni relative al genitore all'interno della gestione consenso FSEr:

25 ☐ dati identificativi del tutore:

- Nome
  - cognome,
  - MPI + Codice Fiscale / STP / ENI
  - numero di cellulare + e-mail (Nel caso in cui il tutore rifiutasse
- 30 l'inserimento dovrà essere mostrato a video un WARNING che



segnala il fatto che non verranno rilasciate le credenziali assegnate al tutore legale per l'accesso al FSEr del paziente sotto tutela).

- 5 Se non presente in cartella l'MPI regionale del tutore DEVE essere recuperato puntualmente dall'applicativo mediante una Query Paziente.

Il presente genitore è munito della potestà:

- ☐ congiunta con il coniuge. In questo caso deve essere richiesto per ciascun coniuge le informazioni della sezione precedente. All'interno del CDA2 saranno presenti 2 elementi <guardian>.
- 10 ☐ in via esclusiva.

Valori possibili per il consenso FSEr:

Consenso alla alimentazione del FSEr	<p>DEVE essere visualizzato:</p> <p>"Con tale consenso e solo dopo la sua acquisizione, il cittadino permette al sistema di formare il proprio FSEr, alimentandolo con i suoi dati e documenti, avendoli sempre disponibili in modalità digitale"</p> <p>Nel caso in cui il consenso venga negato DEVE essere mostrato un WARNING che specifica che se il cittadino nega il consenso alla alimentazione nessun fascicolo verrà formato.</p>
Consenso alla consultazione FSEr	<p>DEVE essere visualizzato:</p> <p>"Con tale consenso il cittadino permette o meno ai soggetti autorizzati, che lo prenderanno in cura, per il tempo strettamente necessario e collegato al processo di cura stesso, di consultare i propri dati sanitari e socio sanitari."</p> <p>Se il cittadino nega il consenso dovrà essere mostrato un WARNING che specifica che i documenti non saranno consultabili a nessun medico, nemmeno colui che ha in cura il paziente, rendendo meno semplice il processo di acquisizione delle informazioni per le finalità di cura.</p>



Consenso alla alimentazione del FSEr con documenti di eventi clinici pregressi	<p>DEVE essere visualizzato:</p> <p>“Con tale consenso si chiede al cittadino se permette che il Fascicolo sia alimentato con i dati e i documenti relativi a eventi accaduti precedentemente alla data in cui ha acconsentito alla formazione del Fascicolo.”</p> <p>Se il valore espresso risulta essere NEGATO, i dati precedentemente prodotti non verranno caricati e quindi non resi consultabili attraverso il Fascicolo.</p> <p>Dovrà essere mostrato un WARNING che specifica che il mancato consenso impedisce anche al MMG/PLS di visualizzare i documenti pregressi.</p> <p>Inoltre deve essere specificato che il recupero dei dati e dei documenti pregressi è strettamente vincolato alla attuale capacità dell'infrastruttura di richiamarli, ponendoli a disposizione nel FSEr.</p>
--	--

### D.3 FSEr - Gestione consenso privacy con delega al care giver

5 Nel caso in cui il paziente decida di vuole affidare la gestione del proprio FSEr ad un care giver, la cartella del MMG/PLS richiederà l'inserimento di alcune informazioni aggiuntionali relative al care giver.

10 Il documento di consenso di tipo advanced esprime la sua volontà del paziente di delegare una persona terza alla gestione del proprio FSEr. In questo caso il MMG/PLS dovrà acquisire le seguenti informazioni relative al care giver all'interno della gestione consenso FSEr:

☐ dati identificativi del care giver:

- Nome
- cognome,
- MPI + Codice Fiscale / STP / ENI



Se non presente in cartella l'MPI regionale del care giver DEVE essere recuperato puntualmente dall'applicativo mediante una Query Paziente.





## Bibliografia

- IHE, IT Infrastructure Technical Framework, Volume 1 (ITI TF-1):  
[http://www.ihe.net/uploadedFiles/Documents/ITI/IHE\\_ITI\\_TF\\_Vol1.pdf](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf)
- 5 • IHE, IT Infrastructure Technical Framework, Volume 3 (ITI TF-3):  
[http://www.ihe.net/uploadedFiles/Documents/ITI/IHE\\_ITI\\_TF\\_Vol3.pdf](http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol3.pdf)
- Documento di specifiche tecniche di sicurezza: "Infrastruttura di sicurezza  
GDL-O Sicurezza vX.0"
- Documento GDL-O Privacy "Casi d'uso e gestione delle policy"
- 10 • DPCM FSE