



**Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni**

Stato dell'arte sulle iniziative nazionali relative allo sviluppo di sistemi ICT interoperabili per la Salute Digitale

Mario Ciampi, Angelo Esposito, Mario Sicuranza

RT-ICAR-NA-2019-04

Data: maggio 2019



Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) – Sede di Napoli, Via P. Castellino 111, I-80131 Napoli, Tel: +39-0816139508, Fax: +39-0816139531, e-mail: napoli@icar.cnr.it, URL: www.icar.cnr.it



**Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni**

Stato dell'arte sulle iniziative nazionali relative allo sviluppo di sistemi ICT interoperabili per la Salute Digitale

Mario Ciampi, Angelo Esposito, Mario Sicuranza

Rapporto Tecnico N: RT-ICAR-NA-2019-04

Data: maggio 2019

I rapporti tecnici dell'ICAR-CNR sono pubblicati dall'Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche. Tali rapporti, approntati sotto l'esclusiva responsabilità scientifica degli autori, descrivono attività di ricerca del personale e dei collaboratori dell'ICAR, in alcuni casi in un formato preliminare prima della pubblicazione definitiva in altra sede.

Stato dell'arte sulle iniziative nazionali relative allo sviluppo di sistemi ICT interoperabili per la Salute Digitale

Mario Ciampi, Angelo Esposito, Mario Sicuranza

Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche

Via Pietro Castellino, 111 – 80131 Napoli, Italia

E-mail: {mario.ciampi, angelo.esposito, mario.sicuranza}@icar.cnr.it

Abstract

Nell'ultimo decennio le iniziative nazionali volte alla realizzazione di servizi per la Salute Digitale sono state numerose, in termini di emanazione di normative, di progettazione tecnica dei sistemi ICT abilitanti e di sviluppo tecnologico. Questo rapporto tecnico fornisce una panoramica delle principali azioni intraprese per la realizzazione dei servizi più importanti di informatica sanitaria nel conteso nazionale, prestando particolare attenzione ai sistemi ICT a supporto della realizzazione del Fascicolo Sanitario secondo un approccio federato e ai possibili servizi ICT che è possibile offrire in regime di telemedicina, nonché alle indicazioni europee sulla tutela della privacy. L'ampia disponibilità di standard e protocolli informatici per lo scambio e la rappresentazione dei dati sanitari, come HL7 e DICOM, e di protocolli di comunicazione, come Bluetooth e ZigBee, permette di progettare e implementare sistemi ICT per la Salute in maniera semplice ed interoperabile.

Keywords: Fascicolo Sanitario Elettronico; Telemedicina; GDPR; standard; interoperabilità.

1. Introduzione

Questo rapporto tecnico descrive le azioni più importanti intraprese in termini di normative e specifiche tecniche per l'attuazione – nel contesto nazionale – delle applicazioni più importanti nell'ambito della Salute Digitale, quali il Fascicolo Sanitario Elettronico (FSE), il taccuino personale dell'assistito e i servizi di Telemedicina. Tali applicazioni, in parte già implementate ed in altra parte in fase di completamento, permetteranno di offrire servizi a valore aggiunto agli assistiti favorendo una più efficiente erogazione di servizi sanitari. Al fine di garantire l'interoperabilità e una facile integrazione con applicativi esistenti, i sistemi ICT abilitanti alla realizzazione delle suddette applicazioni rispettano protocolli e standard di informatica sanitaria consolidati.

Il rapporto tecnico è strutturato come descritto di seguito. Il capitolo 2 descrive le principali iniziative intraprese negli ultimi anni per la realizzazione del FSE sul territorio nazionale, evidenziando in primo luogo le iniziative di natura sperimentale ed in secondo luogo le disposizioni normative emanate dalle istituzioni competenti. Il capitolo 3 illustra le linee di indirizzo sulla Telemedicina e i possibili servizi sanitari che è possibile offrire in regime di telemedicina. Nel capitolo 4 è descritto il General Data Protection Regulation (GDPR), sottolineando in particolare i principi di “privacy by design” e “privacy by default”. Il capitolo 5 è dedicato alla descrizione delle principali caratteristiche dei protocolli di comunicazione e di rappresentazione dei dati sanitari standardizzati come ad esempio HL7 e DICOM. Infine, il capitolo 6 è incentrato sulla descrizione dei principali protocolli standard di comunicazione per l'interazione tra dispositivi eterogenei come quelli utilizzati in ambito sanitario.

2. Fascicolo Sanitario Elettronico

Questo capitolo descrive le principali iniziative sperimentali per la realizzazione del FSE in Italia e le principali norme emanate dalle autorità competenti.

2.1 Iniziative sperimentali per la realizzazione del FSE

Nelle ultime due decadi, in assenza di una norma specifica e nell'ambito dell'autonomia costituzionale in materia di sanità, alcune regioni hanno attivato iniziative per la realizzazione di sistemi tecnologici di FSE, aventi per obiettivo la collezione sistematica dei documenti clinici digitali prodotti dalle proprie strutture sanitarie. L'adozione di processi differenti, lo sviluppo di modelli architetture e tecnologici eterogenei e lo stato di avanzamento disomogeneo di tali progettualità, oltre a costituire una oggettiva disparità nel garantire ai cittadini la stessa possibilità di accesso ai servizi del FSE, ha posto problemi di interoperabilità delle soluzioni già sviluppate dalle singole regioni.

Per tale motivo, nel 2004 il Dipartimento per l'Innovazione Tecnologica (DIT) della Presidenza del Consiglio dei Ministri ha istituito il Tavolo permanente per la Sanità Elettronica delle regioni e delle province autonome (TSE), al quale hanno partecipato il Ministero della Salute e le regioni e province autonome, come sede istituzionale di confronto per l'armonizzazione degli interventi e la definizione di un quadro di regole tecniche condivise per la Sanità Elettronica.

I primi risultati ottenuti dal TSE hanno riguardato la definizione, nel 2005, di una politica nazionale per la Sanità Elettronica coerente con l'Action Plan eHealth 2004 e l'elaborazione, nel 2006, di una strategia architetture di riferimento denominata Infrastruttura di Base per la Sanità Elettronica (IBSE), la quale è stata successivamente sperimentata nel progetto pilota rappresentato dal Programma Rete dei Medici di Medicina Generale e dei Pediatri di Libera Scelta (RMMG/PLS), al quale hanno partecipato le regioni.

Successivamente, nelle more di un possibile intervento normativo che regoli alcuni aspetti di fondo, il Garante per la protezione dei dati personali ha ritenuto opportuno individuare un primo quadro di cautele, al fine di delineare per tempo specifiche garanzie e responsabilità, nonché alcuni diritti, pubblicando il 16 luglio 2009 le **Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario** [1].

Al fine di fornire ulteriori indicazioni circa la corretta implementazione del FSE, il Ministero della Salute ha istituito un Tavolo interistituzionale che ha prodotto l'11 novembre 2010 un documento intitolato **Il Fascicolo Sanitario Elettronico – Linee guida nazionali** [2], approvato in Conferenza Stato-Regioni in data 10 febbraio 2011.

Inoltre, attraverso una serie di accordi stipulati tra il Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica (DDI, ex DIT) della Presidenza del Consiglio dei Ministri e il Consiglio Nazionale delle Ricerche (CNR), è stata progettata nel 2010 e implementata nel 2011 una infrastruttura tecnologica di riferimento per l'interoperabilità del FSE, denominata Infrastruttura tecnologica del Fascicolo Sanitario Elettronico (InFSE), approvata dal TSE. Tale infrastruttura è stata oggetto di due sperimentazioni per l'interscambio di documenti sanitari attraverso l'interoperabilità di sistemi prototipali di FSE delle Regioni Campania, Calabria e Piemonte nel 2012 e delle Regioni Campania, Calabria e Toscana nel 2013. Oltre a ciò, InFSE è stata utilizzata come infrastruttura tecnologica di riferimento nell'ambito del progetto nazionale Sperimentazione di un sistema per l'interoperabilità Europea e Nazionale delle soluzioni di Fascicolo Sanitario Elettronico: Componenti Patient Summary e ePrescription (IPSE) finanziato dal DDI e collegato al progetto europeo epSOS, al quale hanno partecipato il Ministero della Salute, le regioni Abruzzo, Emilia-Romagna, Friuli-Venezia Giulia, Lombardia, Molise, Sardegna, Toscana, Umbria, Veneto e la

provincia autonoma di Trento.

2.2 Normative sul FSE

Le summenzionate iniziative intraprese e i risultati raggiunti hanno rappresentato la base per la definizione di normative specifiche sul FSE.

L'articolo 12 del Decreto-Legge 18 ottobre 2012 n. 179, convertito con modificazione dalla Legge 17 dicembre 2012 n. 221, definisce il FSE e i principali requisiti da rispettare per la sua realizzazione sul territorio nazionale. In particolare, il FSE è definito come *“l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito”*. Esso è alimentato in maniera continuativa dai soggetti che prendono in cura l'assistito nell'ambito del Servizio Sanitario Nazionale (SSN) e dei servizi socio-sanitari regionali, nonché, su richiesta del cittadino, con i dati medici in possesso dello stesso. Il FSE è istituito dalle regioni e province autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali, a fini di:

- a) prevenzione, diagnosi, cura e riabilitazione;
- b) studio e ricerca scientifica in campo medico, biomedico ed epidemiologico;
- c) programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

L'alimentazione del FSE può avvenire esclusivamente sulla base del consenso libero e informato da parte dell'assistito, il quale può decidere se e quali dati relativi alla propria salute non devono essere inseriti. Invece, la consultazione del contenuto presente nel FSE, per le finalità di cui alla lettera a), può essere realizzata soltanto con il consenso dell'assistito e sempre nel rispetto del segreto professionale, salvo i casi di emergenza sanitaria. Il mancato consenso non pregiudica il diritto all'erogazione della prestazione sanitaria. Le finalità di cui alle lettere b) e c) sono perseguite dalle regioni e dalle province autonome, nonché dal Ministero del Lavoro e delle Politiche Sociali e dal Ministero della Salute nei limiti delle rispettive competenze attribuite dalla legge, senza l'utilizzo dei dati identificativi degli assistiti presenti nel FSE, secondo livelli di accesso, modalità e logiche di organizzazione ed elaborazione dei dati definiti in conformità ai principi di proporzionalità, necessità e indispensabilità nel trattamento dei dati personali. Per l'attuazione di tali disposizioni, le regioni e province autonome, possono, nel principio dell'ottimizzazione e razionalizzazione della spesa informatica, anche mediante la definizione di appositi accordi di collaborazione, realizzare infrastrutture tecnologiche per il FSE condivise a livello sovra-regionale, ovvero avvalersi, anche mediante riuso delle infrastrutture tecnologiche per il FSE a tale fine già realizzate da altre regioni o dei servizi da queste erogate.

L'articolo 17 del Decreto-Legge 21 giugno 2013 n. 69, convertito con modificazioni dalla Legge 9 agosto 2013 n. 98, ha effettuato alcune modificazioni all'articolo 12 del Decreto-Legge n. 179/2012 e ss.mm.ii. In particolare, oltre a introdurre la possibilità per le regioni e province autonome di partecipare alla definizione, realizzazione ed utilizzo dell'infrastruttura nazionale per l'interoperabilità per il FSE, resa disponibile dall'AgID, che ha inglobato nel 2012 il DDI), stabilisce le seguenti direttive:

- per favorire la qualità, il monitoraggio, l'appropriatezza nella dispensazione dei medicinali e l'aderenza alla terapia ai fini della sicurezza del paziente, è istituito il dossier farmaceutico quale parte specifica del FSE, aggiornato a cura della farmacia che effettua la dispensazione;

- entro il 31 marzo 2014, l’Agenzia per l’Italia Digitale e il Ministero della Salute, anche avvalendosi di enti pubblici di ricerca, rendono disponibili le linee guida per la presentazione dei piani di progetto regionali per la realizzazione del FSE;
- entro il 30 giugno 2014, le regioni e province autonome presentano all’Agenzia per l’Italia Digitale e al Ministero della Salute il piano di progetto per la realizzazione del FSE, redatto sulla base delle linee guida rese disponibili;
- l’Agenzia per l’Italia Digitale e il Ministero della Salute operano congiuntamente, per le parti di rispettiva competenza, al fine di:
 - a) valutare e approvare, entro sessanta giorni, i piani di progetto presentati dalle regioni e dalle province autonome per la realizzazione del FSE, condizionandone l’approvazione alla piena fruibilità dei dati regionali a livello nazionale, per indagini epidemiologiche, valutazioni statistiche, registri nazionali e raccolta di dati a fini di programmazione sanitaria nazionale;
 - b) monitorare la realizzazione del FSE, da parte delle regioni e delle province autonome, conformemente ai piani di progetto approvati;
- entro il 30 giugno 2015, le regioni e province autonome istituiscono il FSE;
- entro il 31 dicembre 2015, l’Agenzia per l’Italia Digitale, sulla base delle esigenze avanzate dalle regioni e dalle province autonome, nell’ambito dei rispettivi piani, cura, in accordo con il Ministero della Salute, con le regioni e le province autonome, la progettazione e la realizzazione dell’infrastruttura nazionale necessaria a garantire l’interoperabilità dei FSE.

Allo scopo di attuare tali indicazioni normative, l’Agenzia per l’Italia Digitale ed il Ministero della Salute hanno istituito un Tavolo di lavoro tecnico comprendente anche il CNR (in virtù di convenzioni specifiche stipulate con AgID), il CISIS e rappresentanti delle regioni e province autonome. Lo sforzo congiunto ha consentito la pubblicazione delle Linee guida per la presentazione dei piani di progetto regionali per il FSE del 31 marzo 2014 [3]. Tali linee guida, oltre a illustrare le modalità di predisposizione dei piani di progetto, forniscono una guida tecnica inerente allo sviluppo dei sistemi regionali di FSE, con particolare riguardo ai seguenti aspetti:

- modello funzionale;
- gestione del consenso e della privacy;
- modello architetturale dei sistemi di FSE;
- servizi per l’accesso al FSE da parte dell’assistito;
- servizi per il collegamento e l’abilitazione del FSE da parte dei Medici di Medicina Generale e Pediatri di Libera Scelta (MMG/PLS) e delle strutture sanitarie;
- servizi a supporto dell’interoperabilità tra i sistemi regionali di FSE;
- servizi per la gestione dei documenti sanitari.

Le linee guida hanno consentito alle regioni e province autonome di presentare, entro il 30 giugno 2014, i piani di progetto per la realizzazione del FSE.

Successivamente è stato emanato, con la qualifica di regolamento, il Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015 n. 178, attuativo dell’articolo 12 del Decreto-Legge n. 179/2012 e ss.mm.ii., che

ha disciplinato i seguenti aspetti:

- contenuti del FSE, rappresentati da un nucleo minimo di dati e documenti (dati identificativi e amministrativi dell'assistito, referti, verbali pronto soccorso, lettere di dimissione, profilo sanitario sintetico, dossier farmaceutico, consenso o diniego alla donazione degli organi e tessuti) e da ulteriori dati e documenti integrativi;
- profilo sanitario sintetico, definito come il documento socio-sanitario informatico redatto e aggiornato dal MMG/PLS, che riassume la storia clinica dell'assistito e la sua situazione corrente conosciuta;
- taccuino personale dell'assistito, definito come una sezione riservata del FSE all'interno della quale è permesso all'assistito di inserire dati e documenti personali relativi ai propri percorsi di cura, anche effettuati presso strutture al di fuori del SSN; tali dati e documenti sono informazioni non certificate dal SSN e devono essere distinguibili da quelli inseriti dai soggetti del SSN e dei servizi socio-sanitari regionali;
- gestione del consenso e delle informative;
- diritti dell'assistito inerenti all'oscuramento dei dati e documenti;
- trattamenti per finalità di cura, di ricerca e di governo;
- regole tecniche inerenti ai sistemi di codifica dei dati e ai criteri di interoperabilità del FSE;
- misure di sicurezza e sistema di conservazione;
- istituzione del Tavolo tecnico di monitoraggio e attuazione nell'ambito della Cabina di Regia del Nuovo Sistema Informativo Sanitario (NSIS);
- disposizioni transitorie, secondo le quali in sede di prima applicazione delle disposizioni del decreto, le regioni e province autonome assicurano la disponibilità di:
 - a) servizi per l'accesso dell'assistito al proprio FSE;
 - b) servizi per il collegamento e l'abilitazione all'accesso e all'alimentazione del FSE da parte dei MMG/PLS, nonché delle strutture sanitarie;
 - c) servizi a supporto dell'interoperabilità del FSE;
 - d) servizi per la gestione dei referti di laboratorio;
 - e) servizi per la gestione del profilo sanitario sintetico;
- disposizioni finali, che rimandano a ulteriori decreti per la definizione di servizi di elaborazione di dati per finalità di ricerca e di governo, l'adozione di ulteriori disposizioni relativamente ai contenuti del FSE e ai conseguenti interventi di evoluzione dell'infrastruttura nazionale per l'interoperabilità per il FSE.

Il prosieguo delle attività da parte del Tavolo tecnico ha avuto per oggetto l'elaborazione di una prima versione delle specifiche per l'interoperabilità tra i sistemi regionali di FSE da parte delle regioni Emilia-Romagna, Lombardia e Veneto e del CNR, coerenti con il Decreto del Presidente del Consiglio dei Ministri n. 178/2015. Le specifiche tecniche sono state validate attraverso un ambiente di test centrale implementato dal CNR come servizio dell'infrastruttura nazionale per l'interoperabilità nazionale per il FSE resa disponibile dall'Agenzia per l'Italia Digitale entro il 31 dicembre 2015, che ha permesso lo svolgimento di sessioni di test da parte di

11 Regioni nel 2016 [35].

L'articolo 1, comma 382 della Legge 11 dicembre 2016 n. 232 (Legge di bilancio 2017) ha apportato ulteriori modificazioni all'articolo 12 del Decreto-Legge n. 179/2012 e ss.mm.ii., stabilendo in particolare che:

- l'Agenzia per l'Italia Digitale, sulla base delle esigenze avanzate dalle regioni e dalle province autonome, nell'ambito dei rispettivi piani, cura, in accordo con il Ministero della Salute e il Ministero dell'Economia e delle Finanze e con le regioni e le province autonome, la progettazione dell'infrastruttura nazionale necessaria a garantire l'interoperabilità dei FSE, la cui realizzazione è curata dal Ministero dell'Economia e delle Finanze attraverso l'utilizzo dell'infrastruttura del Sistema Tessera Sanitaria, garantendo:
 1. l'interoperabilità dei FSE e dei dossier farmaceutici regionali;
 2. l'identificazione dell'assistito, attraverso l'allineamento con l'Anagrafe Nazionale degli Assistiti (ANA) istituita nell'ambito del Sistema Tessera Sanitaria. Nelle more della realizzazione dell'ANA, l'identificazione dell'assistito è assicurata attraverso l'allineamento con l'elenco degli assistiti gestito dal Sistema Tessera Sanitaria;
 3. per le regioni e province autonome che, entro il 31 marzo 2017, comunicano al Ministero dell'Economia e delle Finanze e al Ministero della Salute di volersi avvalere dell'infrastruttura nazionale, l'interconnessione dei soggetti per la trasmissione telematica dei dati, per la successiva alimentazione e consultazione del FSE da parte delle medesime regioni e province autonome;
 4. a partire dal 30 aprile 2017, la gestione delle codifiche nazionali e regionali, rese disponibili dalle amministrazioni ed enti che le detengono, secondo le modalità da stabilire con decreto del Ministero dell'Economia e delle Finanze, di concerto con il Ministero della Salute;
- i dati risultanti negli archivi del Sistema Tessera Sanitaria relativi alle esenzioni dell'assistito, alle prescrizioni e prestazioni erogate di farmaceutica e specialistica a carico del SSN, ai certificati di malattia telematici e alle prestazioni di assistenza protesica, termale e integrativa.

Al fine di definire le modalità tecniche per l'attuazione di quanto disposto dalle ultime indicazioni normative, è stato istituito un gruppo di lavoro nazionale composto da Agenzia per l'Italia Digitale, Ministero della Salute, Ministero dell'Economia e delle Finanze, Garante per la protezione dei dati personali, regioni e province autonome, Sogei e CNR. Il gruppo ha elaborato un documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità (INI) dei FSE, che definisce le specifiche sul modello architetturale, le funzionalità, i servizi ed i processi dell'infrastruttura nazionale al fine di offrire una visione d'insieme delle modalità in cui i sistemi regionali di FSE interagiscono tra loro, nonché il dettaglio delle funzionalità messe a disposizione dall'INI alle regioni e province autonome che decidono di avvalersene. Tale documento, intitolato "Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12 – comma 15-ter – D.L. 179/2012)", è stato pubblicato nella Circolare AgID n. 4/2017 del 1° agosto 2017 [4].

Il documento progettuale dell'infrastruttura nazionale per l'interoperabilità dei FSE ha stabilito i requisiti di base del Decreto 4 agosto 2017 del Ministero dell'Economia e delle Finanze di concerto con il Ministero della Salute, attuativo dell'articolo 1, comma 382, della Legge n. 232/2016, che disciplina:

- a) le funzioni e i servizi telematici dell'INI;
- b) i procedimenti nonché le modalità con le quali l'INI garantisce, per le regioni e province autonome che comunicano al Ministero dell'Economia e delle Finanze e al Ministero della Salute di volersi

avvalere della medesima infrastruttura nazionale, l'interconnessione dei soggetti per la trasmissione telematica dei dati contenuti nei FSE degli assistiti ai fini della successiva alimentazione e consultazione dei medesimi FSE da parte delle medesime regioni e province autonome;

c) le funzioni e i servizi telematici dell'INI, al fine di garantire ai FSE i dati del Sistema Tessera Sanitaria.

Successivamente, è stata pubblicata la nuova versione delle specifiche tecniche per l'interoperabilità tra i sistemi regionali di FSE [5], in coerenza con quanto stabilito dal Decreto, che stabiliscono le modalità da adottare per l'interoperabilità dei sistemi regionali di FSE con l'INI al fine di collezionare, richiedere e trasmettere dati e documenti sanitari attraverso approcci sicuri e nel rispetto dei consensi stabiliti dagli assistiti. In particolare, nell'ambito dei diversi processi interregionali, ciascuna regione o provincia autonoma può assumere i seguenti ruoli:

- *Regione Di Assistenza (RDA)*: ha l'onere di memorizzare, e di rendere disponibili agli attori autorizzati, tutti i riferimenti (metadati) ai documenti e dati generati per i propri assistiti, anche se prodotti in altri domini regionali.
- *Regione Di Erogazione (RDE)*: eroga una prestazione sanitaria ad un paziente assistito da un altro dominio regionale.
- *Regione Contenente un Documento o dato (RCD)*: rappresenta il dominio regionale in cui è disponibile un documento o dato sanitario o socio-sanitario che si intende consultare.
- *Regione Precedente Di Assistenza (RPDA)*: è un dominio regionale che, precedentemente al cambio della regione o provincia autonoma di assistenza da parte di un assistito, ha svolto per questi il ruolo di RDA.

Il modello architetturale per l'interoperabilità nazionale del FSE è mostrato nella figura successiva.

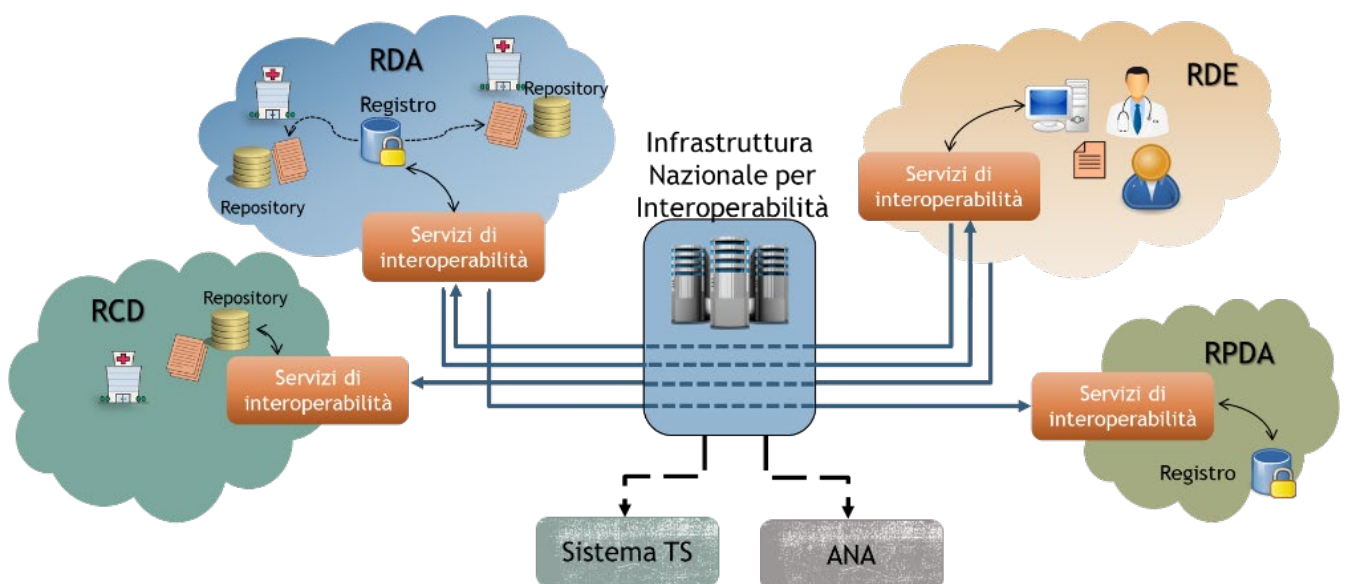


Figura 1. Modello architetturale per l'interoperabilità nazionale del FSE [fonte www.fascicolosanitario.gov.it]

I servizi di interoperabilità che ogni sistema di FSE deve esporre sono conformi a standard internazionali localizzati in ambito nazionale, con particolare riferimento a IHE XDS.b, HL7 CDA Rel. 2.0, ICD9-CM,

LOINC, ATC e AIC. L'uso dei servizi di interoperabilità, descritti sinteticamente di seguito, è veicolato tramite l'INI, che permette la comunicazione tra più domini regionali:

- *Ricerca dei documenti*: consente la consultazione dell'elenco dei documenti presenti nel FSE di un assistito.
- *Recupero di un documento*: permette la consultazione di uno specifico documento presente nel FSE di un assistito.
- *Comunicazione dei metadati*: consente ad un dominio regionale di informare la RDA di una avvenuta creazione di un documento per un assistito di quest'ultima, trasmettendo una serie di metadati associati al documento.
- *Cancellazione dei metadati*: consente ad un dominio regionale di richiedere la cancellazione dei metadati associati ad uno specifico documento nel FSE.
- *Trasferimento dell'indice del FSE*: consente alla RPDA di trasferire alla nuova RDA l'insieme dei riferimenti dei documenti del FSE e delle politiche di accesso ad essi associati.
- *Gestione dei consensi e delle informative*: consente ad un dominio regionale di comunicare le informative regionali e i consensi raccolti all'INI.
- *Gestione delle notifiche*: consente all'INI di notificare alla RDA eventi occorsi a propri assistiti in domini regionali differenti.

I gruppi di lavoro tecnici dedicati hanno fornito ulteriori indicazioni tecniche, inerenti in particolare alle modalità di accesso al FSE, gestione del consenso, gestione delle codifiche, strutturazione dei documenti clinici, firma digitale dei documenti, comunicazione.

Infine, il Decreto del 25 ottobre 2018 "Modifica del decreto ministeriale 4 agosto 2017, concernente le modalità tecniche e i servizi telematici resi disponibili dall'infrastruttura nazionale per l'interoperabilità del Fascicolo sanitario elettronico (FSE)" ha modificato l'articolo 3, comma 1, dove viene aggiunta la lettera f) "servizi on-line per l'assistito volti a garantire l'interoperabilità dei FSE e dei dossier farmaceutici regionali", che permette ad INI di erogare servizi on-line agli assistiti che hanno precedentemente espresso il consenso all'alimentazione del proprio FSE in caso di cambio di assistenza e per i quali non risulta associata una Regione di Assistenza (RDA) o nel caso la nuova RDA non sia operativa, al fine di assicurare la continuità di servizio (art.11, comma 2).

Inoltre, le modifiche al citato Decreto introducono la possibilità per l'assistito di accedere al proprio FSE anche attraverso un accesso unico nazionale, mediante il portale www.fascicolosanitario.gov.it e i servizi messi a disposizione da INI.

3. Telemedicina – Linee di Indirizzo

Questa sezione descrive le linee di indirizzo nazionali sulla Telemedicina emanate dal Consiglio Superiore di Sanità, tali linee guida rappresentano un modello di governance condivisa per le iniziative in settore della Telemedicina nel contesto nazionale.

Nella seduta del 10 luglio 2012 l'Assemblea generale del Consiglio Superiore di Sanità ha approvato le Linee

di indirizzo nazionali sulla Telemedicina [6], con l'obiettivo di disporre di un modello di governance condivisa delle iniziative di Telemedicina a fronte di una diffusione non organica di servizi sanitari erogati con tale modalità nell'ambito di iniziative che troppo spesso si sono ricondotte a sperimentazioni, prototipi, progetti, caratterizzati da casistica limitata e elevata mortalità dell'iniziativa stessa.

Lo sviluppo di strumenti per la Telemedicina consente sia di trovare nuove risposte a problemi tradizionali della medicina, sia di creare nuove opportunità per il miglioramento del servizio sanitario tramite una maggiore collaborazione tra i vari professionisti sanitari coinvolti e i pazienti.

Le Linee di indirizzo elaborate definiscono la Telemedicina come “una modalità di erogazione di servizi di assistenza sanitaria, tramite il ricorso a tecnologie innovative, in particolare alle Information and Communication Technologies (ICT), in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località”. Le finalità sanitarie dei servizi offerti in regime di Telemedicina riguardano: prevenzione secondaria, diagnosi, cura, riabilitazione, monitoraggio.

Le Linee di indirizzo individuano, come principali benefici attesi dall'adozione di tali strumenti, un'equità di accesso all'assistenza sanitaria, una migliore qualità dell'assistenza garantendo la continuità delle cure, una migliore efficacia, efficienza, appropriatezza dei servizi sanitari, un importante contributo all'economia.

Gli ambiti di intervento identificati sono i seguenti:

- Continuità delle cure e integrazione Ospedale – Territorio.
- Patologie rilevanti.
- Sistema dell'Emergenza Urgenza.
- Riorganizzazione della diagnostica di laboratorio e diagnostica per immagini.

I servizi sanitari offerti in regime di Telemedicina possono essere classificati nelle seguenti categorie:

- *Telemedicina specialistica*: comprende le modalità descritte di seguito con cui si forniscono servizi medici a distanza all'interno di una specifica disciplina medica:
 - *Televisita*: è un atto sanitario in cui il medico interagisce a distanza con il paziente. L'atto sanitario di diagnosi che scaturisce dalla visita può dar luogo alla prescrizione di farmaci o di cure. Durante la Televisita un operatore sanitario che si trovi vicino al paziente, può assistere il medico. Il collegamento deve consentire di vedere e interagire con il paziente e deve avvenire in tempo reale o differito.
 - *Teleconsulto*: è un'indicazione di diagnosi e/o di scelta di una terapia senza la presenza fisica del paziente. Si tratta di un'attività di consulenza a distanza fra medici che permette a un medico di chiedere il consiglio di uno o più medici, in ragione di specifica formazione e competenza, sulla base di informazioni mediche legate alla presa in carico del paziente.
 - *Telecooperazione sanitaria*: è un atto consistente nell'assistenza fornita da un medico o altro operatore sanitario ad un altro medico o altro operatore sanitario impegnato in un atto sanitario. Il termine viene anche utilizzato per la consulenza fornita a quanti prestano un soccorso d'urgenza.
- *Telesalute*: riguarda i sistemi e i servizi che collegano i pazienti, in particolar modo i cronici, con i medici per assistere nella diagnosi, monitoraggio, gestione, responsabilizzazione degli stessi. Permette a un medico (spesso un medico di medicina generale in collaborazione con uno specialista) di interpretare a distanza i dati necessari al Telemonitoraggio di un paziente, e, in quel caso, alla presa in carico del paziente stesso.

- *Teleassistenza*: si intende un sistema socio-assistenziale per la presa in carico della persona anziana o fragile a domicilio, tramite la gestione di allarmi, di attivazione dei servizi di emergenza, di chiamate di “supporto” da parte di un centro servizi.

Da un punto di vista architettuale, gli attori coinvolti in un atto sanitario prestato in Telemedicina sono i seguenti:

- Utenti: pazienti/caregiver o medici che, dopo aver trasmesso delle informazioni sanitarie (dati, segnali, immagini, ecc.), ricevono gli esiti di un servizio di Telemedicina (diagnosi, indirizzi terapeutici).
- Centro Erogatore: strutture o operatori del SSN che ricevono le informazioni sanitarie dall’utente e trasmettono a quest’ultimo gli esiti della prestazione.
- Centro Servizi: struttura che ha le funzioni di gestione e manutenzione di un sistema informativo, attraverso il quale il Centro Erogatore svolge la prestazione in Telemedicina, la installazione e manutenzione degli strumenti nei siti remoti, la fornitura, gestione e manutenzione dei mezzi di comunicazione tra pazienti e medici o altri operatori sanitari, l’addestramento di pazienti e familiari all’uso degli strumenti. Nel caso in cui non sia presente un Centro Servizi, le funzioni del Centro Servizi devono essere assolate dal Centro Erogatore.

Infine, le componenti tecnologiche necessarie per l’integrazione dei soggetti coinvolti nell’erogazione e nella fruizione di servizi di Telemedicina sono le seguenti:

- infrastrutture di telecomunicazione: riguardano le tecnologie per la trasmissione dei dati e della comunicazione tra Utente, Centro Erogatore, ed eventualmente Centro Servizi;
- interfacce: rappresentano tutti i sistemi idonei a garantire la connessione e l’accesso dell’Utente, del Centro Erogatore e del Centro Servizi alla rete di servizi di Telemedicina (apparati biomedicali, sistemi hardware/software, applicazioni web, portali, ecc.).

La figura successiva mostra i principali modelli organizzativi individuati dalle Linee di indirizzo, sulla base delle figure professionali, ossia paziente/caregiver (P in figura) e medico o altro operatore sanitario (M in figura), degli attori, ossia Utente, Centro Servizi (CS in figura) e Centro Erogatore, e del tipo di interazione, ossia B2B (relazione tra medici), B2B2C (relazione tra un medico ed un paziente attraverso un operatore sanitario), B2C (relazione tra medico e paziente). Gli attori espongono interfacce (I in figura) che interagiscono tra di loro attraverso infrastrutture di telecomunicazione.

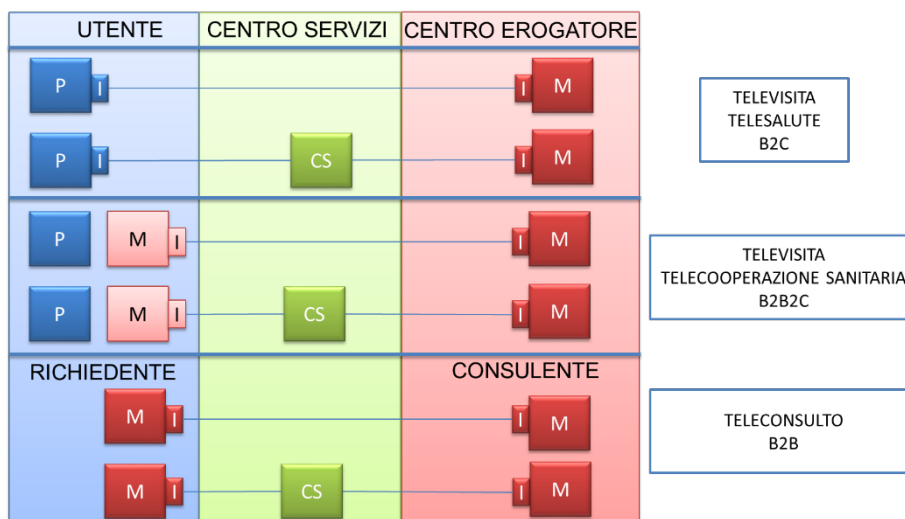


Figura 2. Modelli organizzativi per l'erogazione dei servizi di telemedicina

4. Regolamento Europeo GDPR

Questa sezione descrive i principi di “privacy by design” e “privacy by default” introdotti dal GDPR, indispensabili in particolare nel contesto della sanità elettronica. Molti degli attuali sistemi informativi sanitari sono stati infatti aggiornati per rispondere a quelli che sono i nuovi requisiti previsti dal regolamento europeo.

Il raggiungimento dell’obiettivo del progetto inerente la realizzazione di una piattaforma di taccuino personale capace di collezionare dati eterogenei relativi agli assistiti, che contengono per definizione dati sensibili, richiede che i modelli, le tecniche e i servizi progettati siano conformi alle normative vigenti sulla tutela della privacy.

In particolare, in questo paragrafo si farà esplicito riferimento al GDPR [7], ovvero il Regolamento UE n. 679/2016 sulla protezione dei dati personali, riportando sinteticamente le informazioni salienti, mentre una trattazione dettagliata sarà oggetto dell’Obiettivo Realizzativo 5 “Trasmissione sicura di dati sensibili”.

Il Regolamento è entrato in vigore il 24 maggio 2016 ma sarà applicabile operativamente dal 25 maggio 2018, abrogando la Direttiva 95/46/CE.

L’obiettivo del GDPR è quello di proteggere tutti i cittadini dell’UE dalle violazioni dei dati, alla luce di un contesto internazionale sempre più guidato dai dati e quindi molto diverso dal tempo in cui è stata stabilita la Direttiva del 1995. Sebbene i principi chiave della privacy dei dati siano ancora fedeli alla direttiva precedente, sono state proposte molte modifiche alle politiche di regolamentazione.

Una delle novità principali introdotte dal GDPR riguarda l’applicabilità a tutte le società che trattano i dati personali degli interessati residenti nell’Unione Europea, indipendentemente dalla sede della società. Il GDPR si applicherà anche al trattamento dei dati personali delle persone nell’UE da parte di un responsabile o incaricato del trattamento al di fuori dell’UE, dove le attività riguardano l’offerta di beni o servizi ai cittadini dell’UE e il monitoraggio dei comportamenti che si svolgono all’interno dell’UE.

Le condizioni per la manifestazione del consenso sono state rafforzate e le aziende non potranno più utilizzare termini e condizioni poco chiare, ma l’informativa deve essere fornita in forma intelligibile e facilmente accessibile.

Le organizzazioni in violazione del GDPR (ad es. per una elaborazione dei dati in assenza del consenso da parte dell’interessato) possono essere sanzionate fino al 4% del fatturato globale annuale o a 20 milioni di

euro.

Tra i diritti estesi alle persone interessate dal GDPR, vi è la possibilità per un soggetto di ottenere dal titolare del trattamento la conferma dell'esistenza o meno di dati personali che lo riguardano, dove sono ubicati e per quale scopo. Il responsabile del trattamento deve fornire una copia dei dati personali, a titolo gratuito, in formato elettronico.

Un altro diritto è il cosiddetto "diritto all'oblio", il quale autorizza l'interessato a richiedere al responsabile del trattamento di cancellare i suoi dati personali, cessare la diffusione dei dati e potenzialmente impedire a terzi di elaborare i dati.

L'interessato ha anche il diritto di ricevere i dati personali che lo riguardano, precedentemente forniti in un formato comunemente utilizzabile e machine-readable, e ha il diritto di trasmettere tali dati ad un altro responsabile.

Attualmente, i responsabili sono tenuti a notificare le loro attività di elaborazione dei dati con DPA (Data Protection Act) locali, che, per le multinazionali, rappresentano un notevole ostacolo burocratico, in quanto la maggior parte degli Stati Membri ha requisiti di notifica diversi. Ai sensi del GDPR, invece, ci saranno requisiti interni per l'archiviazione dei dati e l'incarico per la DPO sarà obbligatorio solo per quei responsabili e incaricati le cui attività principali consistono in operazioni di elaborazione che richiedono un monitoraggio regolare e sistematico degli interessati su larga scala o di speciali categorie di dati o dati relativi a condanne e reati penali.

Infine, si segnalano due concetti fondamentali disciplinati nel GDPR: privacy by design e privacy by default. Il principio del privacy by design afferma che qualsiasi azione intrapresa da una società che implichi il trattamento di dati personali deve essere effettuata tenendo conto della protezione dei dati e della privacy in ogni fase, con riferimento anche a progetti interni, sviluppo di prodotti, sviluppo di software, sistemi IT etc. In pratica, una struttura o una divisione che elabora dati personali deve garantire che la privacy sia integrata in un sistema durante l'intero ciclo di vita del sistema o del processo.

Il principio del privacy by default significa che una volta che un prodotto o un servizio è stato rilasciato, devono essere applicate per impostazione predefinita le impostazioni di privacy più severe, senza alcuna immissione manuale da parte dell'utente finale. Inoltre, i dati personali forniti dall'utente devono essere conservati solo per il tempo necessario a fornire il prodotto o il servizio.

5. Protocolli e standard per lo scambio dati in ambito sanitario

Questa sezione descrive le principali caratteristiche dei protocolli di comunicazione e di rappresentazione dei dati standardizzati da organismi internazionali che sviluppano standard di informatica sanitaria più diffusi sul territorio nazionale [8], con particolare riferimento a HL7, DICOM, IHE profilo XDS, Personal Connected Health Alliance.

5.1 HL7

Health Level Seven (HL7) è uno dei standard per la comunicazione di messaggi più diffusi al mondo nel settore della Sanità Elettronica sviluppato dall'associazione HL7 International [9]. Lo standard fu inizialmente definito nel 1987 per l'uso nel sistema sanitario degli Stati Uniti ma al giorno d'oggi lo sviluppo di HL7 coinvolge l'intera comunità internazionale. HL7 coordina gli sforzi con altri organismi internazionali di

standardizzazione (CEN/TC 251, DICOM, ISO/TC 215, W3C). In parallelo con queste collaborazioni formali, HL7 incoraggia la formazione di sezioni nazionali (“affiliates”) in tutto il mondo. Lo standard viene sviluppato con risorse offerte volontariamente da numerose organizzazioni (industrie, agenzie governative, organizzazioni che forniscono o rimborsano l’assistenza, ecc).

La sezione italiana di HL7 [10] è stata costituita il 20 marzo 2003, con l’obiettivo di adattare lo standard alle necessità nazionali, all’interno delle regole generali stabilite da HL7 e in collaborazione con l’UNI, Ente Italiano di Unificazione.

Il termine “Level 7” fa riferimento al livello più alto del modello ISO OSI, al fine di enfatizzare il concetto di una interfaccia di tipo paritario (applicazione-applicazione) posta al settimo livello del modello: HL7 fa riferimento ai dati scambiati, alla tempistica degli scambi, e alla comunicazione di errori fra le applicazioni.

Lo standard di messaggistica non presuppone nessuna particolare architettura né una particolare collocazione del dato rispetto all’applicativo ed è conforme alle necessità sia di un sistema di gestione centralizzato che di un sistema distribuito. I principali scopi dello standard sono descritti di seguito:

- supportare gli scambi informativi fra sistemi implementati con una qualsiasi tecnologia;
- supportare lo scambio dei dati di singole transazioni o di un insieme di transazioni raggruppate in file;
- permettere la presenza di variazioni locali alle singole organizzazioni pur mantenendo un elevato grado di standardizzazione;
- favorire l’evoluzione graduale in base al mutare delle esigenze;
- garantire la conformità agli altri standard presenti in ambito sanitario.

Nel corso degli anni lo standard si è evoluto attraverso una serie di versioni, ed attualmente coesistono la versione 2, giunta alla ottava revisione, la versione 3, nata per superare le limitazioni della versione precedente, e infine FHIR, formalizzato per facilitare l’implementazione di applicazioni sanitarie in maniera più immediata e semplice.

HL7 versione 2

La versione 2 dello standard HL7 (HL7 V2) [11], la cui prima apparizione risale al 1988 e la cui approvazione presso l’ANSI risale al 1997, ha riscosso un ampio successo ed è attualmente implementato in un ampio numero di organizzazioni del mondo dell’healthcare. Lo standard definisce le regole di codifica, la struttura e i tipi di dato ammissibili per la costruzione di messaggi per lo scambio di informazioni in formato elettronico nel mondo sanitario.

Le prime versioni prevedevano di strutturare un messaggio in segmenti posti in un preciso ordine e separati dal simbolo “[”, contenenti a loro volta gruppi di campi. Le versioni più recenti sono invece basate su schemi XML.

In generale è possibile riassumere i vantaggi dello standard HL7 V2 per l’interfacciamento dei sistemi informativi sanitari:

- standard de facto: HL7 V2 è uno standard diffuso a livello internazionale e largamente utilizzato;
- stabile: dopo circa 20 anni di sviluppo e diverse revisioni, nonché naturalmente il largo utilizzo quotidiano, lo standard ha raggiunto una piena maturità evolutiva;

- retro compatibile: le versioni 2.x sono sempre compatibili con le precedenti, anche se naturalmente queste ultime saranno limitate nell'utilizzo delle nuove funzionalità introdotte dalle versioni successive;
- molteplici implementazioni: molte aziende hanno realizzato framework di sviluppo per il supporto a HL7 V2; ne segue che il mercato creatosi è altamente concorrenziale e sostanzialmente affidabile, a tutto vantaggio dei clienti che devono espandere l'interoperabilità del proprio sistema informativo;
- semplice: basandosi su pochi elementi normativi, l'intero protocollo è relativamente semplice da studiare ed implementare;
- flessibile: i messaggi contengono molti elementi opzionali che permettono di adattarsi alle necessità e disponibilità delle entità che li utilizzano, semplicemente concordando quali informazioni condividere;
- costo relativamente basso: per tutte le ragioni precedentemente elencate il costo di utilizzo dello standard HL7 V2 per l'interfacciamento dei sistemi può essere realizzato attraverso una spesa limitata.

D'altra parte però, nel corso degli anni di utilizzo dello standard, sono stati riscontrati alcuni difetti congeniti nella definizione del protocollo:

- pensato principalmente per la sanità americana: sono di conseguenza poco curati tutti gli ambiti che negli USA rivestono un interesse secondario, come per esempio gli aspetti relativi all'assistenza sanitaria primaria e la pubblica sanità, che invece sono particolarmente importanti nel contesto europeo;
- ambiguo: non esistendo una definizione formale e condivisa dei concetti, questi ultimi possono risultare ambigui e non ben definiti; ne seguono difficoltà implementative e la presenza inaspettata di errori semantici, particolarmente critici nel settore sanitario;
- interoperabilità limitata: a causa della semantica non condivisa, HL7 V2 non offre una soluzione universale per l'interoperabilità, in quanto necessita di accordi bilaterali affinché i messaggi siano ben definiti; di conseguenza ogni implementazione è in generale legata a due uniche entità e non all'intero universo degli enti che si interfacciano attraverso lo standard HL7 V2 e questo limita l'utilità ed il vantaggio della sua utilizzazione;
- troppo flessibile: il gran numero di elementi opzionali tende a rendere l'implementazione del protocollo ed in generale l'integrazione dei sistemi più complessa, in quanto costringe le due entità ad una prolungata e profonda analisi delle rispettive necessità;
- destinato a non essere più supportato: nonostante le versioni di HL7 V2 siano mantenute ed evolute, lo sviluppo dello standard è destinato a bloccarsi, in quanto si prevede che sarà rimpiazzato dalle versioni successive;
- standard obsoleto: dopo circa 20 anni il settore dell'ICT è notevolmente cambiato, mentre HL7 V2 poggia sulle stesse basi delle prime versioni; la sicurezza, la privacy e XML sono temi adattati successivamente, con i problemi e le difficoltà che ne conseguono;
- difficoltà sulle certificazioni: non esiste una procedura ufficiale per verificare la compatibilità di un sistema informativo allo standard HL7 V2; inoltre la presenza di molti elementi opzionali rende difficile la stipulazione di contratti efficaci.

In definitiva, la versione 2 di HL7 è sicuramente la più implementata, ma ciò non la rende immune da critiche o da limiti. Lo standard non definisce infatti delle linee guida formalizzate per la costruzione dei messaggi,

molti dettagli tecnici sono spesso descritti in linguaggio naturale e le relazioni tra i campi non sono chiare perché si focalizza l'attenzione sulla struttura sintattica del messaggio, senza esplicitare le relazioni semantiche tra le informazioni contenute. I segmenti sono inoltre riusati in più messaggi e i messaggi riusati in più eventi trigger, imponendo l'utilizzo di campi opzionali per soddisfare il largo riuso. Mentre l'opzionalità ha il vantaggio di dare più libertà ad un messaggio, rendendolo utilizzabile in più contesti, rende difficile stabilire le specifiche delle interfacce dello standard, causando incomprensioni tra fornitore e acquirenti. Troppi campi opzionali e non formalizzati hanno in conclusione portato ad una libera interpretazione delle informazioni presenti nei messaggi dello standard.

HL7 versione 3

La versione 3 dello standard HL7 (HL7 V3) [12] apporta un radicale cambiamento nel processo di sviluppo delle specifiche, formalizzando una metodologia che nelle versioni precedenti era ambigua. Le novità di rilievo introdotte dalla versione 3 sono le seguenti:

- adotta un approccio Object-Oriented per il processo di sviluppo, basandosi sullo standard Unified Modeling Language (UML). Questo cambiamento aumenta il dettaglio, la chiarezza e la precisione delle specifiche, favorendo sia gli attori che presiedono lo sviluppo dello standard, sia gli sviluppatori;
- riduce le opzionalità presenti nelle versioni precedenti;
- rende verificabile la conformità allo standard definendo gli "application role", che sono le responsabilità che deve avere una applicazione nei confronti degli event trigger gestiti;
- svincola le specifiche dalla tecnologia di serializzazione, definendo in modo astratto le strutture dei messaggi.

Una novità fondamentale dello standard HL7 V3 è rappresentata dalla definizione di un modello informativo esplicito e condiviso, il Reference Information Model (RIM), insieme ad una metodologia per derivare da esso le strutture dei messaggi attraverso un processo di raffinazione. La struttura fondamentale del RIM è riportata nella figura successiva.

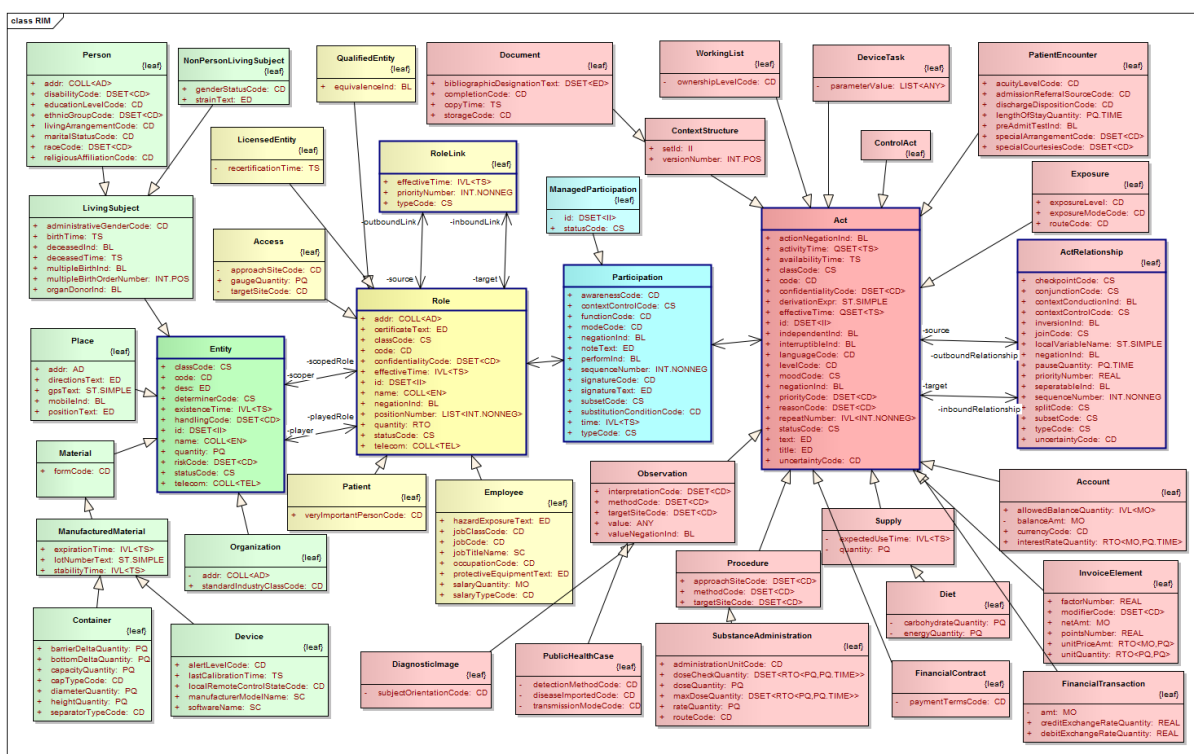


Figura 3. HL7 V3 REFERENCE INFORMATION MODEL

Il RIM è composto da un insieme di 6 classi “backbone” o “core”, descritte di seguito:

- *Act*: rappresenta un’azione che viene eseguita e deve essere documentata (in rosso in figura).
- *Participation*: definisce il contesto di una azione, nei termini di chi la esegue, chi la subisce ed il motivo per cui viene eseguita (in blu in figura).
- *Entity*: definisce un oggetto fisico o una persona che prende parte al processo descritto (in verde in figura).
- *Role*: stabilisce il ruolo che le entità ricoprono nel processo (in giallo in figura).
- *ActRelationship*: rappresenta un legame tra azioni, come ad esempio il legame tra l’ordine di esecuzione di un esame e l’esecuzione stessa (in rosso chiaro in figura).
- *RoleLink*: definisce una relazione tra ruoli diversi (in giallo chiaro in figura).

Una classe è un’astrazione di cose o concetti che sono soggetti di interesse di un dato dominio applicativo; tutte le cose o i concetti che possono essere associati ad una classe hanno le stesse proprietà e sono soggetti e conformi alle stesse regole. Le classi sono persone, luoghi, ruoli, cose ed eventi riguardo i quali sono tenute le informazioni; esse sono definite da un nome, una descrizione, un insieme di attributi, relazioni e stati. Le classi sono correlate ad altre classi in varie relazioni. Le istanze delle classi sono chiamate oggetti.

Il processo HL7 di modellamento delle informazioni per lo sviluppo di applicazioni ICT nel settore della sanità si basa su diversi tipi di modelli informativi correlati tra loro; ogni tipo di modello usa la stessa notazione e la stessa struttura base. I modelli differiscono gli uni dagli altri per quanto riguarda il loro contenuto di informazione, l’estensione e l’uso per il quale sono progettati. Sono definiti i seguenti tipi di modelli di informazione:

- *Domain Message Information Model (D-MIM)*: è un sottoinsieme rifinito del RIM che include un set di classi clone, attributi e relazioni che possono essere usati per creare messaggi per un particolare dominio. Il D-MIM è usato come una base comune sopra la quale sono creati tutti i R-MIM all'interno del dominio.
- *Refined Message Information Model (R-MIM)*: rappresenta vincoli sui modelli D-MIM contenente solo le classi, gli attributi e le associazioni richieste per comporre uno specifico insieme di messaggi.
- *Hierarchical Message Description (HMD)*: consiste in una struttura astratta che rappresenta un messaggio che può essere scambiato tra sistemi.
- *Implementation Technology Specification (ITS)*: definisce le modalità di rappresentazione degli oggetti per la trasmissione dei messaggi.

In definitiva, lo standard HL7 V3 definisce, attraverso il RIM ed un processo di sviluppo formale, una rappresentazione concettuale delle principali entità relative al dominio sanitario e le modalità per formalizzare i contenuti che devono essere scambiati tra diversi sistemi. Questo approccio di tipo top-down, tuttavia, seppur superando i limiti presenti nello standard HL7 V2, non è stato estensivamente utilizzato in ambito internazionale, per i seguenti principali motivi:

- il processo richiesto per lo sviluppo di applicazioni è troppo complesso e laborioso;
- i molteplici diagrammi di modellazione da sviluppare richiedono competenze specifiche non sempre disponibili.

Per tali ragioni, unitamente alla caratteristica di non retro-compatibilità dello standard HL7 V3, la maggior parte dei domini sanitari ha continuato ad utilizzare lo standard HL7 V2 per lo scambio dei messaggi tra sistemi differenti.

5.1.1 HL7 CDA

Clinical Document Architecture (CDA) [13] è uno standard prodotto dall'associazione HL7 che ha riscosso un successo notevole per la strutturazione dei dati all'interno dei documenti clinici.

La prima versione di CDA è stata prodotta nel 2000, ma la versione diffusamente utilizzata è la Release 2, che è stata elaborata a partire dal RIM di HL7 V3. CDA definisce l'architettura di un documento clinico, che rappresenta una forma di gerarchia ordinata di tipo albero in cui tutti gli elementi hanno tra di loro una relazione del tipo genitore-figlio. L'unica specifica implementativa pubblicata è basata sul linguaggio XML.

CDA organizza i documenti clinici in due sezioni: l'header, che contiene un insieme di dati atti a descrivere informazioni di contesto, quali ad es. il nome dell'autore, il nome del paziente, la struttura sanitaria dove è stato prodotto il documento, ecc.; il body, che contiene i contenuti clinici veri e propri.

Le specifiche CDA definiscono un'architettura multilivello, dove ogni livello deriva da un livello più basso. In particolare, esistono tre possibili livelli di astrazione, che specificano il grado di granularità del markup richiesto e non fanno riferimento alla granularità del contenuto:

- Il livello 1 rappresenta la radice della gerarchia e fornisce le specifiche più generali del documento.
- Il livello 2 definisce un insieme di vincoli sulla struttura e sulla semantica del documento basata sui template HL7.

- Il livello 3 aggiunge markup addizionale al documento che consente di esprimere formalmente il contenuto clinico.

Considerato che CDA definisce l'architettura di un documento generico, per ciascuna tipologia di documento clinico che si intende strutturare occorre definire preliminarmente guide implementative che, declinando lo standard al caso specifico, specificano come organizzare i contenuti inerenti. Ogni associazione nazionale affiliata a HL7 International ha il compito di definire le guide implementative per le tipologie di documenti sanitari utilizzate nel territorio nazionale.

5.1.2 HL7 FHIR

Fast, Healthcare, Interoperability, Resources (FHIR) [14,34] è uno standard realizzato per consentire lo scambio di informazioni sanitarie attraverso sistemi informativi differenti, nato con l'obiettivo di superare i limiti degli standard HL7 V2 e V3. La necessità di realizzare velocemente l'integrazione tra sistemi e processi, nonché prevedere l'uso di applicazioni mobile e cloud ha infatti richiesto l'aggiornamento degli standard.

FHIR come indica l'acronimo è veloce da realizzare (Fast), progettato per il dominio della sanità (Healthcare), garantisce l'interoperabilità (Interoperability), definisce risorse (Resources):

- Fast: l'apprendimento risulta facile per gli sviluppatori. Sono presenti molti strumenti ed esempi, inoltre sono fornite librerie software a disposizione dello sviluppatore.
- Healthcare: il dominio di utilizzo è la sanità.
- Interoperability: l'interoperabilità è facilitare l'interazione fra sistemi differenti e standard differenti, permettendo a sistemi informativi non omogenei lo scambio di informazioni.
- Resources: le risorse rappresentano un insieme di componenti informative modulari.

La necessità della dematerializzazione comporta che i dati sanitari vengono digitalizzati e gestiti esclusivamente attraverso sistemi telematici; ad es., la visita di un paziente genera una notevole quantità di dati, ma allo stesso tempo necessita di una serie di informazioni che dovranno necessariamente rispondere a tre concetti chiave:

- Disponibilità: i dati devono essere sempre usabili.
- Rilevabilità: i dati dovranno essere sempre accessibili.
- Comprensibilità: i dati dovranno essere sempre consistenti.

La struttura base in FHIR è la risorsa, che rappresenta una entità unicamente identificabile e contiene dati strutturati standardizzati. Lo standard ha già definito numerose risorse che possono essere utilizzate per rappresentare e scambiare dati sanitari. I formati adottati per la rappresentazione delle risorse sono XML e JSON.

Le risorse sono combinate e personalizzate, per soddisfare le esigenze specifiche dei casi d'uso, come risolvere problemi clinici e amministrativi. Lo scopo di FHIR è la costruzione di un set base di risorse che, da sole o in modo aggregato, consentano di soddisfare la maggior parte dei casi d'uso in ambito sanitario. Tali risorse possono essere utilizzate per definire la struttura e i contenuti informativi di molte applicazioni comuni; inoltre, è prevista la possibilità di generare estensioni in modo da garantire una sufficiente copertura anche per i casi limite non ancora contemplati.

FHIR utilizza un approccio per composizione, a differenza dei precedenti standard HL7 basati su un approccio per costruzione. La possibilità di costruire documenti sanitari e strutture dati mediante FHIR è resa possibile dalla combinazione delle risorse messe a disposizione.

L'utilizzo di FHIR copre vari ambiti: lo scambio dei messaggi tra sistemi, la gestione di sistemi informativi sanitari, l'uso del cloud, i social media, le applicazioni mobile, ecc. FHIR utilizza le nuove tecnologie web, basate sul modello Resource-Oriented Architecture (ROA).

FHIR si pone come obiettivo la semplificazione dei processi di gestione dei dati sanitari, senza sacrificare l'integrità delle informazioni trattate. Per rendere concreto questo scopo, esso fa riferimento a modelli logico-teorici esistenti per fornire meccanismi coerenti, facili da implementare e che restituiscano il giusto grado di rigore nelle operazioni di trasporto delle informazioni tra le applicazioni sanitarie.

Tutte le risorse in FHIR condividono uno stesso set di caratteristiche:

- un modo per definirle, rappresentarle e ricostruirle;
- un insieme di metadati;
- una parte leggibile da un utente osservatore.

Lo standard FHIR contempla due risorse utilizzabili per descrivere come le risorse sono definite ed utilizzate dal sistema in esercizio:

- *Conformance Statement*: descrive le interfacce esposte dal sistema, è utilizzato per conoscere le funzionalità e le condizioni tecniche di utilizzo dell'implementazione software.
- *StructureDefinition*: fornisce una serie di regole utili a vincolare gli elementi opzionali, la cardinalità, le terminologie, i tipi primitivi e le estensioni nelle risorse utilizzate dall'implementazione software.

La definizione di risorse informative basate su strutture dati semplici, formali, facilmente reperibili e aderenti alle ultime tecnologie, nonché la disponibilità di API open source, rendono lo standard facilmente implementabile. Pertanto, FHIR ha catturato notevolmente l'attenzione dei principali decision-makers e vendors, lasciando presagire un'ampia diffusione in ambito internazionale.

5.1.3 Ulteriori standard HL7

Negli ultimi anni, HL7 ha prodotto numerosi standard non orientati alla messaggistica, ma focalizzati sulla definizione di specifiche inerenti a problemi e domini specifici del settore IT Sanità. Non è obiettivo di questo documento trattare tutti i molteplici standard prodotti dall'associazione HL7. Tuttavia, se ne sottolineano due di particolare rilevanza:

- *Electronic Health Record-System Functional Model (EHR-S FM)* [15, 33]: delinea le caratteristiche e le principali funzioni che dovrebbero essere contenute in un sistema di Electronic Health Record. Attraverso la creazione di profili funzionali, questo modello fornisce una descrizione standard e una comprensione comune delle funzioni che un sistema IT dovrebbe offrire per supportare l'assistenza sanitaria. Fino ad oggi, HL7 ha sviluppato o sta sviluppando profili per aree quali la salute dei bambini, le cure in emergenza, le cure a lungo termine, la salute comportamentale e il reporting delle statistiche vitali. In Italia, è stato elaborato da un gruppo di lavoro coordinato da HL7 Italia il *Profilo Funzionale per il FSE Regionale* basato sul modello funzionale EHR-S FM, utilizzato per l'identificazione delle funzioni che i sistemi regionali di FSE devono implementare.

- *Retrieve, Locate, Update Service (RLUS)* [16]: definisce le capacità, le responsabilità, gli input, gli output e il comportamento previsto per una componente di un sistema in grado di interrogare le informazioni e restituire dati e metadati tra sistemi, in maniera conforme all'approccio CRUD (Create, Retrieve, Update, Delete). RLUS può essere utilizzato per gestire una moltitudine di contenuti informativi tramite un meccanismo di accesso standard, promuovendo la coerenza all'interno di un ambiente eterogeneo. Le specifiche funzionali dello standard sono state prodotte da HL7, mentre quelle tecniche da OMG, nell'ambito di una cooperazione stipulata per il progetto Healthcare Services Specification Program (HSSP).

5.2 DICOM

Lo standard Digital Imaging and COmmunications in Medicine (DICOM) [17] definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico con particolare riferimento alle immagini radiologiche.

La diffusione dello standard DICOM si è rivelata estremamente vantaggiosa perché ha consentito di avere una solida base di interscambio di informazioni tra apparecchiature di diversi produttori e sistemi informativi sanitari. Le apparecchiature in grado di produrre immagini DICOM sono molteplici: CT, MRI, PET, ecc. Il sistema informativo sanitario deputato alla archiviazione di immagini DICOM è denominato Picture Archiving and Communication System (PACS).

Il progetto originario venne sviluppato da due associazioni statunitensi: l'American College of Radiology (ACR), responsabile dello sviluppo tecnico-medico del sistema, e la National Electrical Manufacturers Association (NEMA), un consorzio di produttori responsabile tra l'altro degli aspetti inerenti eventuali violazioni di brevetti e normative.

I dati radiologici rappresentabili come immagini o le immagini vere e proprie che vengono archiviate secondo lo standard DICOM sotto forma di file vengono comunemente chiamate immagini DICOM. Lo standard definisce il metodo per incapsulare i dati e per definire come questi debbano essere codificati o interpretati, ma non definisce alcun nuovo algoritmo di compressione. Un'immagine DICOM è composta da due parti: header e body. L'header ha lo scopo di memorizzare informazioni di contesto (metadati), quali la data dello studio, la tipologia di immagine, le modalità con cui è stata acquisita una immagine, ecc. Tali metadati sono identificati da coppie di numeri esadecimali detti "tag". Il body contiene l'immagine vera e propria. La maggior parte delle volte, l'immagine viene archiviata in forma non compressa, secondo la codifica con la quale viene prodotta, ma esistono molti software che sono in grado di produrre o interpretare file DICOM contenenti dati compressi secondo vari algoritmi (JPEG, JPEG Lossless, JPEG Lossy, ecc.).

Il modello dati dello standard DICOM è organizzato in quattro concetti correlati secondo un approccio gerarchico: Patient, Study, Series, Image, come mostrato nella figura successiva. Un paziente può avere molteplici studi in tempi differenti, mentre ciascuno studio può includere diverse serie di immagini con una o più istanze.

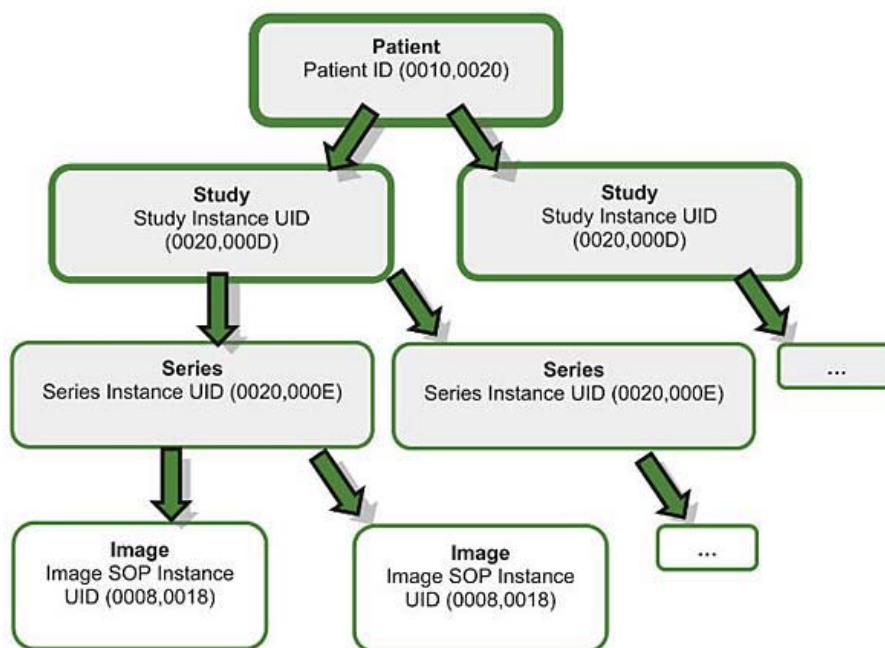


Figura 4. Modello dei dati dello standard dicom

Esistono numerosi programmi che consentono la visualizzazione di immagini DICOM su normali PC, spesso anche liberamente scaricabili via rete internet. Molti di questi permettono anche di eseguire sulle immagini elementari operazioni di post-processing, quali misure lineari e di area.

La versione più diffusa dello standard DICOM è la versione 3.0, secondo la quale le informazioni trasmissibili si possono dividere in due classi: classi di oggetto e classi di servizio.

Le classi di oggetto rappresentano una descrizione formale astratta di entità reali, note come oggetti d'informazione (quali ad es. forme d'onda, referti strutturati, ecc.). Esse, a loro volta, si possono classificare in composite o normalizzate: le prime includono le immagini relative agli esami del paziente, le seconde le informazioni riguardanti specificamente il paziente, gli esami effettuati, gli esiti, ecc. Nell'ambito di ciascuna delle due classi sopra menzionate, sono associate i rispettivi codici di comando (DICOM commands) tramite i quali si possono gestire le informazioni contenute nelle classi medesime.

Le classi di servizio rappresentano invece un insieme di procedure operative tramite le quali può avvenire lo scambio di dati e immagini tra un sistema digitalizzato e un altro. Anche le classi di servizio sono associate a codici di comando, tramite i quali si possono richiedere i servizi desiderati. Le più importanti classi di servizio sono le seguenti:

- *Print*: gestisce le comunicazioni tra una applicazione DICOM e una stampante.
- *Storage*: gestisce il trasferimento e l'archiviazione di immagini tra applicazioni DICOM.
- *Query/Retrieve*: gestisce le operazioni di accesso e trasferimento di immagini in base a un criterio di ricerca.
- *Verification*: verifica le comunicazioni tra applicazioni DICOM.
- *Working list*: gestisce la connessione tra i dati del paziente e le immagini prodotte dalle diverse modalità diagnostiche. In questo modo si ha una relazione univoca tra dati personali e dati dell'immagine.

Gli oggetti d'informazione e le classi di servizio sono i due componenti fondamentali di DICOM: i primi contengono i dati da trattare, le seconde si occupano della manipolazione di tali dati. La combinazione degli oggetti d'informazione e delle classi di servizio forma la cosiddetta SOP Class (Service Object Pair), l'unità funzionale dello standard.

La struttura di un PACS conforme allo standard DICOM è generalmente basata su un server centrale, dove vengono archiviati tutti gli esami del reparto, collegato alle apparecchiature diagnostiche e alle stazioni di refertazione. Tutti i dispositivi collegati in rete hanno un comportamento di tipo client verso il server centrale, potendo eseguire operazioni di invio di informazioni o di ricerca esame.

Le case produttrici di apparecchiature rilasciano tipicamente dei documenti di conformità, nei quali sono presenti tutti i riferimenti alle parti dello standard DICOM implementati sull'apparecchiatura. La dichiarazione di conformità DICOM è un documento molto importante che deve essere studiato attentamente durante la fase di progettazione del PACS, per evitare che vi siano dispositivi non collegabili fra loro o privi di alcune importanti funzioni. L'architettura del PACS è infatti basata su una rete in grado di connettere le apparecchiature di acquisizione delle immagini, le stazioni di visualizzazione e l'archivio digitale.

Negli ultimi anni si è registrato un notevole sforzo indirizzato a favorire il collegamento delle immagini prodotte dalle apparecchiature medicali con il workflow utilizzato nei dipartimenti ospedalieri di radiologia. In particolare, sono stati identificati protocolli HL7 V2 capaci di integrare i sistemi PACS con i sistemi informativi radiologici che gestiscono tali processi e memorizzano i dati risultanti dallo svolgimento delle attività svolte nei reparti, anche noti come Radiology Information System (RIS) [18].

5.3 IHE – Profilo XDS

Integrating the Healthcare Enterprise (IHE) [19] è un'iniziativa internazionale nata nel 1998 dalla collaborazione di Radiological Society of North America (RSNA) e Healthcare Information and Management Systems Society (HIMSS) e si propone di definire in maniera chiara come gli standard esistenti (in particolare DICOM e HL7) devono essere utilizzati dai diversi sistemi informativi per realizzare un'integrazione tra loro. IHE non definisce un vero e proprio standard di comunicazione, bensì costruisce un linguaggio univoco, eliminando le possibili ambiguità contenute negli standard esistenti. IHE non si occupa di come sono fatti i componenti, ma di come possono collegarsi ed interoperare fra loro. Nello stesso tempo IHE vuole essere un ambiente di riferimento sui problemi di integrazione tra i diversi sistemi informativi e le apparecchiature medicali. Per realizzare questo obiettivo è necessario un aggiornamento continuo dei documenti di linee guida (Technical Framework) e la collaborazione aperta tra vendor e utilizzatori.

L'iniziativa IHE dagli Stati Uniti si è diffusa in tutto il mondo con la creazione di diversi comitati IHE nazionali e regionali. Attualmente la struttura è divisa in tre grandi Regioni (Nord America, Europa, Asia) a loro volta divise in affiliate nazionali. Questo tipo di suddivisione permette di gestire la localizzazione, ovvero la caratterizzazione in ambito regionale o nazionale di quanto contenuto nei Technical Framework internazionali.

In particolare, IHE è un'iniziativa volta a stimolare l'integrazione dei sistemi informativi che supportano le strutture sanitarie moderne. Il suo obiettivo fondamentale è quello di garantire che nella cura dei pazienti tutte le informazioni necessarie per le decisioni mediche siano corrette e disponibili agli operatori sanitari. L'iniziativa IHE è sia un processo che un forum per incoraggiare gli sforzi di integrazione. Essa definisce un quadro tecnico per l'attuazione delle norme stabilite di messaggistica per raggiungere specifici obiettivi clinici. IHE comprende un rigoroso processo di testing per l'attuazione di questo quadro. Inoltre, organizza sessioni formative ed esposizioni, dove i più importanti professionisti del settore medico si incontrano per dimostrare

i benefici di questa iniziativa e incoraggiare la sua adozione da parte dell'industria e degli utenti [20].

IHE definisce una serie di profili di integrazione, ognuno dei quali mira a risolvere problematiche relative ad uno specifico dominio. I profili IHE vincolano ulteriormente le scelte di configurazione e, se necessario, gli standard da utilizzare per assicurare che essi possono essere utilizzati nei loro rispettivi domini in modo integrato tra i vari attori. Nei casi in cui si rendono necessari chiarimenti o estensioni a standard esistenti, IHE fornisce raccomandazioni agli organi competenti di normalizzazione.

In alcuni casi, IHE raccomanda la selezione di opzioni specifiche supportate da tali norme, tuttavia, IHE non introduce scelte tecniche che contraddicono la conformità a questi standard. Se errori o estensioni a standard esistenti vengono identificati, la politica di IHE è quello di comunicarli agli organismi di normazione competenti per la risoluzione all'interno della loro conformità e l'evoluzione di standard strategici.

IHE è quindi un quadro di attuazione, non uno standard. Dichiarazioni di conformità per i prodotti devono ancora essere fatte in riferimento diretto a norme specifiche. Inoltre, i fornitori che hanno implementato funzionalità di integrazione IHE nei loro prodotti possono pubblicare dichiarazioni di integrazione IHE per comunicare le capacità dei loro prodotti. Per i vendors che pubblicano dichiarazioni di integrazione, IHE assume la piena responsabilità per il loro contenuto.

Uno dei profili di integrazione definiti da IHE più diffusi su scala internazionale è Cross-Enterprise Document Sharing (XDS) [21], che ha come obiettivo quello di fornire uno strumento che faciliti la registrazione, la distribuzione e l'accesso ai dati medici elettronici. Lo scopo principale è quello di fornire delle specifiche basate su standard esistenti per la gestione e la condivisione di documenti fra diversi ambienti medici.

Il profilo prevede che le varie strutture coinvolte formino uno stesso "Affinity Domain", che rappresenta un set di linee guida e di infrastrutture condivise. In questo insieme è inclusa la modalità con cui i pazienti sono identificati, le regole di accesso ai dati, i formati dei dati accettati, i contenuti dei documenti, l'organizzazione e la rappresentazione dei dati clinici [22].

La prima versione del profilo (XDS.a) differisce da una sua seconda versione denominata XDS.b, in quanto in quest'ultimo caso vengono adottati degli standard in revisioni più recenti (ebXML 3.0, SOAP v1.2, MTOM/XOP).

Nel profilo XDS si definiscono i seguenti attori:

- *Document Source*: è l'entità predisposta alla creazione ed alla pubblicazione dei documenti. Il suo compito è quello di spedire al Document Repository i documenti assieme ai loro metadati, che saranno successivamente registrati nel Document Registry.
- *Document Consumer*: questo attore interroga il Document Registry per ottenere determinati un elenco di metadati associati a documenti che soddisfano determinati criteri di ricerca, e si preoccupa del recupero di tali documenti interagendo con il Document Repository che li detiene.
- *Document Registry*: è il detentore di tutti i metadati di ciascun documento che è stato registrato nel sistema. Tra i metadati c'è anche il riferimento al repository in cui effettivamente si trova il documento. Tale attore ha anche il compito di rispondere alle query sottomesse dal Document Consumer sui documenti che rispondono ai criteri di ricerca. Esegue inoltre ulteriori controlli di validazione sui documenti al momento della loro registrazione.
- *Document Repository*: è in primo luogo il responsabile della conservazione persistente dei documenti. Inoltre, nel momento in cui riceve un determinato documento dal Document Source, provvede alla sua registrazione sul Document Registry. I documenti vengono immagazzinati e subito resi disponibili per il recupero da parte del Consumer attraverso un URI assegnato dal repository. Se questo attore è integrato con il Document Source costituisce il cosiddetto Integrated Document Source Repository.

- *Patient Identity Source*: assegna un identificativo univoco ad ogni paziente di cui conserva una serie di informazioni come ad esempio i dati anagrafici.

Nel profilo XDS si definiscono le seguenti transazioni utilizzate dagli attori per scambiare informazioni, come mostrato nella figura successiva:

- *Provide and Register Document Set-b*: è avviata dal Document Source e coinvolge il Document Repository. Il Document Source invia al Document Repository un insieme di documenti e per ciascuno di essi spedisce il contenuto “grezzo” in forma di flusso di byte (questo garantisce l’indipendenza dal formato del documento) e i metadati corrispondenti. Il Document Repository è quindi tenuto a conservare in maniera persistente il contenuto del documento, mentre dovrà fornire i metadati al Document Registry.
- *Register Document Set - b*: il Document Repository che riceve un insieme di documenti dal Document Source invia i metadati al Document Registry tramite questa transazione. Il Document Registry prima di effettuare il salvataggio dei metadati deve effettuare alcune validazioni su ciascun documento, e se anche uno solo dei documenti non risulta valido, allora l’intera transazione è cancellata; al termine della fase di validazione il risultato viene retituito al Document Repository, il quale, in caso di documenti non validi, non dovrà salvare nessuno dei documenti del set.
- *Registry Stored Query*: il Document Consumer effettua questa transazione su un Document Registry per effettuare la ricerca di tutti i documenti che soddisfano i criteri specificati nella query. Il Document Registry, a seguito della query, restituisce una lista di elementi, che posseggono tra le altre cose metadati e identificativi. Tali informazioni permettono il recupero degli effettivi documenti dal Repository che li contiene.
- *Retrieve Document Set*: una volta che il Document Consumer ottiene le informazioni per recuperare i documenti di interesse dal Document Registry, tramite questa transazione li può recuperare direttamente dal Document Repository.
- *Patient Identity Feed*: lo scopo di questa transazione basata su messaggi conformi allo standard HL7 V2 è quello di fornire al Document Registry gli identificativi di tutti i pazienti che sono stati registrati all’interno dell’Affinity Domain.
- *Patient Identity Feed HL7 V3*: ha lo stesso scopo della transazione precedente, ma è basata su messaggistica conforme allo standard HL7 V3.

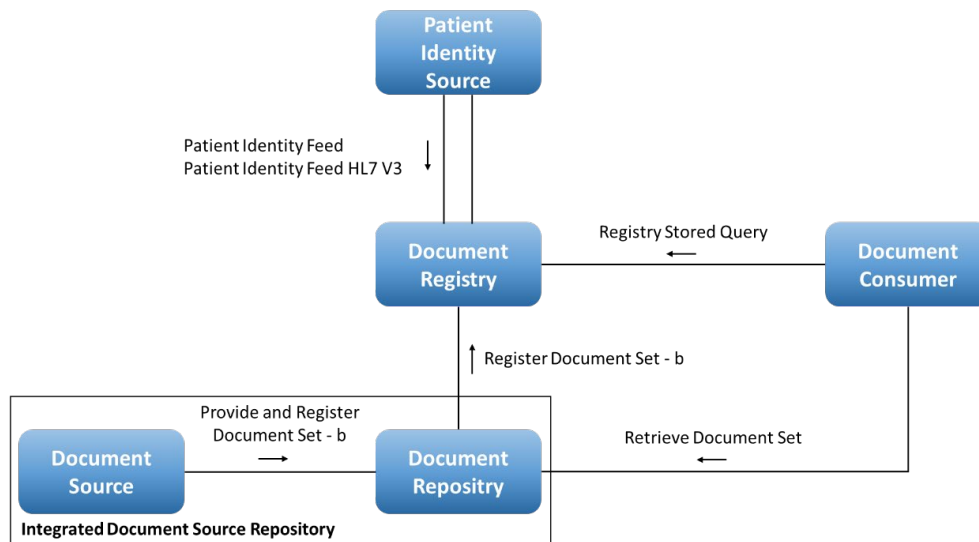


Figura 5. Attori e transazioni del profilo IHE XDS

Gli oggetti informativi gestiti dal profilo XDS sono i seguenti:

- *XDS Document*: si definisce come la più piccola unità di informazione che può essere memorizzata in un Document Repository e registrata da un Document Registry. Il profilo XDS non prevede la possibilità di accedere a singole porzioni di un XDS Document: questa operazione può essere svolta solamente da un Document Consumer o dal Document Source. Un documento deve possedere un identificativo globalmente univoco tra tutti gli Affinity Domain: questo consente la possibilità ad un Document Repository di essere usato all'interno di più Affinity Domain, ma offre anche la possibilità di scambiare documenti tra Affinity Domain diversi. Il Document Registry deve mantenere un singolo record ("Document Entry") per ogni XDS Document presente in un Document Repository. Il profilo XDS descrive tutti i metadati che devono essere associati ad un documento. La responsabilità della coerenza fra metadati e contenuto del documento è solamente del Document Source; non è previsto alcun controllo da parte del Document Repository né del Document Registry. Solo il Document Source ha la possibilità di cambiare lo stato di un documento da "approved" a "deprecated" o di eliminare il documento stesso, ed è l'unico attore che può sostituire un documento preesistente con uno nuovo.
- *XDS Folder*: lo scopo di questo oggetto è quello di raggruppare più XDS Document che per diverse ragioni si possono considerare in relazione. Le principali caratteristiche di un XDS Folder sono:
 - può contenere soltanto documenti relativi alla cura dello stesso paziente;
 - non si possono avere XDS Folder nidificati;
 - un documento può appartenere a più XDS Folder;
 - ciascun XDS Folder possiede un identificativo univoco.
- *XDS Submission Set*: il concetto di tale oggetto è correlato ad uno o più "prestazioni mediche" effettuate su un paziente da un ente sanitario che vuole eseguire una XDS Submission Request. In questo modo l'evento è reso persistente, ossia in esso vengono specificati i nuovi documenti da mettere in condivisione e nuove cartelle, ma possono essere inclusi anche documenti preesistenti che però hanno una relazione con quell'evento. Per ogni XDS Submission Request, viene creata una sola XDS Submission Set legata al singolo Document Source che ha iniziato una transazione di condivisione. Una XDS Submission Set può essere oggetto di una query con lo scopo di recuperare

tutti i documenti relativi ad essa, quindi rilevanti per l'evento che la XDS Submission Set rappresenta. Un documento può essere referenziato da più XDS Submission Set: in questo modo vecchi documenti rilevanti ai fini di una cura recente possono essere messi in relazione a nuove XDS Submission Set. XDS permette piena libertà nel mettere in relazione una XDS Submission Set ad un incontro, una visita, una prestazione medica o a qualsiasi altro evento previsto.

- *XDS Submission Request*: può essere visto come l'involucro usato all'atto della condivisione di qualsiasi altro oggetto XDS all'interno dell'Affinity Domain. Attraverso le XDS Submission Request si possono condividere XDS Document, XDS Folder e XDS Submission Set. Le uniche due transazioni che mettono in condivisione dei dati e che quindi utilizzano XDS Submission Request sono "Provide and Register Document Set - b" e "Register Document Set - b". In particolare una Submission Request contiene:
 - zero o più documenti nuovi che devono essere salvati e condivisi nel sistema;
 - i metadati per ciascun nuovo documento presente in una XDS Submission Request;
 - zero o più XDS Folder con la lista dei documenti che deve contenere. Questi documenti possono essere nuovi, quindi presenti in una XDS Submission Request, oppure possono essere già stati immessi e condivisi nell'Affinity Domain;
 - eventualmente una lista di documenti (nuovi o già condivisi) che devono essere aggiunti a XDS Folder già esistenti;
 - una e una sola XDS Submission Set che contiene tutti i documenti e gli XDS Folder creati in una XDS Submission Request. Eventualmente può essere inclusa una lista di documenti preesistenti.

5.4 Personal Connected Health Alliance

Personal Connected Health Alliance [23] è una organizzazione no profit costituita con lo scopo di facilitare lo sviluppo e l'adozione di soluzioni ICT per il personal health attraverso un approccio integrato. Stabilita nel 2006 come Continua Health Alliance, l'organizzazione pubblica e promuove le linee guida denominate Continua Design Guidelines, che specificano un framework di implementazione aperto basato su standard internazionali per l'interoperabilità end-to-end dei dispositivi e dei sistemi sanitari connessi personali.

L'ultima versione delle Continua Design Guidelines identificano quattro stack tecnologici per favorire l'interoperabilità end-to-end, come mostrato nella figura successiva:

- *Personal Health Devices*: rappresentano i dispositivi personali capaci di generare dati di natura sanitaria;
- *Personal Health Gateway*: consiste in dispositivi (quali smartphone, laptop, PDA, ecc.) in grado di acquisire e processare i dati raccolti dai Personal Health Devices;
- *Health & Fitness Service*: rappresenta un centro di servizio al quale il Personal Health Gateway invia i dati per operazioni di post-processing dei dati acquisiti;
- *Healthcare Information Service (HIS)*: rappresenta un sistema informativo sanitario (ad es. FSE, Fascicolo Sanitario Personale, ecc.) deputato alla memorizzazione persistente dei dati.

Ciascuna componente di uno stack tecnologico interagisce con le componenti degli altri stack tecnologici

attraverso apposite interfacce): Personal Health Devices Interface, Services Interface, HIS Interface. Per ciascuna tipologia di interazione sono stati identificati gli standard internazionali di informatica sanitaria da utilizzare.

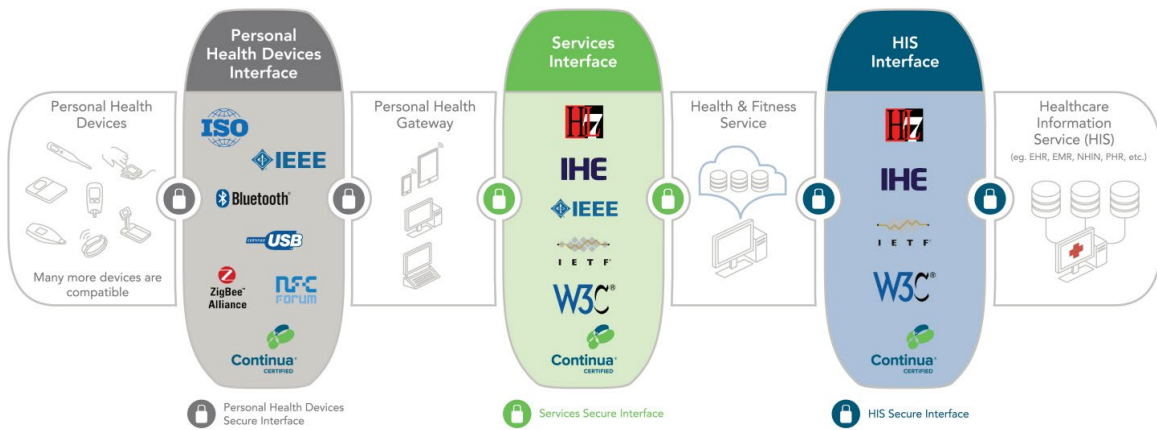


Figura 6. Stack tecnologici delle Continua Design Guidelines

Con riferimento alle interazioni tra i Personal Health Devices e il Personal Health Gateway, lo standard di riferimento è ISO/IEEE 11073 Personal Health Devices (X73PHD) [24], che specifica i seguenti aspetti:

- *nomenclatura*: definisce codici binari per la codifica delle risorse terminologiche;
- *Domain Information Model (DIM)*: definisce un modello informativo comprendente oggetti contenenti rappresentazioni di parametri vitali e le loro relazioni;
- *modello di servizio*: definisce le modalità di scambio dei messaggi;
- *modello di comunicazione*: formalizza una macchina a stati finiti (FSM) per la rappresentazione degli stati relativi alla connessione dei dispositivi personali con il Personal Health Gateway, come mostrato nella figura successiva. Tale modello è posto al di sopra dei protocolli di comunicazione fisici. Inoltre, converte i dati astratti modellati secondo il DIM in un messaggio binario traducendo regole codificate secondo la notazione Abstract Syntax Notation One (ASN.1) in primitive aderenti allo standard Medical Device Encoding Rules (MDER).

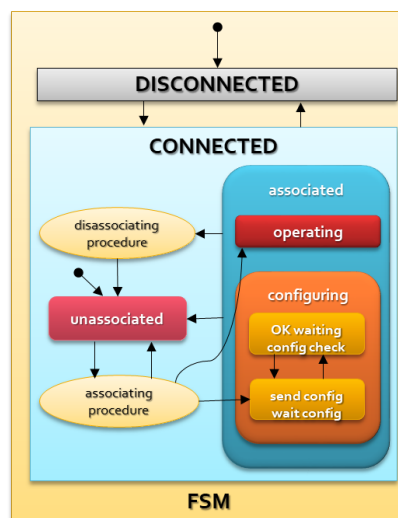


Figura 7. Macchina a stati finiti per la connessione dei dispositivi personali

Lo standard definisce un protocollo per lo scambio dati generico ed ulteriori specializzazioni per specifici dispositivi personali, quali pulsossimetri, monitoraggio della pressione del sangue, termometri, glucometri, ecc., come rappresentato nella figura successiva.

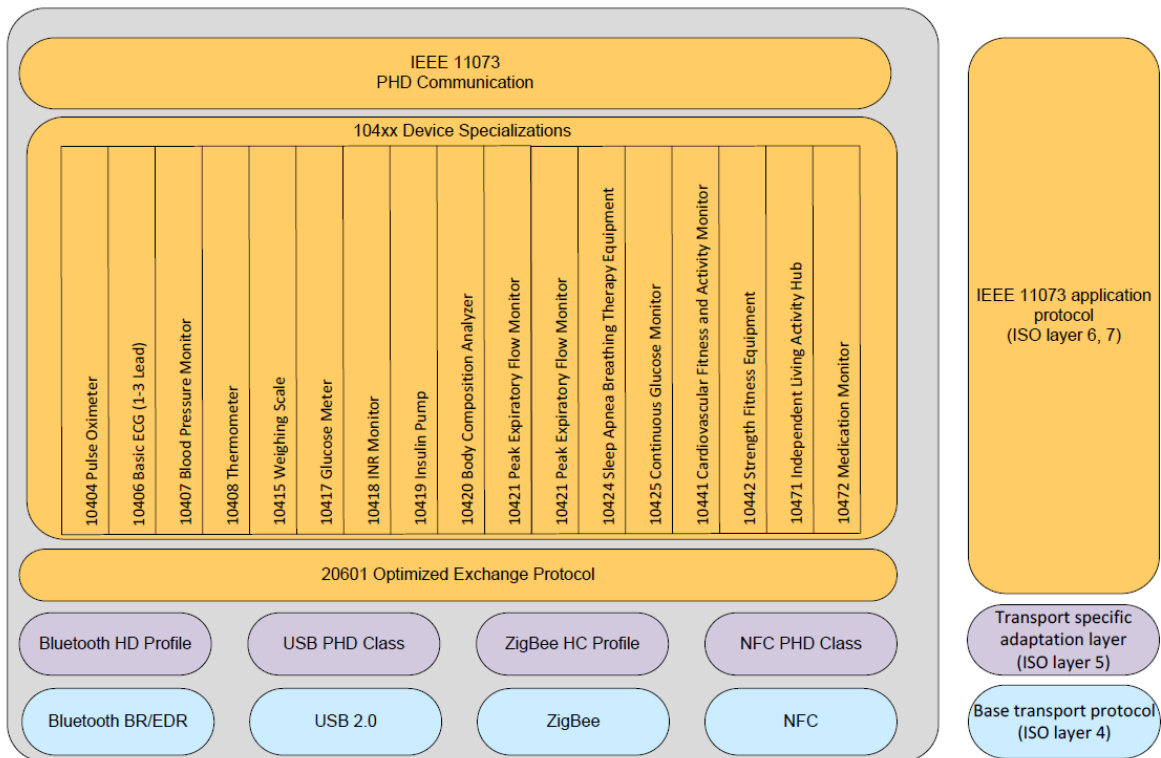


Figura 8. Protocolli di comunicazione DELLO STANDARD ISO/IEEE 11073

Per quanto riguarda l'interazione tra il Personal Health Gateway e l'Health & Fitness Service, le linee guida sono basate sul dominio IHE Patient Care Device (PCD) [25], che fornisce specifiche per casi d'uso in cui almeno un attore è un dispositivo medico presente presso il punto di cura di un paziente. In particolare, il profilo del dominio IHE PCD scelto è Device Enterprise Communication (DEC) [26], che specifica le modalità per comunicare dati di un dispositivo ad applicazioni enterprise, mediante protocolli basati sullo standard HL7 V2. Inoltre, i contenuti dei messaggi in formato HL7 V2 possono essere trasmessi anche usando lo standard HL7 FHIR. Gli attori e le transazioni identificate per il profilo DEC sono mostrate nella figura successiva.

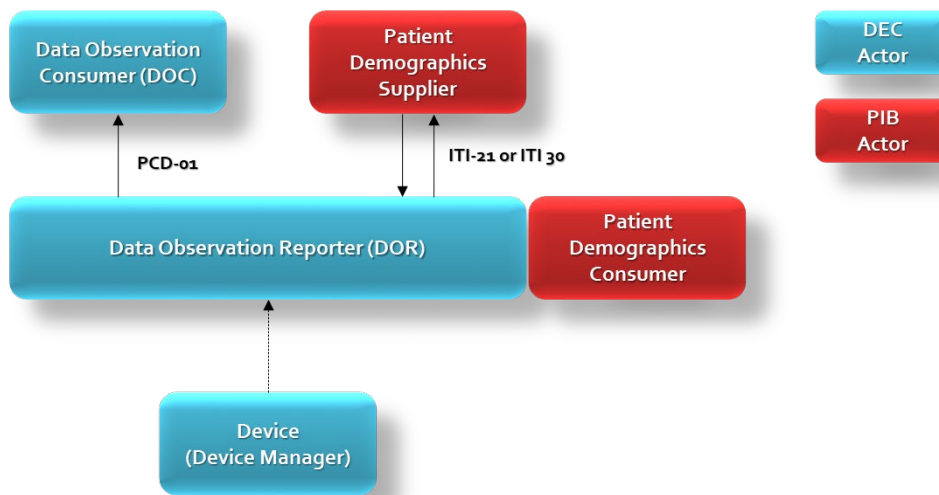


Figura 9. Attori e transazioni del profilo IHE PCD DEC

Al fine di facilitare la codifica delle risorse terminologiche secondo i formalismi standard, è suggerito l'utilizzo dello standard IHE PCD Rosetta Terminology Management (RTM) [27], che consiste in tabelle di mappatura delle codifiche utilizzate dai principali vendor con quelle specificate dagli standard, come mostrato nella figura successiva.

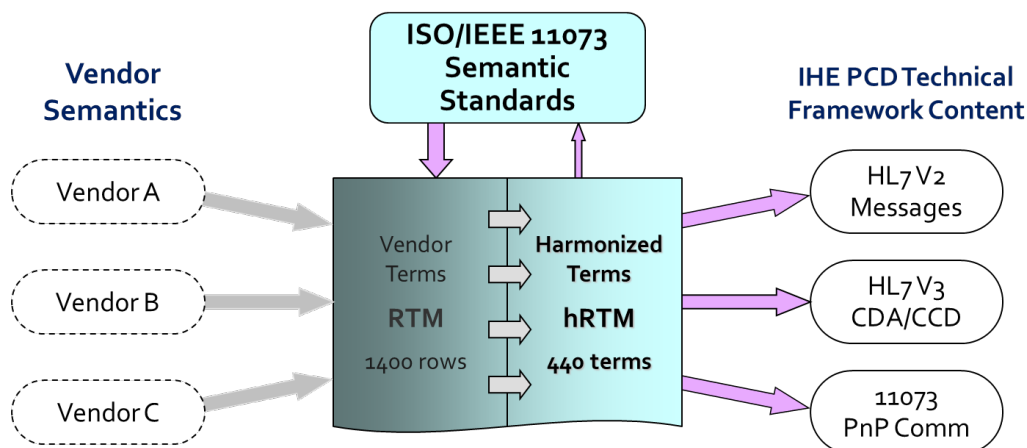


Figura 10. modello di mappatura semantica dello standard IHE PCD RTM

Infine, l'interazione con l'ultimo stack tecnologico è basata sui protocolli di comunicazione specifici del particolare sistema informativo sanitario. Si raccomanda in particolare l'utilizzo di standard per la strutturazione dei documenti sanitari e la codifica dei contenuti. Con riferimento al formato dei documenti, lo standard identificato è HL7 Personal Healthcare Monitoring Report (PHMR) [28], che definisce le modalità per strutturare, secondo lo standard HL7 CDA Rel. 2.0, documenti di reportistica contenenti i dati acquisiti dai dispositivi personali e processati. Per quanto riguarda gli standard di codifica, si fa riferimento, tra gli altri, a SNOMED, LOINC, UCUM e IEEE 11073.

6. Protocolli e standard di comunicazione tra i dispositivi

Questa sezione è incentrata sulla descrizione dei principali protocolli di comunicazione standard per l'interazione tra dispositivi eterogenei. Considerata l'ampia disponibilità di protocolli definiti in ambito internazionale, di seguito sono presentate le interfacce previste dalle Continua Design Guidelines per l'acquisizione di dati da dispositivi personali sanitari, le quali possono essere suddivise nelle due seguenti categorie:

- Interfacce per la trasmissione dati tramite cavo: relativamente a questa categoria, l'interfaccia di riferimento è Universal Serial Bus (USB).
- Interfacce per la trasmissione dati wireless: per quanto riguarda questa categoria, sono prese in esame le interfacce Bluetooth, ZigBee e Near Field Communication (NFC).

6.1 Trasmissione dati tramite cavo

L'interfaccia di comunicazione di riferimento per la trasmissione di dati acquisiti da dispositivi personali sanitari è USB [29], utilizzata per favorire la funzionalità Plug and Play, in quanto consente sia la connessione, sia la comunicazione e sia l'alimentazione tra calcolatori e dispositivi elettronici.

La comunicazione su bus USB è del tipo master/slave: un Host funge da master, ossia è responsabile della configurazione e della comunicazione attraverso il bus, mentre i Device fungono da slave, ossia da punti terminali capaci di rispondere ai comandi del protocollo. Ciascun Device è universalmente identificato dalla coppia (VendorId, ProductId). Inoltre, gli Hub permettono di implementare una rete a stella, in quanto permettono di aumentare le connessioni USB. Gli Hub possono essere connessi in cascata fino ad un massimo di 5 livelli.

I cavi utilizzati per le connessioni su bus USB sono composti da 4 fili, due per la comunicazione e due per l'alimentazione.

La comunicazione tra Host e Device è denominata transfer, la quale può essere composta da una o più transaction non parallele. A sua volta, ciascuna transaction è organizzata in un insieme di packets: il token, che contiene informazioni relative al tipo di transaction e al Device, e il data packet, che rappresenta il payload. Esistono quattro differenti tipologie di transfer:

- *Control transfer*: consiste in messaggi utilizzati per la configurazione dei Device;
- *Bulk transfer*: permette di trasferire grandi moli di dati in un tempo non determinato;
- *Interrupt transfer*: consente di trasferire dati secondo una tempistica specificata;
- *Isochronous transfer*: permette di trasferire dati in tempo reale (quali streaming audio o video) con garanzie sul tempo di trasferimento.

Lo sviluppo dell'interfaccia USB cominciò nel dicembre del 1994 ad opera di 7 imprese: Compaq, DEC, IBM, Intel, Microsoft, NEC e Nortel. Da allora, USB ha continuato a diventare più veloce con ogni revisione delle specifiche. In basso sono riportate le principali revisioni o versioni di USB:

- *USB 1.0 (Low Speed)*: è stata la prima versione di USB ad essere presentata ufficialmente nel gennaio del 1996 ed è in grado di trasferire dati fino a 1,5 Mbps;

- *USB 1.1 (Full Speed)*: è stata rilasciata nell'agosto del 1998 ed è capace di trasferire dati fino a 12 Mbps;
- *USB 2.0 (High Speed)*: è stata rilasciata nell'aprile del 2000 e supporta la massima velocità teorica di trasferimento dati fino a 480 Mbps. In realtà, il throughput effettivo massimo è limitato a 280 Mbps. USB 2.0 è retrocompatibile con USB 1.0 e USB 1.1;
- *USB 3.0 (SuperSpeed)*: è stata rilasciata nel novembre del 2008 ed è in grado di supportare velocità di trasferimento dati teoriche fino a 5 Gbps, sebbene la velocità reale che si può ottenere è di circa 3,2 Gbps;
- *USB 3.1 (SuperSpeed+)*: è stata rilasciata nel luglio del 2013 ed è in grado di trasferire dati teorici di 10 Gbps, il doppio di quelli di USB 3.0. In realtà, la velocità di trasferimento massima raggiungibile è di 7,2 Gbps;
- *USB 3.2 (SuperSpeed+)*: è stata rilasciata nel settembre del 2017 ed è in grado di trasferire dati teorici di 20 Gbps. È retrocompatibile con le versioni USB 3.1, 3.0 e 2.0.

I connettori USB più comuni sono i seguenti:

- *USB Tipo A*: è il tipo più comune di connettore e porta USB introdotto nel 1996. Il connettore è ampio e ingombrante e si trova all'estremità del cavo USB inserito nell'Host;
- *USB Tipo B*: introdotto nel 1996, è generalmente utilizzato all'estremità del cavo che si collega alla stampante, allo scanner e ad altri dispositivi di grandi dimensioni;
- *Mini USB*: sono versioni più piccole dei connettori USB Tipo A e USB Tipo B. Sono stati introdotti nel 2000. Tuttavia, i connettori Mini USB sono molto rari al giorno d'oggi, poiché sono diventati obsoleti dai nuovi connettori Micro USB;
- *Micro USB*: sono ancora più piccoli dei connettori Mini USB e sono oggi i connettori USB più utilizzati, specialmente su smartphone e fotocamere. Sono stati introdotti nel 2007;
- *USB Tipo C*: è la versione più recente di un connettore USB, rilasciata nel 2014, ed è caratterizzata da tre elementi: è piccolo, reversibile e generalmente utilizzato per le porte USB 3.1.

6.2 Trasmissione dati wireless

Questo paragrafo descrive le principali tecnologie per la connettività e trasmissione di dati wireless maggiormente utilizzate per l'interazione con i dispositivi personali, quali Bluetooth, ZigBee e NFC.

6.2.1 Bluetooth

Bluetooth [30] è una tecnologia radio a corto raggio, che è stata sviluppata inizialmente da Ericsson per le reti di tipo Personal Area Network (PAN) e la cui ultima versione, Bluetooth 5.0, è stata presentata nel giugno 2016. Il Bluetooth è uno standard sviluppato da un gruppo di produttori di elettronica che consente a qualsiasi tipologia di dispositivo elettronico - dai computer e telefoni cellulari a tastiere e cuffie - di effettuare le proprie connessioni, senza fili, cavi o qualsiasi azione diretta da un utente. È un tipo di rete ad hoc che opera su piccole aree, come ad esempio una stanza. Le principali caratteristiche della tecnologia Bluetooth sono:

- elimina cavi tra dispositivi fissi e mobili;
- facilita sia la comunicazione sia dei dati sia della voce;
- offre la possibilità di realizzare reti ad hoc e offre la massima sincronicità tra tutti i dispositivi personali.

Il Bluetooth è uno standard dinamico in cui i dispositivi possono trovarsi automaticamente tra di loro, stabilire connessioni e scoprire cosa possono fare l'uno per l'altro. Il Bluetooth è concepito come uno standard che funziona su due livelli:

- fornisce specifiche per realizzare un accordo a livello fisico: in particolare Bluetooth è uno standard basato su radiofrequenza;
- fornisce anche specifiche per un accordo al livello successivo: in questo livello i prodotti devono mettersi d'accordo relativamente alle modalità di invio dei bit, del numero di bit che vengono inviati alla volta e in che modo le parti in una conversazione possono essere certe che il messaggio ricevuto è uguale al messaggio inviato.

Esistono due tipi di topologie per Bluetooth: Piconet e Scatternet.

Piconet è una piccola rete ad hoc di dispositivi (normalmente 8 stazioni), che presenta le seguenti caratteristiche:

- è basato sul modello master/slave;
- tutte le stazioni slave sincronizzano i loro clock con il master;
- esistono due possibili tipologie di comunicazione: one-to-one o one-to-many;
- una stazione potrebbe essere nello stato parked;
- ogni Piconet ha un unico modello di salto (hopping);
- ciascun master può connettersi con 7 slave simultanei o con più di 200 slave non attivi (ossia nello stato parked) per Piconet.

Scatternet può essere formata facendo fungere uno slave da master di un'altra Piconet. Le caratteristiche principali della topologia Scatternet sono:

- è il collegamento di più Piconet attraverso la condivisione di dispositivi master o slave comuni;
- un dispositivo può fungere sia da master che da slave;
- i collegamenti radio sono simmetrici (la stessa connessione radio può essere master o slave);
- è un sistema ad alta capacità: ogni Piconet ha la capacità massima (720 Kbps).

L'architettura di Bluetooth è organizzata in diversi livelli, come mostrato nella figura successiva.

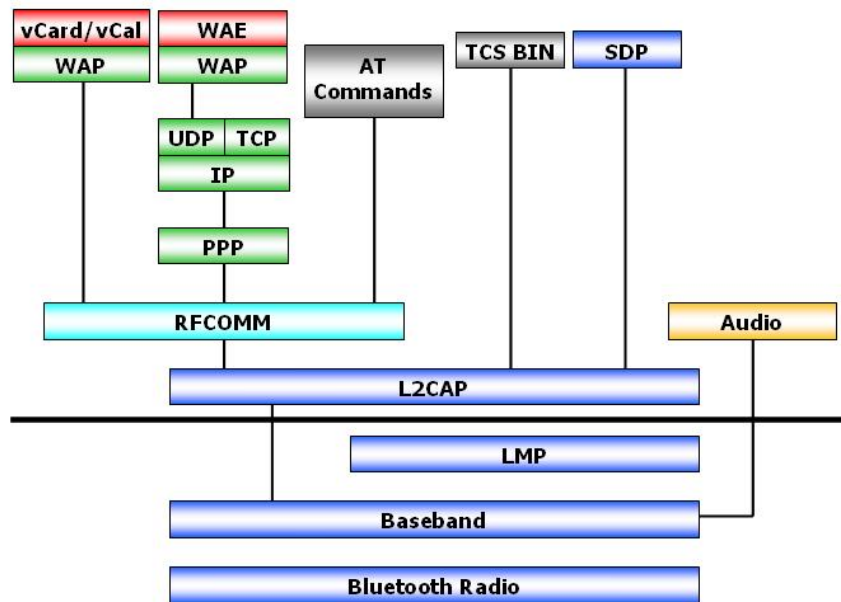


Figura 11. Architettura della tecnologia bluetooth

I livelli dell'architettura della tecnologia Bluetooth sono descritti di seguito:

- *Radio layer*: è responsabile della modulazione e demodulazione dei dati in segnali a radiofrequenza per la trasmissione nell'etere. Questo livello descrive i requisiti fisici che un componente ricevitore-trasmittitore di un dispositivo Bluetooth deve avere, le quali includono caratteristiche di modulazione, tolleranza della radiofrequenza e livello di sensibilità.
- *Baseband/Link Controller layer*: le specifiche Bluetooth non stabiliscono una chiara distinzione tra le responsabilità della componente Baseband e quelle del Link Controller. In generale, la parte del livello relativa alla Baseband è responsabile della corretta formattazione dei dati per la trasmissione da e verso il livello radio, ed inoltre gestisce la sincronizzazione dei collegamenti. La parte del Link Controller di questo livello è responsabile dell'esecuzione dei comandi del gestore di collegamenti e della creazione e della gestione del collegamento stabilito dal Link Manager.
- *Link Manager layer*: traduce i comandi che riceve dal livello superiore nelle operazioni relative alla componente Baseband. È responsabile della creazione e della configurazione dei collegamenti e della gestione delle richieste di cambio di potenza, tra le altre attività. Le specifiche Bluetooth definiscono due tipi di collegamenti tra dispositivi Bluetooth:
 - Synchronous, Connection-Oriented (SCO), per comunicazione isocrona e vocale utilizzando, ad esempio, cuffie;
 - Asynchronous, ConnectionLess (ACL), per la comunicazione di dati, come lo scambio di vCard.
- *HCI (Host Controller Interface) layer*: funge da confine tra i livelli inferiori dello stack del protocollo Bluetooth e i livelli superiori. Le specifiche Bluetooth definiscono un HCI standard per supportare i sistemi Bluetooth implementati su due processori separati. Ad esempio, un sistema Bluetooth su un computer potrebbe utilizzare il processore di un modulo Bluetooth per implementare i livelli inferiori dello stack (Radio, Baseband/Link Controller e Link Manager). Potrebbe quindi utilizzare il proprio processore per implementare i livelli superiori.

- *L2CAP (Logical Link Control and Adaptation Protocol) layer*: ha il compito di stabilire connessioni tra collegamenti ACL esistenti o richiedere un collegamento ACL se non ne esiste già uno; effettuare il multiplexing tra diversi protocolli di livello superiore per consentire ad applicazioni diverse di utilizzare un singolo collegamento ACL; ricompattare i pacchetti di dati che riceve dai livelli superiori nella forma prevista dai livelli inferiori. Questo livello utilizza il concetto di canali per tenere traccia della provenienza dei pacchetti di dati e dove dovrebbero andare.
- *SDP (Service Discovery Protocol) layer*: definisce le azioni sia per i server che per i client dei servizi Bluetooth. Le specifiche definiscono un servizio come qualsiasi funzione utilizzabile da un altro dispositivo (remoto) Bluetooth. Un client SDP comunica con un server SDP utilizzando un canale riservato su un collegamento L2CAP per scoprire quali servizi sono disponibili. Quando il client trova il servizio desiderato, richiede una connessione separata per utilizzare il servizio. Il canale riservato è dedicato alla comunicazione SDP in modo che un dispositivo sappia sempre come connettersi al servizio SDP su qualsiasi altro dispositivo. Un server SDP mantiene il proprio database SDP, che è un set di record di servizio che descrivono i servizi offerti dal server.
- *RFCOMM (Radio Frequency Communication) layer*: emula le impostazioni della linea di cavi seriali e lo stato di una porta seriale RS-232. RFCOMM si connette ai livelli inferiori dello stack del protocollo Bluetooth attraverso il livello L2CAP. Attraverso l'emulazione della porta seriale, RFCOMM supporta le applicazioni legacy proprie di quest'ultima.
- *OBEX (Object Exchange) layer*: è un protocollo di trasferimento che definisce gli oggetti dati e un protocollo di comunicazione che due dispositivi possono utilizzare per scambiare facilmente tali oggetti. Bluetooth ha adottato questo protocollo dalla specifica IrOBEX IrDA perché i livelli inferiori del protocollo IrOBEX sono molto simili ai livelli inferiori dello stack del protocollo Bluetooth. Un dispositivo Bluetooth che desidera configurare una sessione di comunicazione OBEX con un altro dispositivo è considerato il dispositivo client. Il client invia prima le richieste SDP per assicurarsi che l'altro dispositivo possa fungere da server dei servizi OBEX. Se il dispositivo server è in grado di fornire servizi OBEX, risponde con il suo record di servizio OBEX. Questo record contiene il numero di canale RFCOMM che il client deve utilizzare per stabilire un canale RFCOMM. Ulteriori comunicazioni tra i due dispositivi sono convogliate in pacchetti, che contengono richieste/risposte e dati. Il formato del pacchetto è definito dal protocollo di sessione OBEX.

Le specifiche Bluetooth definiscono una vasta gamma di profili, descrivendo tipi diversi di compiti, alcuni dei quali non sono ancora stati implementati da alcun dispositivo o sistema. Seguendo le procedure dei profili, gli sviluppatori possono essere sicuri che le applicazioni che creano funzioneranno con qualsiasi dispositivo conforme alle specifiche Bluetooth.

Una versione che riveste una particolare importanza è quella denominata Bluetooth Low Energy (LE), che ha lo scopo di offrire connettività wireless a bassa potenza, attraverso una serie di tecniche di ottimizzazione a discapito della velocità.

6.2.2 ZigBee

ZigBee [31] è uno standard per reti wireless personali a bassa potenza, ovvero reti wireless a corto raggio (circa 10-100 metri). La prima versione delle specifiche è stata pubblicata nel 2004, mentre nel dicembre del 2014 è stato annunciato il rilascio della versione 3.0. ZigBee viene comunemente utilizzato per applicazioni di controllo e monitoraggio wireless, quali reti di sensori wireless (WSN), monitoraggio di impianti industriali,

controllo dell'edificio, ospedali, misurazione intelligente e automazione domestica. Esistono in realtà profili pubblici definiti nella specifica ZigBee per molti di questi casi d'uso.

ZigBee opera nelle bande radio industriali, scientifiche e mediche e la frequenza esatta dipende dal contesto geografico nel mondo: in particolare, utilizza la banda 868 MHz in gran parte dell'Europa, 915 MHz negli Stati Uniti e 2,4 GHz in molte altre località. La banda a 2,4 GHz è molto comune poiché molti dei chipset disponibili lo usano. Le velocità disponibili dipendono dalla banda in uso, sebbene il massimo sia 250 Kbps. La tecnologia ZigBee è più lenta di altre tecnologie wireless popolari come il WiFi, ma è anche più economica.

Una rete ZigBee consente ad un insieme di dispositivi di comunicare in modalità wireless attraverso diverse topologie possibili. Ogni dispositivo ha sia un indirizzo MAC (Media Access Control) che un indirizzo di rete ZigBee e la rete nel suo insieme ha il proprio identificativo di PAN condiviso da tutti i dispositivi. L'architettura della rete ZigBee, mostrata nella figura successiva, è composta da componenti organizzate in più livelli:

- *Physical Layer (PHY)*: è responsabile di modulazione, demodulazione e trasmissione fisica di pacchetti via etere.
- *Media Access Control Layer (MAC)*: simile ai livelli MAC in altri protocolli, ZigBee in realtà non usa tutte le sue caratteristiche. Questo livello esegue funzioni come CSMA/CA per evitare collisioni durante la trasmissione di frame. Il livello definisce anche le topologie di rete che ZigBee sviluppa e migliora a livelli più alti della pila.
- *Network Layer (NWK)*: garantisce il corretto funzionamento del livello MAC sottostante e fornisce un'interfaccia al livello superiore. Permette di scoprire e unire reti e si espande sulle topologie definite a livello MAC al fine di realizzare reti mesh, una topologia popolare di ZigBee. Il livello determina anche i percorsi attraverso reti e supporta gli indirizzi ZigBee.
- *Application Layer (APL)*: il livello superiore nello stack del protocollo ZigBee è costituito dalle seguenti componenti principali:
 - *Application Framework*: fornisce una descrizione relativa alle modalità di creazione di un profilo sullo stack ZigBee per garantire che i profili possano essere generati in modo coerente. Specifica inoltre una gamma di tipi di dati standard per profili, descrittori che facilitano l'individuazione dei servizi, formati di frame per il trasporto dei dati e un costrutto di coppie chiave-valore per lo sviluppo rapido di profili semplici basati sugli attributi;
 - *ZigBee Device Object (ZDO)*: definisce il ruolo di un dispositivo all'interno della rete (coordinatore, router o dispositivo finale), inizia e/o risponde alle richieste di collegamento e di scoperta e stabilisce una relazione sicura tra i dispositivi di rete. Fornisce inoltre un ricco set di comandi di gestione definiti nel profilo del dispositivo ZigBee (utilizzati nella messa in servizio ZigBee);
 - *Application Support Sublayer (APS)*: implementa le funzionalità necessarie alle applicazioni ZigBee e funge da interfaccia per il livello sottostante. Esegue un filtraggio dei pacchetti duplicati dal livello sottostante e mantiene una tabella di nodi nella rete.

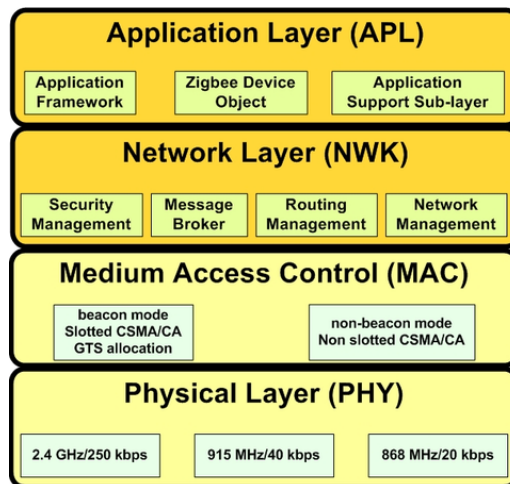


Figura 12. Architettura della tecnologia ZigBee

Un dispositivo, all'interno di una rete ZigBee, può assumere il ruolo di tre tipi di nodi, sulla base della topologia della rete ZigBee, e come i dispositivi aiutano a instradare i messaggi. I tipi di nodo, che vincolano le modalità con le quali un dispositivo instrada i messaggi, sono descritti di seguito:

- *Coordinatore:* ogni rete ZigBee deve avere un unico coordinatore. Questo nodo, che rappresenta il primo nodo da avviare, inizializza il resto della rete, selezionando la frequenza da utilizzare e l'identificativo della rete e consentendo ad altri nodi di unirsi alla rete.
- *Router:* è una componente opzionale responsabile di inoltrare messaggi ad altri nodi. I nodi possono anche unirsi alla rete tramite un router, con quest'ultimo che diventa il nodo principale.
- *Dispositivo terminale:* è un nodo semplice che invia e riceve messaggi ma non esegue altre funzioni speciali nella rete. I dispositivi terminali sono gli unici nodi che possono transitare in uno stato dormiente: infatti, il nodo padre (coordinatore o router) si occupa di memorizzare i messaggi finché il dispositivo finale non si riattiva.

Le reti ZigBee possono essere organizzate secondo tre diverse topologie che influenzano il modo in cui i messaggi vengono instradati e le modalità di comunicazione tra i dispositivi:

- *Topologia a stella:* tutti i dispositivi si connettono a un singolo nodo Coordinatore e tutte le comunicazioni passano attraverso quest'ultimo. I nodi figli possono anche essere di tipo router, sebbene in questa topologia non eseguono alcuna funzionalità di routing e agiscono essenzialmente come un dispositivo finale. Il throughput della rete è limitato dal coordinatore e se il coordinatore si guasta l'intera rete non funziona.
- *Topologia ad albero:* il coordinatore costituisce il nodo radice di un albero. I dispositivi terminali sono nodi foglia (anche se un router può anche essere una foglia se nessun nodo figlio si è ancora unito) e i nodi intermedi sono router. La comunicazione diretta può avvenire solo tra un nodo figlio e il suo nodo genitore, ma tutti i nodi possono comunicare insieme tramite i messaggi che attraversano l'albero verso un antenato comune e quindi verso il nodo di destinazione. In questa topologia i router sono in grado di estendere il raggio della rete oltre a quello di ogni singolo collegamento dispositivo-dispositivo. Tuttavia, se un router non funziona, non vi è alcun percorso alternativo e alcune parti della rete possono essere disconnesse.
- *Topologia mesh:* è una delle topologie più flessibili offerte da ZigBee. È simile alla topologia ad albero, ma senza non è basata su una struttura rigida e un router può comunicare direttamente con

qualsiasi altro router o con il coordinatore se è nel raggio d'azione. Pertanto, possono esistere molteplici percorsi attraverso la rete verso un determinato nodo, e ZigBee prevede una funzione capace di individuare il percorso migliore per raggiungere un dato nodo.

6.2.3 NFC

NFC [32] è una tecnologia per la comunicazione wireless tra dispositivi a distanza ravvicinata, attraverso un contatto fisico o in prossimità (meno di 4 centimetri). La frequenza operativa di tale comunicazione è di 13,56 (+/-7) MHz, che è molto bassa, e quindi offre il vantaggio di integrarsi facilmente in dispositivi portatili senza la necessità di consumare molta batteria. La prima versione di NFC è stata pubblicata nel giugno del 2009, mentre la versione corrente, ossia 3.1.1, è stata approvata nel febbraio del 2014.

Esistono fondamentalmente due tipi di comunicazione possibili nei dispositivi basati su NFC:

- passiva: in questo tipo di comunicazione, i dispositivi NFC non alimentati possono essere letti utilizzando dispositivi abilitati NFC, in grado di fornire potenza;
- attiva: in questo tipo di comunicazione, entrambi i dispositivi utilizzano potenza per trasmettere dati tra di loro; essa può essere generalizzata come una trasmissione Peer-to-Peer (P2P).

I protocolli di comunicazione di tali dispositivi sono basati su una evoluzione dello standard RFID (Radio-Frequency IDentification). In particolare, il dispositivo passivo NFC può essere “intelligente”, ossia possiede un minuscolo calcolatore con il quale può eseguire alcune elaborazioni. Il potenziale NFC è molto ampio e include applicazioni come carte di credito contactless, sistemi tariffari di trasporto pubblico, moneta elettronica memorizzata nel telefono cellulare, ecc.

Questa tecnologia facilita la comunicazione con dispositivi medici in modo molto ergonomico, in quanto l'atto di toccare, ad esempio, un misuratore di pressione sanguigna con il telefono cellulare indica chiaramente che l'utente desidera trasferire le misurazioni. Inoltre, la vicinanza aumenta significativamente la sicurezza.

Nel gergo NFC, il dispositivo passivo viene semplicemente chiamato “tag”, mentre quello attivo è denominato lettore, perché è solo in grado di leggere tag. Il lettore e il tag hanno bobine, non antenne. Quando la bobina del lettore è alimentata, genera un campo magnetico. Quando un tag si avvicina, le due bobine formano un trasformatore e il tag può trarre energia dal lettore. In particolare, esistono differenti tipologie di tag per motivi di retrocompatibilità con le prime versioni delle specifiche.

La comunicazione tra dispositivi NFC è basata su un “campo vicino” (near field), che è composto da campi elettrici e magnetici che, separatamente, non sono in grado di raggiungere lunghe distanze, ma possono essere rilevati solo nelle vicinanze del ricevitore. Poiché il tag non ha una fonte di alimentazione, comunica con il lettore modulando il proprio consumo di energia.

Lo stack protocol della tecnologia NFC, come mostrato nella figura successiva, è basato sugli standard ISO/IEC 14443 e FeliCa e includono ISO/IEC 18092 e quelli definiti da NFC Forum. In generale, l'architettura può essere suddivisa nei seguenti livelli:

- *Application layer*: si occupa del formato dei dati da scambiare tra dispositivi NFC e tra un dispositivo NFC e un tag. Il formato dei messaggi è basato su una struttura denominata NFC Data Exchange Format (NDEF);
- *Data link layer*: gestisce le diverse modalità operative di comunicazione e del meccanismo anti-collisione, al fine di evitare problemi in caso di trasmissioni dati da parte di più dispositivi nello stesso

tempo. Il protocollo Logical Link Control Protocol (LLCP) offre servizi sia connectionless sia orientati alla connessione, analogamente ai protocolli UDP (User Datagram Protocol) e TCP (Transmission Control Protocol);

- *Physical layer*: si occupa di modulazione, codifica e parametri relativi alla radiofrequenza, come frequenza, potenza, ecc.

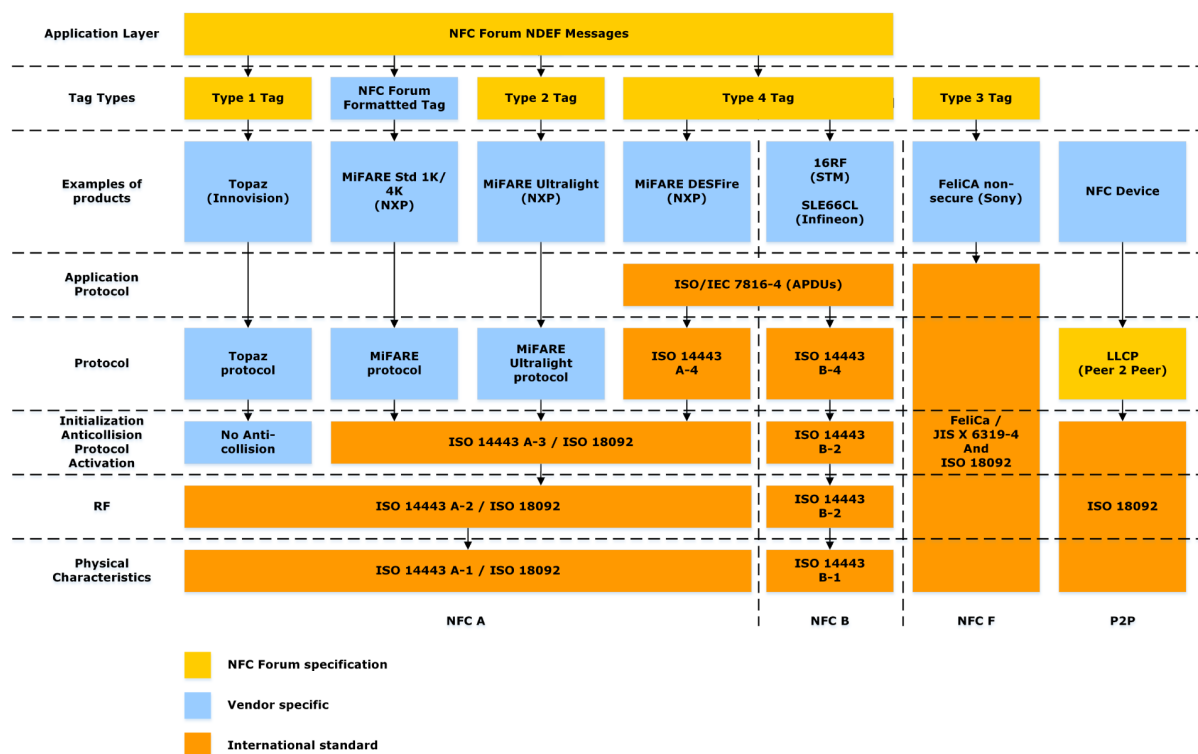


Figura 13. Stack protocol della tecnologia NFC

7. Ringraziamenti

Il presente lavoro è stato parzialmente finanziato dal progetto “Big Data Architecture for Personal Health Record”, presentato nell’ambito del Bando MISE grandi progetti R&S – PON, e “Realizzazione di servizi e strumenti a favore delle Pubbliche Amministrazioni per l’attuazione del Fascicolo Sanitario Elettronico”, oggetto di una convenzione tra l’Agenzia per l’Italia Digitale e il CNR. Si ringrazia la dott.ssa Rita Capasso per il supporto tecnico fornito.

8. Riferimenti bibliografici

- [1] Garante per la protezione dei dati personali, “Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario”, 2009, <http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116>
- [2] Ministero della Salute, “Il Fascicolo Sanitario Elettronico – Linee guida nazionali”, 2010, http://www.salute.gov.it/imgs/C_17_pubblicazioni_1465_allegato.pdf
- [3] Agenzia per l’Italia Digitale, “Linee guida per la presentazione dei piani di progetto regionali per il FSE”, 2014, http://www.agid.gov.it/sites/default/files/linee_guida/fse_linee_guida_31032014_dpcm_dt.pdf

- [4] Agenzia per l'Italia Digitale, "Documento di progetto dell'Infrastruttura Nazionale per l'Interoperabilità dei Fascicoli Sanitari Elettronici (art. 12 – comma 15-ter – D.L. 179/2012)", Circolare AgID n. 4/2017, 2017, http://trasparenza.agid.gov.it/moduli/downloadFile.php?file=oggetto_allegati/1724915213800_O04+-+AGID+CIRC+n.+04+-+01+ago+2017.pdf
- [5] Agenzia per l'Italia Digitale e Ministero della Salute, "Specifiche tecniche per l'interoperabilità tra i sistemi regionali di FSE", 2017, <https://www.fascicolosanitario.gov.it/linee-guida-manuali-documenti-tecnici>
- [6] Ministero della Salute, "Linee di indirizzo nazionali sulla Telemedicina", 2012, http://www.salute.gov.it/imgs/C_17_pubblicazioni_2129_allegato.pdf
- [7] European Union General Data Protection Regulation, <https://www.eugdpr.org/>
- [8] Tranfaglia, "Standard di integrazione in sanità DICOM e HL7", 2008, http://www.ingbiomedica.unina.it/studenti/ing_bioS/mat_did/TELEMED/telemed_031208.pdf
- [9] Health Level Seven International, <http://www.hl7.org>
- [10] Health Level Seven Italia, <http://www.hl7italia.it/>
- [11] Health Level Seven Version 2 Product Suite, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=185
- [12] Health Level Seven Version 3 Product Suite, https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186
- [13] Health Level Seven Clinical Document Architecture Release 2, http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7
- [14] Health Level Seven FHIR, <https://www.hl7.org/fhir/>
- [15] Health Level Seven Electronic Health Record-System Functional Model, Release 1, http://www.hl7.org/implement/standards/product_brief.cfm?product_id=18
- [16] Health Level Seven Retrieve, Locate, Update Service, Release 1, http://www.hl7.org/implement/standards/product_brief.cfm?product_id=89
- [17] Digital Imaging and Communications in Medicine, <http://dicom.nema.org/>
- [18] Pontiggia, "Sistemi di elaborazione dell'informazione radiologica", 2006, <https://www.ge.infn.it/~corvi/doc/didattica/radioprotezione/radiologia.pdf>
- [19] Integrating the Healthcare Enterprise, <https://www.ihe.net/>
- [20] De Gironimo, "IHE Technology Framework - Un modello di ottimizzazione della gestione dei dati clinici e integrazione tra le apparecchiature mediche in ambito di Cardiologia", 2012, http://amslaurea.unibo.it/3715/1/de_gironimo_simone_tesi.pdf
- [21] Integrating the Healthcare Enterprise Cross-Enterprise Document Sharing, http://wiki.ihe.net/index.php/Cross-Enterprise_Document_Sharing
- [22] Petronio, "Soluzione IHE per l'Electronic Health Record: studio e implementazione dell'attore XDS Registry per il progetto O3", 2006, http://bugbuster.altervista.org/files/Tesi_Petronio.pdf
- [23] Personal Connected Health Alliance, <http://www.pchalliance.org/>
- [24] ISO/IEEE 11073 Personal Health Devices, <http://www.11073.org/>
- [25] Integrating the Healthcare Enterprise Patient Care Device, https://www.ihe.net/Patient_Care_Devices/
- [26] Integrating the Healthcare Enterprise Patient Care Device Device Enterprise Communication, https://wiki.ihe.net/index.php/PCD_Profile_DEC_Overview
- [27] Integrating the Healthcare Enterprise Patient Care Device Rosetta Terminology Management, https://wiki.ihe.net/index.php/PCD_Profile_Rosetta_Terminology_Mapping_Overview

- [28] Health Level Seven Personal Healthcare Monitoring Report, Release 1, http://www.hl7.org/implement/standards/product_brief.cfm?product_id=33
- [29] USB Implementers Forum, Inc., <http://www.usb.org/about>
- [30] Bluetooth Special Interest Group, <https://www.bluetooth.com/>
- [31] ZigBee Alliance, <http://www.zigbee.org/>
- [32] NFC Forum <https://nfc-forum.org/>
- [33] “Profilo Funzionale di Fascicolo Sanitario Elettronico (FSE) regionale HL7 Italia”, 31 marzo 2014, disponibile http://www.hl7italia.it/sites/default/files/H17/docs/public/HL7Italia-PF_FSE_Regionale-v01.00-WP.pdf
- [34] M. Mercorella, M. Ciampi, M. Esposito, A. Esposito and G. De Pietro, “An Architectural Model for Extracting FHIR Resources from CDA Documents,” 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Naples, 2016, pp. 597-603
- [35] M. Ciampi, M. Sicuranza, A. Esposito, and G. De Pietro, “Progettazione e realizzazione di servizi per l’interoperabilità del Fascicolo Sanitario Elettronico mediante l’infrastruttura InFSE”, Istituto di Calcolo e Reti ad Alte Prestazioni del Consiglio Nazionale delle Ricerche, sede di Napoli, Technical Report no. RT-ICAR-NA-2015-04, data di pubblicazione Agosto 2015, disponibile su <http://www.na.icar.cnr.it/pubblicazioni/RT-ICAR-NA-2015-04%20.pdf>
- [36] M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, P. Donzelli, “A federated interoperability architecture for health information systems”, International Journal of Internet Protocol Technology, vol. 7, no. 4, pp. 189-202, 2013
- [37] M. T. Chiaravalloti, M. Ciampi, E. Pasceri, M. Sicuranza, G. De Pietro, R. Guarasci, “A model for realizing interoperable EHR systems in Italy”, in the proc. of the 15th International HL7 Interoperability Conference, pp. 13-22, 2015
- [38] M. Sicuranza, M. Ciampi, “A semantic access control for easy management of the privacy for EHR systems”, in the proc. of the Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), IEEE, pp. 400-405, 2014