SISTEMI DI CLOUD COMPUTING PER IL "TRIAGE" AUTOMATIZZATO DI PRONTO SOCCORSO: PROFILI E CRITICITA' DI CARATTERE TECNICO E LEGALE

Introduzione

L'Istituto Italiano per la Privacy, il CATTID de La Sapienza, Microsoft e il Centro Italiano per la Sanità Digitale hanno collaborato in questi mesi ad un progetto rivoluzionario ed estremamente avanzato, in grado di incidere fortemente sugli scenari dell'e-health nazionale e internazionale: si analizza la possibilità di rielaborare tutti i dati sanitari (sintomi, diagnosi, cure) dei pazienti dell'intero sistema sanitario nazionale, per poi generare – attraverso un sistema esperto appoggiato su piattaforma cloud – il "triage" dei pazienti che arrivano in pronto soccorso.

Il "triage" è un sistema di valutazione rapida dell'urgenza (normalmente declinata secondo i codici-colore bianco, verde, giallo, rosso): in base al risultato di "triage", il paziente sarà considerato in prima istanza più o meno grave, e seguirà uno specifico iter di cura interno al pronto soccorso.

Già oggi il sistema "triage" è utilizzato nei presidi di pronto soccorso: la differenza starebbe nella sua automatizzazione, grazie ad un "cervello informatico" in grado di rielaborare i miliardi di dati relativi a casi pregressi, per poi indicare quale potrebbe essere il codice-urgenza più probabile sulla base dei sintomi e delle altre informazioni raccolte nell'immediato dal paziente, nel singolo caso in esame in quel momento.

Questo progetto non mira ad escludere l'intervento umano del medico di first aid, ma solo ad adiuvarlo nella capacità di valutazione, in particolare in tutte le situazioni nelle quali – per ragioni organizzative, logistiche o fortuite – lo sportello di pronto soccorso risulti sottodimensionato o privo di competenze specializzate. Naturalmente,

il riuso e l'elaborazione di una mole così ampia e complessa di dati sarebbero resi possibili solo grazie all'adozione di una tecnologia di cloud computing.

Le problematiche affrontate nel lavoro sono sia di natura tecnologica, sia di carattere giuridico (si pensi ai temi della privacy dei pazienti e all'anonimizzazione dei dati sanitari). Lo studio, che viene pubblicato in italiano e in inglese, rappresenta un passo d'avanguardia in Europa per la ricerca giuridica e informatica sul tema, e può costituire un valido esempio per altre iniziative analoghe finalizzate alla valorizzazione del patrimonio informativo sanitario pubblico.

La prima presentazione dello studio si è tenuta il 5 dicembre 2012 a Bruxelles nell'ambito del convegno "Innovating for better health: doing New with Less". La presentazione italiana avverrà presso il Parlamento, a Roma, nel primo trimestre del 2013.

DATI SANITARI E CLOUD COMPUTING PER FINALITA' DI TRIAGE DI PRONTO SOCCORSO: PROFILI E CRITICITA' IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

(di Luca Bolognini, Diego Fulco, Enrico Pelino – Istituto Italiano per la Privacy – www.istitutoitalianoprivacy.it)

Scelte metodologiche e struttura della presente analisi giuridica

Il Progetto "Triage" opera su dati idonei a rivelare lo stato di salute (sinteticamente: "dati sanitari") riferiti a un numero rilevante di soggetti. Come tale, ha un'incidenza diretta sulla disciplina giuridica in materia di protezione dei dati personali. Di qui la necessità di analizzarlo alla luce della normativa suddetta, anche allo scopo di evidenziare quale possa essere la configurazione di minore impatto.

La scelta della *data minimisation* – questo è l'obiettivo – risponde da un lato a un vero e proprio obbligo di legge, espresso all'art. 3 del Codice privacy (d.lgs. 30 giugno 2003), e ulteriormente ribadito agli art. 5.c e 23 del nuovo Regolamento sul trattamento dei dati personali di prossima adozione a livello europeo, dall'altro si lega a considerazioni immediate e pratiche, connesse con un'opportuna economia giuridica e di mezzi nella gestione del Progetto.

All'esame e all'approfondimento di tali considerazioni sono dedicati i paragrafi che seguono.

La soluzione più adeguata – si vedrà – appare quella di utilizzare dati anonimi, e di farlo già nella fase iniziale del flusso informativo che alimenta il database centrale del Progetto, in modo da far circolare all'interno della struttura di cloud computing che fornisce la piattaforma informatica del sistema solo informazioni dissociate da una componente identificativa.

Tutto ciò ha naturalmente ripercussioni di un certo rilievo nella definizione della complessiva architettura del Progetto. Va registrato comunque, in senso positivo, che

la scelta di impostare il più possibile l'elaborazione su dati anonimi è stata già presa in considerazione dai partecipanti e si può dire che risponda perciò a un approccio condiviso.

Strutturalmente, il presente documento si articola in tre sezioni: una prima dedicata all'inquadramento in chiave giuridica degli elementi essenziali che compongono la fisionomia del Progetto, vale a dire: i flussi di dati, i soggetti coinvolti, le finalità; una seconda volta a esaminare in chiave generale il complesso dei profili giuridici, e con i essi le connesse difficoltà che il Progetto involge, avendo già in mente uno schema di massima delle scelte possibili per superare il livello di complessità che sarebbe altrimenti inevitabile: è in questa fase che si evidenzieranno le ragioni a supporto dell'utilizzo di informazioni rese anonime; una terza e conclusiva fase sarà dedicata al raffinamento della struttura e all'approfondimento di alcune questioni giuridiche conseguenti alle scelte strutturali adottate.

L'ultima parte evidentemente presuppone a monte una stabile definizione della struttura del Progetto e si presenta anche come la sede ideale per avanzare eventuali proposte di intervento normativo da sottoporre al vaglio del legislatore.

1. FISIONOMIA GIURIDICA MINIMA DEL PROGETTO TRIAGE

1.1 Obiettivi del Progetto e flussi di dati

Il Progetto si articola intorno a un'idea di base, quella di fornire indicazioni sanitarie utili e orientanti (più avanti definite sinteticamente "*output*") ai reparti di pronto soccorso nella fase di attribuzione dei codici cosiddetti "triage".

In sintesi estrema, si intende cercare una corrispondenza (*match*) tra elementi del quadro sintomatico e anamnestico del paziente di pronto soccorso ed elementi corrispondenti archiviati nel database del Progetto e riferiti a un numero considerevole di pazienti "storici". I dati dei pazienti storici sono collegati a determinate diagnosi, cosicché, attraverso un'elaborazione in chiave statistica o medico-statistica, i profili di tali diagnosi sono resi noti al personale di pronto soccorso, che di essi terrà dovuto conto nell'attribuzione dei codici *triage*.

In tal modo si potrà utilizzare una conoscenza collettiva, sedimentata nel database che raccoglie gli interventi medici precedenti, da reimpiegare nella fase di attribuzione dei codici di urgenza ai pazienti, fase che si caratterizza per una particolare immediatezza d'intervento e tempi contingentati.

L'utilità dell'*output* di Progetto consiste quindi nel migliorare l'efficienza e la tempistica della fase del *triage*, fornendo insieme al personale sanitario un utile strumento che integra la diagnosi e agli organismi sanitari una risorsa che contribuisca a ottimizzare l'organizzazione dei reparti di pronto soccorso.

La tecnologia che le parti hanno intenzione di utilizzare per lo *storage* dei dati che costituiscono il database, per il funzionamento generale del sistema e per la gestione dei flussi informativi è stata individuata, per ragioni di contenimento dei costi e di efficienza generale nelle prestazioni, in una tecnologia cloud. Ci si pone sul punto la questione delicata dell'allocazione dei ruoli privacy rispetto a questo cloud, ossia l'attribuzione della posizione di "titolare" e "responsabile di trattamento" ai soggetti coinvolti. Sul punto si tornerà più avanti.

Il database condiviso sarebbe costituito e alimentato da informazioni sanitarie provenienti dalle documentazioni di pronto soccorso già in possesso degli organismi sanitari pubblici e privati che partecipano al Progetto, e che sono definiti di seguito anche quali "*provider*".

È immediato perciò individuare due flussi di dati per ciascun *provider*: uno in entrata, dai pazienti di pronto soccorso al *provider*, uno in uscita, da quest'ultimo verso il database condiviso del Progetto.

Non sembrano invece ravvisabili flussi di dati per così dire "orizzontali", ossia da *provider* a *provider*. Se questo elemento fosse confermato, si otterrebbe il vantaggio di un'opportuna semplificazione in termini di schemi privacy applicabili.

Va poi individuato un terzo flusso di informazioni, quello per così dire "di ritorno", che dal database condiviso veicola l'*output* di Progetto ai singoli reparti di pronto soccorso, in modo che questi possano utilizzarli in raffronto con il quadro sanitario dei pazienti che di volta in volta accedono alla struttura.

Avendo in mente questo disegno essenziale del flusso informativo, è opportuno chiedersi se e in quale punto prevedere che il flusso suddetto sia costituito non da dati personali ma da dati anonimi.

Sembra opportuno, come meglio si argomenterà, collocare tale momento nella fase in cui il dato sanitario viene gestito dal *provider*, ossia prima che questi lo conferisca al database condiviso. Della trasformazione in forma anonima si occuperebbe perciò direttamente il *provider*, seguendo regole comuni rispetto a tutte le strutture partecipanti al progetto. Non appare invece concretamente possibile, ancorché desiderabile, un ulteriore arretramento del momento di utilizzo di dati anonimi.

La scelta di lavorare su dati anonimi comporta che eventuali correzioni delle informazioni dovute a una migliore definizione del quadro sanitario del paziente interessato non saranno di regola possibili dopo l'anonimizzazione. Occorre valutare sul punto l'impatto a livello medico-statistico. Insomma, la determinazione del passaggio in corrispondenza del quale utilizzare dati anonimi ha precise conseguenze anche di carattere scientifico sull'architettura del Progetto.

1.2 I soggetti coinvolti

Soggetti "attivi" di trattamento, ossia soggetti che svolgono attività di trattamento di dati riferibili a terzi, sono i *provider*. Può trattarsi di:

- organismi sanitari pubblici;
- organismi sanitari privati. Questi ultimi infatti, sia pure con differenze su base regionale, possono svolgere attività di pronto soccorso.

Ai sensi dell'art. 28 Codice va identificata come *provider* la struttura sanitaria nel suo complesso e non il singolo reparto di pronto soccorso. Ciò a meno che il reparto non eserciti un autonomo potere decisionale sul trattamento dei documenti di pronto soccorso.

Oltre ai *provider*, potrebbe essere individuato come soggetto attivo di trattamento l'eventuale entità centrale (sempre che vi sia) che si occupa della gestione del

database condiviso ed eventualmente anche della decisione sulle modalità di aggregazione e di elaborazione medico-statistica delle informazioni.

Naturalmente, se si sceglie – come appare preferibile e probabile – di far operare questo eventuale soggetto centrale su dati già anonimi, esso si collocherebbe al di fuori dell'applicazione della normativa in materia di tutela dei dati personali e dunque non potrebbe essere annoverato tra i soggetti "attivi" di trattamento. Ancora una volta è evidente l'impatto dell'anonimizzazione sull'architettura del Progetto.

A questo passaggio, e in generale ad un esame dei ruoli nel cloud, si riserverà comunque un maggiore approfondimento nel seguito.

Sono invece soggetti "passivi", ossia soggetti che "subiscono" le operazioni di trattamento svolte dai *provider*, i seguenti:

- pazienti di pronto soccorso che potremmo definire, per praticità, "storici", ossia persone fisiche che sono già state pazienti e alle quali è perciò già associata una documentazione di pronto soccorso. Sono propriamente la fonte da cui viene generato il primo flusso di dati personali, quello che alimenta le risorse informative del *provider*. Nella terminologia del Codice privacy si tratta di "interessati di trattamento", ossia soggetti ai quali i dati si riferiscono;
- pazienti destinatari della prestazione di pronto soccorso, che chiameremo anche nel prosieguo, ma solo per comodità, "pazienti attuali", poiché si tratta dei pazienti a cui viene attualmente somministrata l'attività di pronto soccorso e che sono quindi destinatari anche dell'*output* di Progetto. I pazienti attuali possono evidentemente essere sia pazienti storici che tornano in una struttura di pronto soccorso come anche pazienti nuovi. Il paziente "attuale" può diventare a sua volta paziente "storico" se i suoi dati sono raccolti e immessi nel flusso di Progetto.

La possibile dissociazione tra paziente storico, ossia interessato di trattamento, e destinatario di trattamento costituisce perciò un tratto saliente dell'architettura del Progetto. Si tratta di una caratteristica di interesse nell'analisi giuridica.

1.3 Finalità del Progetto

Il passaggio relativo alle finalità del Progetto può sembrare di minore rilevanza o al limite autoevidente. Così non è. In effetti, le finalità del trattamento rappresentano sempre un elemento di portata determinante nella disciplina giuridica in materia di dati personali.

Astrattamente, un progetto in ambito di eHealth può essere ricondotto, a seconda della specifica configurazione che gli viene data, a finalità diverse: di cura, di carattere amministrativo in ambito sanitario, di ricerca medica e medico-statistica.

È chiaro che la classificazione nell'una o nell'altra dipende concretamente dall'impostazione che si sceglie e dagli obiettivi che ci si pone.

In base alle informazioni fornite e ai colloqui avuti con il team medico che partecipa al progetto, sembra possibile nel caso di specie individuare essenzialmente due finalità, compresenti: una di integrazione della diagnosi sanitaria di pronto soccorso e una di ausilio nella programmazione e gestione dell'assistenza sanitaria fornita nei reparti di pronto soccorso, dunque finalità rispettivamente riconducibili agli artt. 85, co. 2 e 85, co. 1 Codice.

Stando alla visione attuale del Progetto, non è possibile indicarne una come prevalente.

Le finalità suddette rimandano a norme diverse e presentano scostamenti più o meno rilevanti nella disciplina applicabile, come si vedrà più oltre.

Deve ritenersi, almeno stando alla visione che attualmente è consentito avere del Progetto, che non siano invece perseguite finalità propriamente di ricerca. Infatti il Progetto non mira ad espandere la conoscenza medica, ma soltanto a rendere rapidamente disponibile un ricco campione di associazioni tra quadro clinico e diagnosi: si propone quindi semmai l'obiettivo di una mera velocizzazione dei tempi di decisione e quello di fornire agli operatori un ampio compendio delle diagnosi prospettabili con maggiore verosimiglianza, il tutto con vantaggi organizzativi per l'intero reparto e con maggiore efficienza nella gestione dei pazienti.

Nell'ipotesi, astratta, in cui dovessero emergere dall'*output* del Progetto indicazioni scientifiche suscettibili di arricchire lo stato della conoscenza, si tratterebbe perciò non di risultati cercati quanto piuttosto di scoperte occasionali.

Ugualmente, deve escludersi che il Progetto abbia la finalità di acquisizione di dati statistici, in quanto l'elaborazione statistica costituisce nella specie uno strumento piuttosto che una finalità.

Dovendo escludersi finalità direttamente statistiche e di ricerca scientifica in ambito medico, non si approfondirà nel seguito la peculiare disciplina ad esse collegata. Solo per completezza di analisi ci si limita a segnalare che l'emanando Regolamento europeo sulla protezione dei dati personali all'art. 81, co. 2 tratteggia, per linee sintetiche, il profilo di un'attività che presenta dei punti di contatto con quella del Progetto[1], classificandola nell'ambito statistico e scientifico. Si tratta a ben vedere di punti di contatto insufficienti ad attrarre il Progetto nell'orbita dei trattamenti per finalità scientifica o statistica. L'ipotesi comunque va tenuta sullo sfondo, anche alla luce dell'approfondimento giuridico che il Regolamento registrerà nei prossimi mesi.

2. QUESTIONI GIURIDICHE DI CARATTERE GENERALE INERENTI AL PROGETTO

Individuata in questi termini essenziali la fisionomia giuridica del progetto, il passaggio successivo, come anticipato, è quello dell'esposizione dei principali istituti giuridici richiamati e delle loro conseguenze più evidenti, incluse le difficoltà da superare. In chiave solutiva, si potrà apprezzare l'utilità apportata dalla scelta di operare su dati anonimi fin dal primo momento in cui ciò è possibile.

[1] Si confronti sul punto l'art. 81, co. 2 del Regolamento: *"Processing of personal data concerning health which uitis necessary for historical, statistical or scientific research purposes, such as patient registries set up for improving diagnoses and differentiating between similar types of diseases and preparing studies for therapies, is subject to the conditions and safeguards referred to in Article 83"*.

Sono essenzialmente tre le condizioni di liceità da osservare: informativa, consenso, autorizzazione del Garante. Mentre l'informativa è requisito di applicazione omogenea, consenso e autorizzazione sono legati a parametri variabili, quali la finalità perseguita con il trattamento e la natura privata o pubblica del *provider* sanitario.

Qui di seguito si procede all'analisi di tali elementi, nell'ordine dato.

A tal fine è utile premettere alcune considerazioni a proposito della dissociazione tra interessato e destinatario del trattamento sanitario. Tale dissociazione costituisce infatti un tratto caratteristico del Progetto e si salda a una precisa fisionomia normativa del Codice privacy. In definitiva la dissociazione si prospetta tutte le volte in cui il paziente di pronto soccorso sia terzo rispetto ai pazienti storici. Si presentano quindi in definitiva due schemi, a seconda che l'interessato di trattamento:

a) sia anche il soggetto diretto destinatario della prestazione medica di pronto soccorso;

b) non sia il soggetto diretto destinatario della prestazione medica di pronto soccorso.

Ci si riferirà nel prosieguo all'ipotesi a) come al "modello normale" o "modello associato", anche per contrapporla all'ipotesi b), che sarà indicata come il "modello dissociato", tutto ciò con l'avvertenza che non si tratta di terminologia del legislatore, ma soltanto di soluzione adottata qui per praticità di discorso. L'utilità di distinguere questi due modelli sta nel fatto che la disciplina normativa è per essi diversa.

2.1 L'obbligo di fornire l'informativa all'interessato e l'esercizio dei diritti dell'interessato

L'obbligo di fornire un'informativa agli interessati è previsto per tutti i trattamenti di dati personali e deve di regola essere assolto prima della richiesta di consenso, che si qualifica per questo come consenso "informato", ossia preceduto da una valida informativa.

Va tuttavia precisato che mentre tutte le volte in cui il consenso è richiesto occorre che questo trovi il supporto di un'informativa, non è vero necessariamente il contrario: ossia, l'informativa è dovuta anche quando il consenso non è richiesto. Come si

noterà tra breve, ad esempio, nel caso di finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria da parte di organismi sanitari pubblici il consenso non è richiesto, benché l'informativa risulti ugualmente dovuta.

Ciò perché l'informativa serve a dare contezza all'interessato di una serie elementi conoscitivi di fondamentale importanza, anche in vista dell'esercizio dei diritti riconosciuti al medesimo. Tra gli essenziali elementi conoscitivi che l'informativa deve apportare occorre annoverare i seguenti: l'identificazione del titolare del trattamento, la definizione dell'ambito di conoscenza dei dati, le finalità del trattamento, l'indicazione, come si è detto, dei diritti esercitabili.

Assolvere all'obbligo dell'informativa per i *provider* pubblici e privati, un'informativa evidentemente di carattere successivo e integrativo rispetto a quella fornita al momento dell'originaria raccolta, potrebbe però tradursi in un aggravio notevole di costi ed avere un impatto considerevole sull'organizzazione complessiva del Progetto.

Una possibile soluzione potrebbe essere ravvisata nell'applicazione dell'art. 13, co. 5, lett. c), che consente di prescindere dall'informativa cosiddetta "successiva" (ossia che interviene a trattamento già avvenuto) quando essa *"comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile"*. Si tratta in ogni caso di un provvedimento rimesso alle valutazioni di un soggetto terzo, l'Autorità garante.

Peraltro, si deve segnalare che la disposizione appena citata fa riferimento all'informativa resa da titolare diverso da quello che ha raccolto originariamente il dato presso l'interessato, caso che non collima con quello del *provider*.

Si vedrà più avanti che una valida soluzione può essere trovata piuttosto nella trasformazione in forma anonima dei dati sanitari.

2.2 Il requisito del consenso

Come si è osservato, l'obbligo o no di acquisire il consenso dipende dalla finalità del trattamento e dalla natura pubblica o privata del *provider*. Di seguito si tracceranno le linee del quadro applicabile, distinguendo tra finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria e finalità di cura, entrambe come si è detto compresenti nel caso in esame.

2.2.1 Finalità di programmazione, gestione, controllo e valutazione dell'assistenza sanitaria

Diversa disciplina seguono gli organismi sanitari pubblici e quelli privati. Quanto ai primi, ai sensi del combinato disposto degli artt. 20 e 85, co. 1 Codice, il trattamento dei dati sanitari viene effettuato senza il consenso dell'interessato, rientrando la finalità in esame tra quelle di rilevante interesse pubblico in ambito sanitario. In definitiva, l'unico incombente per i soggetti pubblici resta quello della fornitura di un'idonea informativa agli interessati.

Gli organismi sanitari privati, diversamente, per poter trattare dati personali per la finalità di cui sopra sono tenuti a raccogliere il consenso degli interessati. Devono inoltre procedere in base a previa autorizzazione dell'Autorità Garante. Come gli organismi pubblici, quelli privati sono tenuti a fornire un'idonea informativa.

2.2.2 Finalità di cura

L'analisi qui è più complessa perché tiene conto non solo della differenza tra organismo sanitario privato e pubblico ma anche delle diverse norme applicabili a seconda che ricorra il "modello dissociato" o quello "associato"

Partendo dal primo schema (dissociato: interessato e destinatario non coincidono), va detto che la disciplina applicabile si struttura per gli organismi pubblici e privati in maniera quasi del tutto analoga, pur collegandosi a disposizioni diverse del Codice privacy, e nonostante qualche differenza di formulazione[2]. I *provider* sanitari pubblici

[2] Per gli organismi sanitari privati è indicata una finalità di salvaguardia della vita e dell'incolumità del terzo, mentre per gli organismi sanitari pubblici una finalità di tutela della salute e

e privati non sono infatti tenuti a raccogliere il consenso dell'interessato ma devono necessariamente procedere con la previa autorizzazione dell'Autorità garante per la protezione dei dati personali.

Si applicano qui rispettivamente gli articoli 26, co. 4, b) e 76 del Codice. L'autorizzazione, sia per gli organismi privati sia per quelli pubblici, è al momento in cui si scrive la n. 2/2011.

Nel caso invece in cui ricorra identità tra interessato e destinatario della prestazione sanitaria, ossia quello che si è più sopra definito come "modello normale" o "associato" (per distinguerlo dal precedente), il quadro presenta più evidenti differenze tra organismi pubblici e privati [3], in quanto solo gli organismi privati hanno bisogno di una previa autorizzazione del Garante (al momento vale l'autorizzazione generale n. 2/2011), mentre entrambe le tipologie di *provider* sono tenute a richiedere il consenso dell'interessato[4] (art. 26 Codice per i privati; articolo 76, co. 1, lett. a e art. 85, co. 2 Codice per i pubblici). Tale consenso, in ipotesi di impossibilità fisica, incapacità di agire o di intendere e di volere può essere prestato da una serie di sostituti.

Per completare l'esame, va infine evidenziato come in ambito sanitario si applicano al consenso una serie di semplificazioni, che si innestano sulle più generali regole di cui all'art. 23 Codice. Vale la pena di passarle in veloce rassegna.

In applicazione delle regole generali, il consenso deve essere:

- espresso. Un consenso tacito, ad esempio per comportamento concludente, non è considerato sufficiente, almeno allo stato della disciplina attuale;
- libero, ossia privo di condizionamenti e pressioni psicologiche[5];

---

dell'incolumità del terzo. La differenza di formulazione, pure esistente, non va esagerata, anche in considerazione del fatto che trova un denominatore comune nel riferimento all'incolumità.

[3] La finalità è per entrambi quella della tutela della salute e dell'incolumità fisica.

[4] Si segnala che questa impostazione del legislatore differisce da quella del legislatore europeo, che all'art. 8.3 della Direttiva 95/46/EC aveva introdotto invece una deroga al consenso per l'attività preventive, diagnostiche, di cura, post-terapeutiche. Conforme invece la disciplina nazionale sull'attività di ricerca medica, che anche a livello europeo richiede il consenso. Cfr. sul punto Gruppo di lavoro ex art. 29 (è il gruppo dei Garanti europei), WP 131, p. 8.

[5] Cfr. Gruppo ex art. 29, *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE) sul fascicolo sanitario elettronico* 2007, p. 8, lett. *aa)*: *"Il consenso deve essere dato liberamente: consenso 'libero' significa una decisione*

- informato, ossia preceduto da un'informativa.

Per effetto delle regole specifiche applicabili al settore sanitario (cfr. art. 81 Codice), il consenso al trattamento dei dati sanitari può essere:

- espresso con unica dichiarazione per più trattamenti;
- rilasciato oralmente. Va registrata la deroga alla regola generale che impone la forma scritta per il consenso relativo a dati sensibili;
- annotato, in caso di espressione orale, da parte del titolare del trattamento, senza bisogno di ulteriori formalità per la sua documentazione.

Le semplificazioni suddette si applicano sia agli organismi sanitari privati sia a quelli pubblici.

2.3 L'autorizzazione del Garante

Il terzo requisito evidenziato è costituito dall'autorizzazione del Garante. Anche in questo caso ciò che incide sulla necessità di procedere con o senza previa autorizzazione è la diversa finalità e, in parte, la natura pubblica o privata del *provider*. Lo schema, che si è già visto, è il seguente:

- se la finalità è di carattere amministrativo, l'autorizzazione riguarda soltanto gli organismi sanitari privati;
- se la finalità è di cura, l'autorizzazione riguarda sempre gli organismi sanitari privati, e riguarda anche quelli pubblici nella sola ipotesi della dissociazione tra interessato e destinatario della prestazione.

Quanto alla qualificazione giuridica dell'autorizzazione del Garante, si può brevemente dire che si tratta di un atto amministrativo. Esso interviene al termine di una sequenza procedimentale che trae inizio dalla richiesta del titolare di trattamento e che si conclude con la decisione adottata dal Garante nel termine di quarantacinque

volontaria, presa da una persona in pieno possesso di tutte le sue facoltà e senza alcuna forma di coercizione, sociale, finanziaria, psicologica o d'altro tipo. Un consenso dato in una situazione medica sotto la minaccia di non essere curati o di ricevere cure peggiori non può essere considerato 'libero'. Il consenso dato da una persona che non abbia avuto la possibilità di fare veramente una scelta o che sia stata messa davanti al fatto compiuto non può essere considerato valido".

giorni, decorsi i quali la mancata pronuncia equivale a rigetto. L'Autorità garante può anche emettere autorizzazioni generali per categorie di interessati a norma dell'art. 40 Codice.

Come già notato, l'autorizzazione al momento vigente è quella generale n. 2/2011 del 24 giugno 2011, doc. web n. 1822577, valida fino al 31 dicembre 2012, che soddisfa pienamente le esigenze del Progetto.

2.4 La soluzione rappresentata dalla trasformazione in dati anonimi

Come appare dal quadro appena tracciato, le differenze di finalità e di natura pubblica o privata dell'organismo sanitario coinvolto determinano il richiamo di una disciplina molto articolata, nella quale sono evidenti i disallineamenti, le complessità e in ultima analisi i problemi di funzionamento che potrebbe subirne l'organizzazione del Progetto. In definitiva si pone un problema non irrilevante di costi e in generale di impegno di risorse organizzative per provvedere alla fornitura dell'informativa integrativa di quella già a suo tempo rilasciata e per la raccolta del consenso dell'interessato, nei casi in cui ciò sia richiesto. C'è poi il problema ulteriore di conciliare adempimenti che fanno capo – almeno per quanto è possibile evincere dal primo schizzo del Progetto – a due finalità compresenti.

Simili elementi di articolazione possono essere sciolti con il ricorso a dati anonimi. Al punto si è già fatto cenno più volte in precedenza ed è questa ora la sede per approfondirlo.

La trasformazione in dato anonimo del dato sanitario sarebbe rimessa direttamente ai *provider*, sulla base di regole omogenee condivise da tutti i partecipanti. Il successivo flusso da ciascuno di essi al database centrale sarebbe perciò formato da informazioni totalmente sganciate da qualsiasi collegamento con persone identificabili.

Nello specifico, l'anonimizzazione fa perdere di significato alla stessa individuazione delle finalità del trattamento, essendo irrilevante rispetto a dati anonimi l'utilizzo che si intende fare dell'informazione. Allo stesso modo, l'obbligo di fornire un'informativa o di raccogliere un consenso ha senso, e portata normativa, solo

rispetto a dati personali, non certo ad informazioni prive di collegamento con un soggetto identificato. L'orbita applicativa del Codice privacy coincide in definitiva con l'orbita stessa del dato personale.

Al più, in relazione all'informativa può porsi il problema, molto circoscritto invero, se quella inizialmente fornita al momento della raccolta del dato sanitario (ossia l'informativa ai pazienti "storici") dovesse menzionare espressamente la possibilità di rendere anonimo il dato e se, alla luce di ciò, essa vada opportunamente integrata.

A rigore, l'art. 13 Codice non prevede che l'informativa elenchi i trattamenti, ma solo le finalità e le modalità di trattamento, mentre la trasformazione in forma anonima dei dati personali va considerata come un trattamento[6]. Non si ritiene perciò necessario che l'informativa la indichi.

Nella parte speciale si approfondirà maggiormente il tipo di tecnica di anonimizzazione che il Progetto vorrà adottare, premettendo che l'anonimato, per essere tale, deve avere il carattere dell'irreversibilità. Tale scelta determina conseguenze che vanno apprezzate sul piano della funzionalità del Progetto e possono esserlo solo in un momento in cui lo schizzo iniziale andrà precisandosi e arricchendosi di dettagli.

Può ulteriormente porsi, in materia di trasformazione anonima del dato sanitario, il problema se sia o no consentito agli organismi sanitari pubblici partecipanti al Progetto procedere *tout court* ad una anonimizzazione dei dati. In particolare, può porsi la questione del coordinamento con l'art. 20 Codice, che consente a tali soggetti di effettuare un trattamento di dati sensibili solo in presenza di norma di legge che indichi i tipi di dati che possono essere trattati, le operazioni di trattamento eseguibili e le finalità di rilevante interesse pubblico perseguite.

A ben guardare il problema appare superabile, sol che si faccia riferimento all'art. 3 Codice. La norma in questione è dotata di immediato significato precettivo e dispone

[6] La trasformazione in forma anonima si compone di una serie di operazioni che sono tipicamente di trattamento: consultazione dei dati sanitari, selezione di quelli rilevanti per finalità di progetto, dissociazione da una copia di questi ultimi della sola componente informativa.

nei termini seguenti: *"I sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità"*. La regola trova peraltro un richiamo espresso e una sua specifica declinazione all'art. 94 Codice per le banche dati di dati idonei a rivelare lo stato di salute in ambito sanitario.

In altre parole, tutte le volte in cui il trattamento di dati sanitari avvenga attraverso sistemi informatici, ed è il caso di specie, per finalità che possono essere realizzate attraverso dati anonimi, ed è il caso di specie, la trasformazione dei dati in forma anonima non rappresenta una semplice opzione ma un obbligo di legge, al quale i soggetti pubblici (come quelli privati) sono tenuti.

Ulteriore questione, della quale ci si occuperà nella parte speciale di approfondimento, riguarda la possibilità che gli organismi pubblici considerino i dati sanitari anonimizzati del Progetto alla stregua di dati pubblici suscettibili di essere considerati nei termini della normativa sul riuso dei dati pubblici, ossia il d.lgs. 24 gennaio 2006, n. 36. La questione verrà esplorata in maggiore dettaglio una volta che saranno chiarite all'interno del Progetto le determinazioni relative all'eventuale riuso dei dati.

2.5 Ruoli privacy in un sistema di cloud e semplificazione derivante dall'utilizzo di dati anonimi

Occorre infine considerare il problema dell'allocazione dei ruoli attivi di trattamento in un sistema cloud. I ruoli in questione sono quelli di titolare di trattamento e di responsabile di trattamento, cui sono connessi profili di responsabilità diversa nel Codice privacy.

Sinteticamente, il titolare di trattamento è il soggetto apicale che effettua il trattamento, ossia quello che ne decide le finalità, le modalità e ha il potere di disegnare il quadro delle misure di sicurezza da adottare.

Il responsabile è un soggetto preposto dal titolare al trattamento e ogni sua decisione deve inserirsi nell'alveo delle scelte fatte a monte dal titolare. Ciò non toglie che il responsabile possa godere di un suo margine decisionale, pur entro la sfera di direzione e scelta che compete al titolare del trattamento. Va segnalato che nella pratica sorgono spesso difficoltà nell'individuazione dell'esatta linea di demarcazione tra responsabile esterno di trattamento (ossia esterno alla struttura del titolare) e titolare autonomo. L'analisi va condotta caso per caso, e – semplificando molto il discorso – si basa su una misura dei reali rapporti di forza tra le parti.

In grandi sistemi di cloud pubblici, il soggetto che fornisce il servizio, il *cloud service provider*, si trova spesso il condizione di forza contrattuale, come emerge dalla constatazione che è di regola il soggetto che decide il profilo della sicurezza del cloud e la configurazione tecnologica del medesimo. Il *cloud service provider* inoltre determina, per la parte che gli compete, le finalità del trattamento (ad es., la fornitura di un servizio di *storage* dei dati).

Ancora: il cliente spesso fruisce del servizio per mera adesione a un contratto rispetto al quale non ha rilevante possibilità negoziale. La diversità di forza contrattuale tra cliente e *cloud service provider* in sistemi molto complessi ed estesi si rivela anche nei limitati poteri di controllo e verifica che il cliente ha nei confronti del *cloud service provider*. In definitiva, pur con variazioni possibili caso per caso, tutti questi indici fanno ritenere corretto ravvisare nel *cloud pubblico* un modello articolato su due titolari autonomi di trattamento (cliente e CSP).

Discorso di segno opposto deve farsi di regola quando si consideri invece un cloud privato, ossia un cloud non aperto a tutti, ma anzi disegnato sulle esigenze di un particolare committente. In questo caso, i ruoli tendono a ribaltarsi e in linea di massima il *cloud service provider* andrebbe visto come responsabile di trattamento e il cliente come titolare di trattamento.

Ci si può porre ulteriormente il problema se i vari organismi che partecipano al Progetto siano tutti titolari autonomi o svolgano un trattamento congiunto.

Va tuttavia osservato che tutti questi problemi, come già anticipato, vengono a dissolversi, come viene a dissolversi l'interesse ad un loro approfondimento, ove i dati elaborati nel cloud siano tutti dati anonimi, non potendo in alcun modo prospettarsi, rispetto a questi ultimi, anche a livello teorico, un'allocazione di ruoli privacy.

Ancora una volta, l'utilizzo, già prospettato dai partecipanti al progetto, di dati anonimi abbatte in maniera decisiva le complessità giuridiche da affrontare.

2.6 Sintesi al termine della parte generale

Al termine di questa parte dello studio giuridico, pare opportuno sintetizzare brevemente i risultati dell'analisi condotta.

Innanzitutto, si è chiarito che le finalità del trattamento posto in essere con il Progetto sono di due ordini, e cioè finalità di cura (nel senso di velocizzazione e precisazione della diagnosi) e finalità di organizzazione e programmazione dell'assistenza sanitaria (nel senso di maggiore efficienza della medesima).

Si è inoltre individuato un tratto significativo del Progetto nella (possibile) dissociazione tra interessato del trattamento e destinatario della prestazione sanitaria, notando come tale dissociazione assuma rilievo nella disciplina che il Codice riserva al trattamento per finalità di tutela della salute. In particolare, nel caso che destinatario del trattamento sia un terzo, è consentita la deroga al consenso obbligatorio ed invece richiesta l'autorizzazione del Garante.

Consenso e autorizzazione subiscono un'inversione per i soggetti pubblici quando invece interessato e destinatario coincidano. Per gli organismi sanitari privati è richiesta, anche, la previa autorizzazione.

Il quadro muta ancora nel caso in cui la finalità di trattamento sia di carattere amministrativo, come è una finalità di organizzazione e programmazione dell'assistenza sanitaria.

In ogni caso, quale che sia la finalità, è necessario fornire un'informativa.

Emerge una disciplina complessa, che alterna elementi fissi (l'informativa) a elementi variabili (il consenso e l'autorizzazione), e comporta, in linea generale, l'allocazione di adeguate risorse.

La soluzione più lineare in chiave di semplificazione di costi, di organizzazione e di impatto giuridico è quella di utilizzare informazioni anonime già al momento in cui il flusso informativo viene diretto dai *provider* al database condiviso. In questo modo, ogni adempimento inerente al circuito di informazioni che sostanzia il Progetto viene a collocarsi al di fuori del perimetro del Codice privacy. Ciò vale evidentemente anche per l'intera configurazione del sistema di *cloud*, che verrebbe a operare su un database di informazioni completamente dissociate da una componente identificativa.

Non solo peraltro il ricorso a dati anonimi si tradurrebbe in un'economia giuridica e di risorse, ma costituirebbe per molti versi una strada obbligata, essendo richiesto da espressa norma di legge, l'art. 3 del Codice.

Se invece, in una successiva e più matura fase di evoluzione del Progetto si ritenga che rendere i dati sanitari irreversibilmente anonimi non soddisfi le esigenze sanitarie che si perseguono, si dovrà ritornare al quadro già tracciato nella prima parte della sezione generale di questo paper e dunque osservare il complesso reticolo di adempimenti già dettagliatamente segnalati. Il presente lavoro indica cioè una soluzione, pur lasciando aperta la possibilità di prescinderne, a seconda delle concrete necessità del Progetto.

Nella sezione che segue, la terza e l'ultima di questo lavoro, si approfondiranno i temi conseguenti a quelli appena esposti e in qualche misura definibili "di dettaglio". Ovviamente sarà possibile affrontarli solo dopo che la fisionomia tecnica del Progetto abbia ulteriormente acquistato in definizione. Si può anticipare comunque già da ora che i temi da approfondire riguardano, almeno, le seguenti aree:

- modalità e caratteristiche dell'anonimizzazione che sarà applicata dai partecipanti al progetto, compresi i profili connessi con l'irreversibilità del dato;
- valutazione circa l'opportunità di applicare misure di sicurezza a dati comunque anonimi;

- possibili utilizzi ulteriori dei dati di Progetto e in particolare valutazione giuridica delle prospettive che saranno affacciate in tema di riuso dei dati;
- eventuali proposte normative a livello nazionale o europeo.

IL RIUTILIZZO DEI DATI NEL SETTORE DELLA SANITÀ PUBBLICA: IL PROGETTO E-TRIAGE "TRIAGE ON THE CLOUD"

Francesco Bartoli, Carlo Maria Medaglia (C.A.T.T.I.D. Sapienza University Rome)

1. RACCOLTA REQUISITI

Introduzione

L'approccio seguito per definire le specifiche dei requisiti del sistema eTriage parte dall'identificazione dei concetti necessari per l'evoluzione dell'attuale sistema Triage adottato come modello di valutazione a priori dell'anamnesi del paziente. Saranno sviluppati i seguenti punti:

1. Identificazione dei potenziali attori e gruppi di utenti del sistema;
2. Raccolta dei fabbisogni e delle aspettative del sistema da un punto di vista funzionale, di sicurezza, di privacy e usabilità;
3. Formalizzazione dei requisiti e specifiche della piattaforma attraverso l'uso dello standard UML (Unified Modeling Language).

1.1 Categorie di Requisiti

I requisiti saranno classificati in categorie differenti in modo tale da semplificarne la gestione e valutarne la singola obbligatorietà o opzionalità.

Requisiti Funzionali sono definiti come l'insieme delle azioni e funzioni fondamentali che devono essere implementate dal sistema a partire da sorgenti di dati in ingresso in maniera da generare output appropriati.

Requisiti dei Dati sono definiti come l'insieme delle condizioni che debbono sussistere sul contenuto del dato e la sua semantica senza tenere in considerazione i

formati con cui vengono elaborati dal sistema eTriage. Si assume che essi siano indipendenti dalla tipologia di database che sarà utilizzato.

Requisiti di Interoperabilità specificano la capacità del sistema di condividere informazioni e servizi concentrandosi sulle interfacce che garantiscano l'interoperabilità verso sistemi esterni e agli standard che debbono essere supportati per mettere in pratica tale condizione.

Requisiti di Usabilità sono definiti come l'insieme delle caratteristiche che definiscono l'aspetto delle interfacce e la loro facilità d'uso e di apprendimento.

Requisiti di Operatività che specificano condizioni e livelli di performance ed esercibilità della piattaforma.

Requisiti di Sicurezza specificano tutti i fattori che debbono proteggere l'applicazione da modifiche, usi indesiderati, accessi dolosi o accidentali. Tra gli esempi ci saranno l'utilizzo di tecniche crittografiche, restrizioni delle comunicazioni, integrità dei dati, etc.

Requisiti Legali indicano tutta una serie di condizioni che regolino un adempimento delle norme di tutela della Privacy e di eventuali licenze o qualsiasi requisito attinente l'ambito della giurisprudenza.

1.2 Livello di necessità

Sono stati identificati tre livelli:

- ✓ **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
- ✓ **Condizionale** (Implica che tale requisito aumenterebbe il valore del sistema, ma non lo renderebbe inaccettabile nel caso sia assente)

- ✓ **Opzionale** (Implica che la funzione potrebbe o no essere di effettivo valore e consente di proporre qualcosa che ecceda i requisiti desiderati)

1.3 Stakeholder eTriage

Prima di procedere ad un attenta valutazione dei requisiti funzionali e alla loro specifica sono stati individuati tutti gli attori e i portatori di interesse del presente sistema. Particolare enfasi è stata data ai fornitori di dati (data provider) che in questo caso costituiscono il cuore del sistema. Infatti l'obiettivo funzionale di eTriage è proprio quello di mettere a fattor comune in modo organico le informazioni raccolte da questo gruppo di attori.

Il gruppo di utenti individuati come usufruitori dei dati (Data Retriever) e servizi eTriage sono stati catalogati come pazienti di telemedicina (teleassistenza domiciliaria), servizi di pronto soccorso ambulatoriale o mobile (ambulanze) e addirittura piccole strutture ospedaliere che non hanno specifici reparti.

L'ultimo gruppo di attori del sistema è costituito dagli amministratori (Admin) della piattaforma.

Nella realtà verrà contemplato nel modello concettuale del sistema e tra gli attori passivamente coinvolti nella definizione delle specifiche anche il Garante della Privacy in quanto soggetto indirettamente coinvolto nei processi di accesso ai dati sanitari.

1.4 Specifiche dei requisiti dalle indagini raccolte

1.4.1 Requisiti funzionali

1.4.1.1 RF1 – Dominio di applicazione

Categoria requisito	Requisito Funzionale
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)

Descrizione del requisito	Il sistema contemplerà solo ed esclusivamente i referti, ossia i dati clinici contenuti nelle documentazioni di Pronto Soccorso
Attore	Data provider, Data retriever
Motivazione	Il quadro sinottico aggregato di un referto costituirà uno strumento di valore statistico probante a una qualsiasi valutazione in sede di ingresso in Pronto Soccorso
Valutazione	Si ipotizza una semplificazione del modello che non contempli la storia delle Schede di Dimissione Ospedaliera SDO pregresse del singolo paziente
Autori del requisito	Francesco Bartoli (CATTID)

1.4.1.2 RF2 – Fornitura dei dati

Categoria requisito	Requisito Funzionale
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Il sistema sarà alimentato dalle fonti Triage dell'attuale sistema sanitario. Le fonti dovranno pilotare l'inserimento dei dati nel sistema eTriage attraverso delle interfacce di accesso ai dati dei pazienti depersonalizzati.
Attore	Data provider
Motivazione	Il dato sanitario è residente negli archivi dei data provider e non può essere condiviso liberamente unitamente all'associazione anagrafica
Valutazione	Le interfacce potrebbero essere messe a disposizione come web service o in modalità RESTful
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.2 Requisiti dei dati

1.4.2.1 RdD1 – Accessibilità Open Data

Categoria requisito	Requisito del Dato
Livello di necessità	(X) **Condizionale** (Implica che tale requisito aumenterebbe il valore del sistema, ma non lo renderebbe

	inaccettabile nel caso sia assente)
Descrizione del requisito	Il sistema esporrebbe un sottoinsieme dei propri dati pubblicamente accessibili con licenze Open Data
Attore	Data retriever
Motivazione	Alcuni sottoinsiemi del dato sanitario depersonalizzato possono essere forniti ai cittadini per conoscenza e servizi a valore aggiunto.
Valutazione	I dati potrebbero essere rilasciati secondo le licenze di tipo Creative Commons.
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.2.2 RdD2 – Paziente

Categoria requisito	Requisito del Dato
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Un paziente in eTriage è definito da una tupla che raccoglie i concetti di sintomatologia, osservazioni e accertamenti diagnostici, diagnosi, in modo da modellizzare l'analisi patologica nella prima fase di trattamento sanitario fino alla compilazione del referto di Pronto Soccorso
Attore	Data retriever
Motivazione	Il modello del paziente che giunge al pronto soccorso deve contemplare la storia della sua attuale malattia
Valutazione	
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.2.3 RdD3 – Referto Pronto Soccorso

Categoria requisito	Requisito del Dato
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Un referto di pronto soccorso dovrà contenere almeno le seguenti informazioni: insieme delle sintomatologie riportate dal paziente, l'insieme degli accertamenti diagnostici effettuati nel percorso di Pronto Soccorso, la diagnosi medica emessa in detta sede.
Attore	Data retriever
Motivazione	La storia della malattia corrente del paziente è limitata

	temporalmente al singolo evento di ammissione in Pronto Soccorso e concettualmente alle categorie di informazioni elencate sopra
Valutazione	Una qualsiasi persona si reca al Pronto Soccorso sofferente di alcuni sintomi, viene accettato e sottomesso ai dovuti accertamenti ed esami diagnostici, dopodiché viene stabilita una diagnosi medica di ammissione che eventualmente può evolvere in un ricovero o in trattamenti ambulatoriali o farmaceutici
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.2.4 RdD4 – Codifica referti Pronto Soccorso

Categoria requisito	Requisito del Dato
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	La codifica dei dati clinici contenuti nei referti di Pronto Soccorso dovrà seguire lo standard ICD-9-CM già imputato alle Schede di Dimissione Ospedaliera SDO
Attore	Data retriever
Motivazione	Armonizzazione dell'evoluzione nella storia ospedaliera del paziente fino alla SDO e univocità nel contemplare la classificazione delle malattie e delle diagnosi riconosciuta in campo internazionale.
Valutazione	La struttura dell'ICD9-CM prevede quattro sezioni principali di cui 2 relative alla classificazione delle malattie (codici di diagnosi): • indice alfabetico delle malattie e dei traumatismi • elenco sistematico delle malattie e dei traumatismi ed altre 2 relative alla classificazione delle procedure diagnostiche e terapeutiche: • indice alfabetico degli interventi chirurgici e delle procedure diagnostiche e terapeutiche • elenco sistematico degli interventi chirurgici e delle procedure diagnostiche e terapeutiche

	Inoltre sono presenti due classificazioni supplementari: • la classificazione supplementare dei fattori che influenzano lo stato di salute ed il ricorso alle strutture sanitarie (codici V) • la classificazione supplementare delle cause esterne di traumatismo e avvelenamento (codici E)
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.3 Requisiti d'interoperabilità

1.4.3.1 RdI1 – Formato dei dati in output

Categoria requisito	Requisito d'Interoperabilità
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Il sistema espone i dati attraverso interfacce web service e API Restful con formati XML/JSON
Attore	Data retriever
Motivazione	Garantire l'interoperabilità per l'accesso e il riuso dei dati di trattamento sanitario di Pronto Soccorso.
Valutazione	Si può accedere al dato strutturato o a servizi specifici sempre attraverso il Web.
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.3.2 RdI2 – Formato dei dati in input

Categoria requisito	Requisito d'Interoperabilità
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Il sistema dovrà accettare i dati pilotati dalle fonti attraverso interfacce web service e API Restful con formato rispettoso del protocollo standard di scambio dati in ambito clinico HL7
Attore	Data provider
Motivazione	Garantire l'interoperabilità e l'utilizzo d'interfacce

	comuni secondo le normative standard in vigore sullo scambio di informazioni cliniche.
Valutazione	L'utilizzo di HL7 lascia campo aperto verso successive evoluzioni e adeguamenti normativi che la materia sanitaria potrà subire dal punto di vista dell'Information Technology per la fase di Pronto Soccorso
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.3.3 RdI2 – Formato dei dati in input

Categoria requisito	Requisito d'Interoperabilità
Livello di necessità	(X) **Opzionale** (Implica che la funzione potrebbe o no essere di effettivo valore e consente di proporre qualcosa che ecceda i requisiti desiderati)
Descrizione del requisito	Il sistema dovrà definire un HL7 CDA (Clinical Document Architecture) del referto di Pronto Soccorso
Attore	Data provider
Motivazione	Garantire l'interoperabilità e l'utilizzo d'interfacce comuni secondo le normative standard in vigore sullo scambio di informazioni cliniche.
Valutazione	Un gruppo di lavoro per definire a livello nazionale un profilo di interoperabilità definito normativamente nelle strutture di Pronto Soccorso
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.4 Requisiti di usabilità

Non applicabili

1.4.5 Requisiti di operatività

1.4.5.1 RdO1 – Hosting del sistema

Categoria requisito	Requisito di Operatività
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Il sistema dovrà essere ospitato come servizio Cloud su architettura Microsoft SQL Azure
Attore	Data Retriever
Motivazione	Microsoft SQL Azure garantisce un'architettura innovativa e servizi per l'usufruizione del dato da parte di dispositivi eterogenei i quali necessitano di disponibilità e

	accessibilità 24h/7d
Valutazione	SQL Azure può esporre servizi basati sui dati archiviati nel corrispondente database.
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.6. Requisiti di sicurezza

Non applicabili

1.4.7 Requisiti legali

1.4.7.1 RL1 – Paziente depersonalizzato

Categoria requisito	Requisito Legale
Livello di necessità	(X) **Essenziale** (Implica che il sistema non potrà essere accettato a meno che il requisito sia implementato nella maniera concordata)
Descrizione del requisito	Il sistema dovrà accettare dalle fonti dei dati in origine (data provider) solo quadri sinottici depersonalizzati dall'identità anagrafica del paziente al momento prevista nell'attuale sistema sanitario nazionale.
Attore	Data provider
Motivazione	Il dato sanitario costituisce un dato sensibile ai sensi della legge sulla Privacy
Valutazione	Il paziente in eTriage può essere pensato come un concetto slegato dall'identità anagrafica
Autori del requisito	• Francesco Bartoli (CATTID)

1.4.7.2 RL2 – Referto di Pronto Soccorso

Categoria requisito	Requisito Legale
Livello di necessità	(X) **Condizionale** (Implica che tale requisito aumenterebbe il valore del sistema, ma non lo renderebbe inaccettabile nel caso sia assente)
Descrizione del requisito	Il referto di Pronto Soccorso dovrà essere compilato secondo la codifica delle diagnosi e delle procedure utilizzando la classificazione ICD-9-CM.
Attore	Data provider
Motivazione	Il referto di pronto soccorso è un atto pubblico con valenza probatoria (art 2700 cc) che contiene informazioni utili a dimostrare la veridicità di quanto riportato al medico in occasione dell'accesso e riporta dati anamnestici, obiettivi, diagnostico strumentali e

	prognostici

Valutazione

Autori del requisito	• Francesco Bartoli (CATTID)

2 ARCHITETTURA ETRIAGE

L'architettura del sistema eTriage si prefigge di utilizzare i dati collezionati nelle strutture ospedaliere e di servirli in modo anonimo per offrire servizi di teleassistenza nella fase di primo intervento ed emergenza soprattutto in quei piccoli ospedali e nelle ambulanze dove sono prestate le prime cure, che a volte risultano decisive nell'efficacia del trattamento patologico. A tendere lo scenario dei possibili utenti serviti dal sistema "evolved Triage" potrebbe evolvere coinvolgendo anche i grandi ospedali e offrire teleassistenza medica a domicilio.

eTriage prevede di ospitare questa enorme banca dati in un sistema Cloud che sia trasparente all'identità personale dei pazienti in modo da tutelare la loro privacy e rendere la natura delle informazioni possedute dal sistema totalmente prive di alcuna limitazione dovuta alla sensibilità del dato.

I data provider delle informazioni resterebbero gli ospedali che partecipano al pilota dove localmente rimangono confinate le identità personali dei pazienti che hanno subito trattamenti ospedalieri. In tal modo sarà disaccoppiato il concetto di identità personale da quello di paziente di una struttura ospedaliera.

L'architettura generale sarebbe quella della figura sottostante:

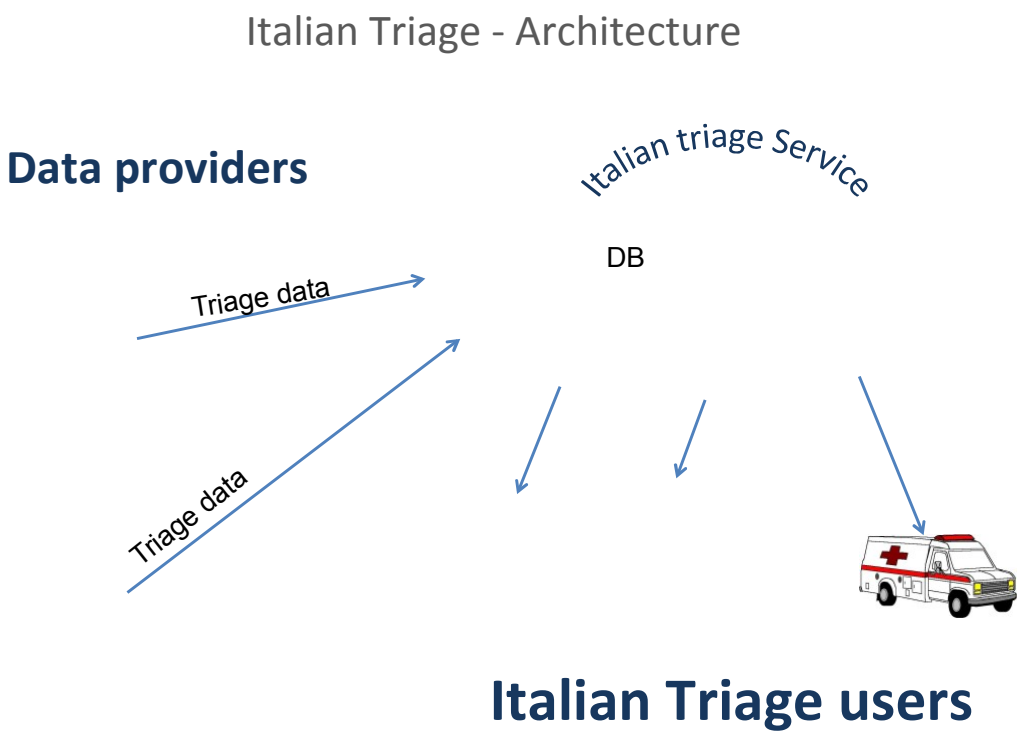

Figure Architettura generale Triage

2.1 Modello concettuale

Dal punto di vista concettuale il disegno del sistema deve sviluppare il modello di paziente come una triade di concetti strettamente sanitari slegati dall'identità anagrafica per contemplare la riutilizzabilità del dato sanitario senza incontrare vincoli ostativi al trattamento di dati sensibili secondo la norma giuridica italiana.
Il concetto cardine alla base di questo modello è il seguente:

Un paziente non possiede un'identità anagrafico-giuridica

Ciò consente di focalizzare l'attenzione sulle prime fasi di intervento (Pronto Soccorso) sulla patologia di un potenziale paziente e delineare quelli che sono i concetti e le relazioni che delineano il suo quadro clinico. Il modello logico funzionale descrive questi concetti basilari:

- ✓ Un paziente ha una sintomatologia
- ✓ Un paziente ha una serie di parametri vitali e sanitari che possono essere analizzati attraverso determinati accertamenti diagnostici
- ✓ Un paziente riceverà una diagnosi

Questo è lo scenario che mostra il modello logico funzionale di un paziente ogni qual volta un soggetto si reca in una struttura ospedaliera per ricevere delle cure di primo soccorso in relazioni a sintomi emersi. In questa situazione una qualunque persona è declinata in un paziente e in particolare nel modello appena descritto.

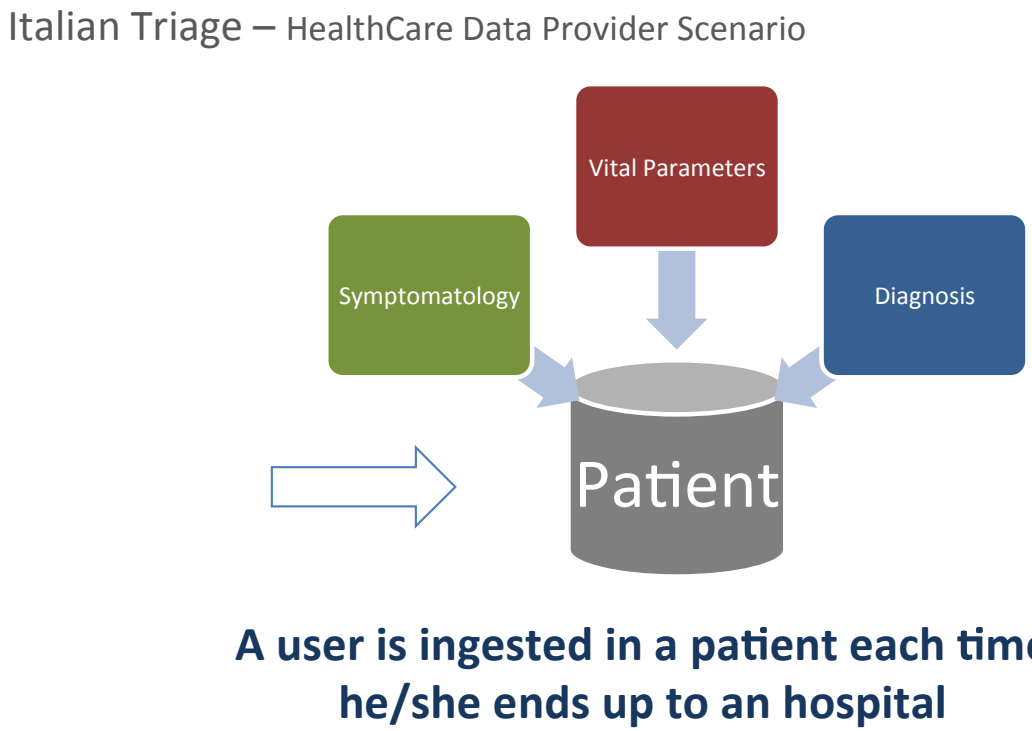

Figure Modello concettuale di un paziente

E' importante rilevare come il modello ben si sposa con lo scopo di fornire servizi nella fase embrionale di un intervento in Pronto Soccorso. Ciò significa che i concetti presi in considerazione sono quelli formalmente indicativi per stabilire l'identificazione della natura di una sintomatologia sebbene una malattia possa produrre successivi nuovi sintomi e non manifestarsi in maniera chiara sin da subito. Infatti, è evidente come il modello appena descritto sia fondamentalmente legato al tempo e alla storia del paziente e quindi come la diagnosi sia un fattore che può variare nel tempo rispetto alla corrente sintomatologia ma anche alle storie precedenti dello stesso paziente.

Al momento si presume di trattare un modello semplificato, poco dipendente dal tempo, che racchiuda solo l'associazione concettuale di una singola storia sanitaria di Pronto Soccorso di un paziente. Il Cloud eTriage fornirà valore aggiunto derivato dall'unione di questi tre concetti in virtù di un'architettura distribuita sulle sorgenti di dati Triage riferiti ai referti di Pronto Soccorso in modo da fornire servizi di consultazione rapida per una valutazione patologica di massima (suggerimenti diagnostici) secondo la codifica standard delle malattie che già è utilizzata per le SDO.

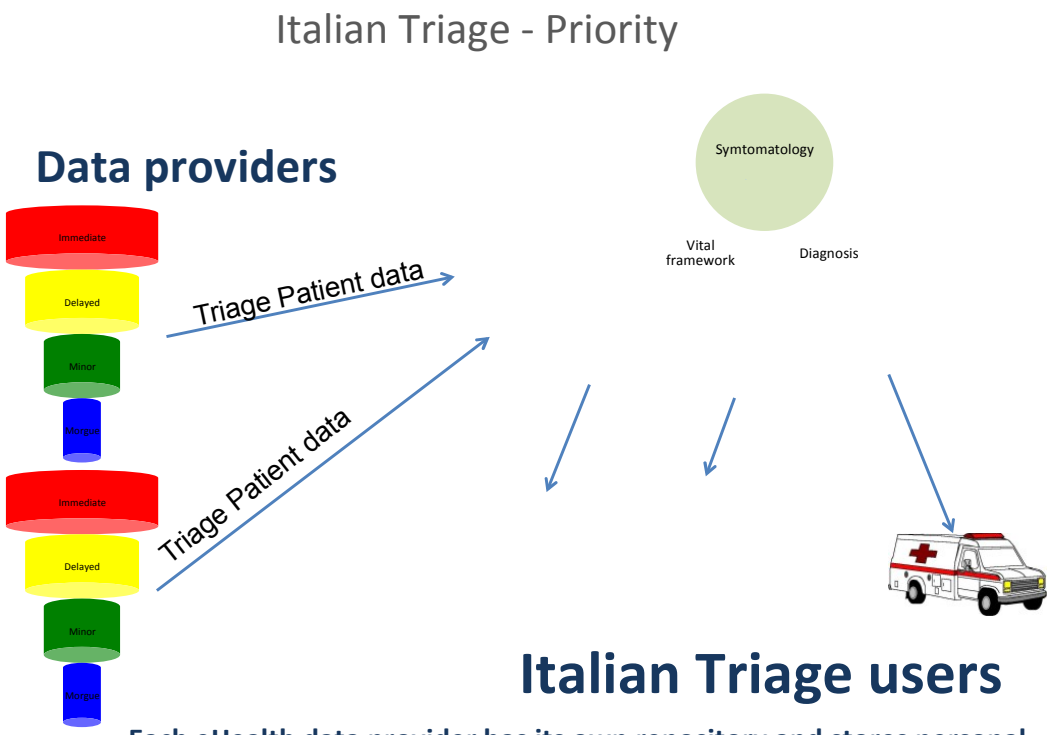

Figure Modello servizi Triage e loro integrazione in eTriage

Il modello dei dati che sarà individuato avrà inoltre un bagaglio di informazione aggiuntiva in quanto collega ogni singola storia dei pazienti alla priorità con cui si è intervenuti nella fase preliminare di valutazione patologica, evidenziando di fatto la priorità di intervento non sulla singola codifica di diagnosi ma sul quadro sinottico aggregato delle informazioni di Sintomatologie, Accertamenti diagnostici, Diagnosi.
Al momento la classificazione di un'ammissione, infatti, è regolata da una scala piramidale (e un corrispondente colore) in base alla priorità di intervento:

- ✓ Urgente (colore rosso)
- ✓ In attesa (colore giallo)
- ✓ Modesta (colore verde)
- ✓ Insignificante (colore blu)

2.2 Classificazioni e Standard utilizzati

2.2.1 Sistema di classificazione nella sanità italiana

Il sistema attualmente riconosciuto e adottato dal Ministero della Salute è quello della Classificazione internazionale delle malattie (ICD) che organizza le malattie ed i traumatismi in gruppi sulla base di precisi criteri.

La classificazione è approvata in ambito internazionale e riconosciuta dal 1979 con la sigla ICD-9-CM nella versione ampia che include anche gli interventi e le procedure diagnostiche.

In Italia a partire dal primo gennaio 2009 viene adottata su tutto il territorio nazionale la versione 2007 di ICD-9-CM per declinare le informazioni cliniche rilevate nella Scheda di Dimissione Ospedaliera sia per la codifica delle diagnosi, principali e secondarie, sia delle procedure, anch'esse principali e secondarie.

Visti i vantaggi di uniformità e armonizzazione di cui potrebbe beneficiare tutto il processo della filiera ospedaliera si è scelto di utilizzare la predetta codifica ICD-9-CM anche nel modello di codifica di un referto di Pronto Soccorso su sistema eTriage.

2.2.3 Protocolli di comunicazione

Sul fronte dello scambio dati in ambito sanitario è stato preso in esame HL7 che risulta essere lo standard per la comunicazione di messaggi più diffuso internazionalmente nel settore dell'ICT sanità: esso descrive le interfacce tra applicazioni diverse, le definizioni dei dati da condividere, nonché gli eventuali stati di preclusione nella comunicazione.

Lo scopo di tale protocollo risiede soprattutto nel comunicare le informazioni relative ad un paziente tra applicazioni diverse rendendo le varie entità del mondo sanitario interoperabili nel trattare i dati clinici.

Tale scelta presuppone di lasciare ampio spazio all'integrazione di un numero illimitato di data provider rendendo flessibile il processo secondo un meccanismo di tipo plug&play.

L'unico vincolo di riconducibilità alla fonte dati sarà quello di prevedere nelle modalità che saranno stabilite nella modellazione delle interfacce generali del nosologico relativo alla singola struttura ospedaliera.

2.3 Implementazione Database eTriage

2.3.1 Modello logico

La progettazione della base dati ha tradotto l'analisi dei requisiti soprastanti per la gestione dei dati di una cartella clinica di pronto soccorso in modo da organizzarla nel modello logico che proponiamo di seguito:

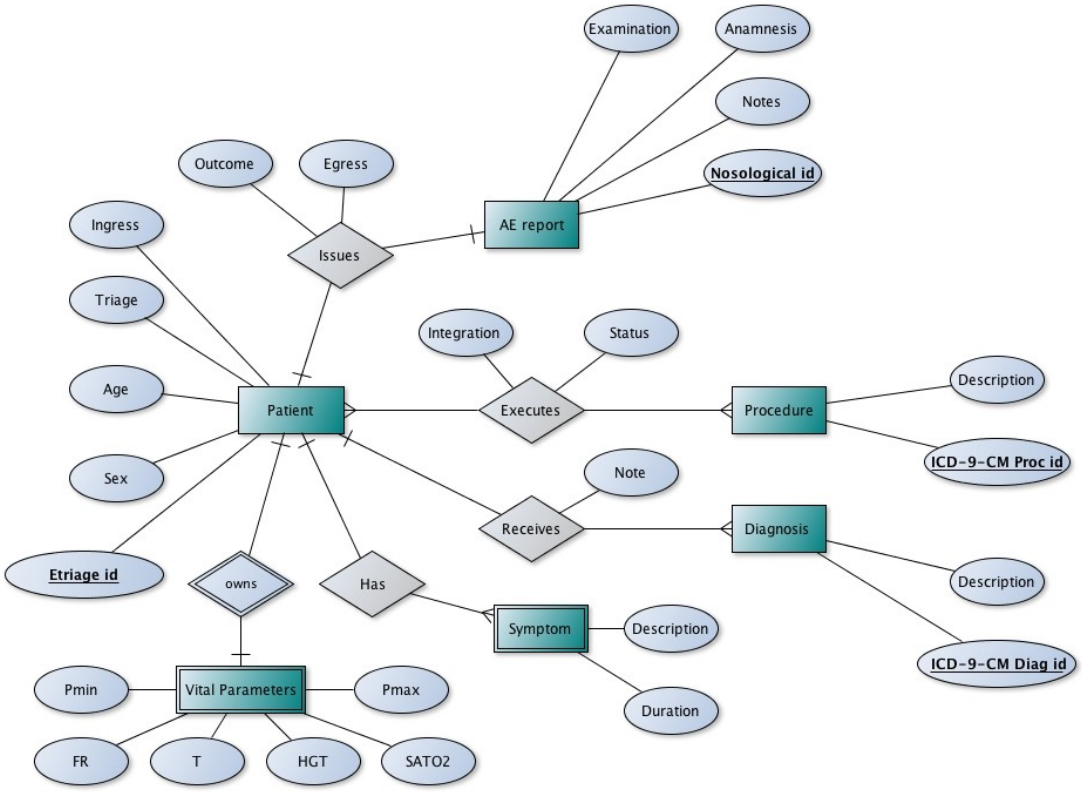

Figure Modello logico della base dati eTriage

Nella figura è possibile notare in verde le entità coinvolte nella modellazione tra cui le principali:

- Il paziente come elemento cardine della struttura che viene descritto dalle informazioni rilevanti ai fini della cartella di Pronto Soccorso senza alcun riferimento ai dati personali;
- La scheda del trattamento di Pronto Soccorso associata a ciascun paziente;
- Le procedure eseguite secondo la codifica ICD-9-CM;
- La diagnosi ricevuta secondo la codifica ICD-9-CM.

2.3.2 Codifica ICD-9-CM

Nella trasposizione del modello concettuale la tassonomia delle codifiche ICD-9-CM è stata predisposta di sana pianta dalla struttura ufficiale con cui è organizzata dal Ministero della Salute. Nella figura sottostante vediamo il prospetto del modello in opera sul database di SQL Azure:

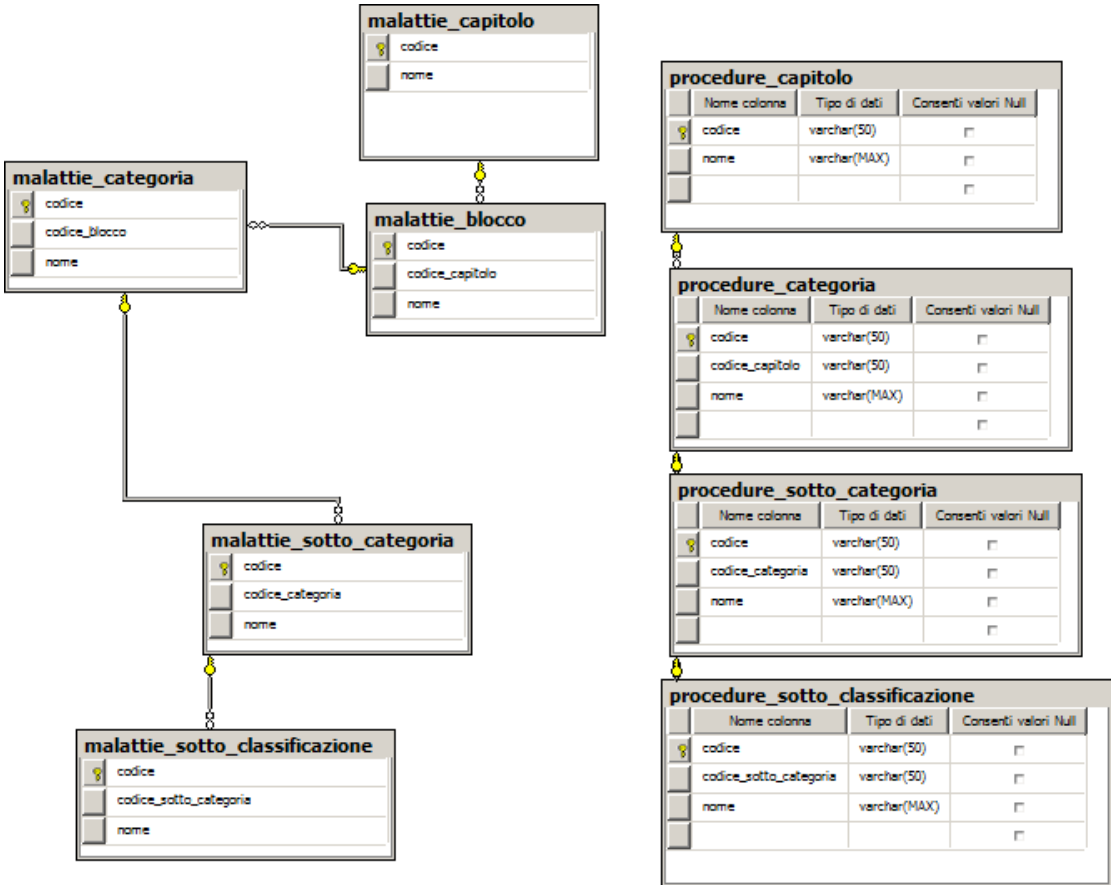

Figure Organizzazione codifiche delle malattie e procedure ICD-9-CM

2.4 Implementazione Servizi eTriage

2.4.1 Windows Azure

Windows Azure è una piattaforma cloud aperta e flessibile che consente di compilare rapidamente, distribuire e gestire applicazioni attraverso una rete globale di data center gestiti da Microsoft. È possibile compilare applicazioni utilizzando qualsiasi linguaggio, strumento o framework. Le funzionalità e i servizi sono esposti utilizzando protocolli REST. È inoltre possibile integrare le applicazioni cloud pubbliche con l'ambiente IT esistente.

Windows Azure offre un contratto di servizio mensile del 99,95% e permette di compilare ed eseguire applicazioni a elevata disponibilità senza concentrarsi sull'infrastruttura. Fornisce l'applicazione di patch automatica al sistema operativo e ai servizi, bilanciamento del carico di rete predefinito e resilienza agli errori hardware. Supporta un modello di distribuzione che consente di aggiornare l'applicazione senza tempi di inattività.

Con Windows Azure è facile scalare le applicazioni a qualsiasi dimensione. È una piattaforma self-service completamente automatizzata tramite cui è possibile fornire risorse in pochi minuti. L'utilizzo delle risorse può essere adattato con flessibilità alle proprie esigenze. Si paga solo per le risorse utilizzate dall'applicazione. Windows Azure è disponibile in più data center logici in tutto il mondo, consentendo di distribuire le applicazioni nell'area in cui si trovano i clienti.

2.4.2 Windows Azure Architecture

L'architettura di Windows Azure è stata realizzata per offrire servizi on-demand basati sul cloud. L'infrastruttura è dislocata in diversi data center posizionati negli Stati Uniti, Europa e Asia, ed è basata sulla virtualizzazione delle risorse fisiche come CPU e memoria. Ciò permette di ottenere vantaggi in termini sia di scalabilità verticale sia di scalabilità orizzontale. Nel primo caso è possibile decidere di aumentare le risorse disposizione, come CPU e memoria, nel secondo caso è possibile aumentare o diminuire le istanze applicative a seconda delle esigenze.

Windows Azure offre differenze modalità di utilizzo del cloud:

- *Windows Azure Storage Services*: fornisce un infrastruttura per l'archiviazione persistenze e durevole dei dati strutturati e non strutturati;
- *Windows Azure Hosted Services*: l'ambiente di esecuzione delle applicazioni;

- *Windows Azure platform AppFabric*: un insieme di servizi per la creazione di applicazioni distribuite utilizzabili anche da soluzioni ibride nel cloud e *on premisise*.
- *SQL Azure*: una versione di SQL Server adatta per essere eseguita in un ambiente di cloud computing.

2.4.3 Windows Azure Storage Services

È il servizio di archiviazione dei dati in modo persistente e durevole. Tale servizio è accessibile da qualsiasi tipo di applicazione anche se non è in distribuita nel cloud di Windows Azure, ma in esecuzione on-premise. I Windows Azure Storage sono suddivisi in tre principali tipologie:

- *Table Storage Services*, permette di memorizzare entità applicative in forma tabellare;
- *Blob Storage Services,* dedicato alla memorizzazione di file binari come documenti o immagini;
- *Queue Storage Services,* per la creazione di code di messaggi scambiati tra i componenti di una soluzione;
- *Drive Storage Services*, consiste in un drive NTFS che fornisce le funzionalità di un completo file system remoto.

Tutti questi servizi sono raggiungibili tramite URI che identificato univocamente le specifiche risorse.

2.4.4 Windows Azure Computing: Hosting Services

In Windows Azure è possibile sviluppare qualsiasi tipologia di applicazione Web o di back-end sviluppata con tecnologie .NET, JAVA e PHP per citare le principali.
In Windows Azure queste applicazioni vengono definite Hosted Services e si suddividono in due diverse tipologie, o ruoli con compiti ben definiti: Web Role e Worker Role.

Un'applicazione di tipo Web Role è sostanzialmente un applicativo web, distribuita su piattaforma Windows Azure, il cui compito è interfacciarsi verso i client, utenti finali o altri sistemi.

Al contrario di un Web Role un applicativo di tipo Worker Role ha lo scopo di lavorare in background, offrendo il massimo disaccoppiamento in termini di ricezione ed elaborazione dei dati. Questa tipologia di applicativi non offrono nessun tipo di interfaccia verso client.

2.4.5 WCF Data Services

WCF Data Services (precedentemente noto come "ADO.NET Data Services") è un componente di .NET Framework che consente di creare servizi che si basano su OData (Open Data Protocol) per esporre e utilizzare dati sul Web o su Intranet tramite la semantica REST (Representational State Transfer). In OData i dati sono esposti come risorse indirizzabili tramite URI. Per accedere ai dati e apportarvi modifiche è possibile utilizzare i verbi HTTP standard GET, PUT, POST e DELETE.

WCF Data Services utilizza il protocollo OData per l'indirizzamento e l'aggiornamento delle risorse. In questo modo, è possibile accedere ai servizi da qualsiasi client che supporti OData . OData consente di richiedere e scrivere dati nelle risorse utilizzando formati di trasferimento noti, ovvero JSON (JavaScript Object Notation), un formato per lo scambio di dati basati su testo ampiamente utilizzato nelle applicazioni AJAX, e Atom, un set di standard per lo scambio e l'aggiornamento di dati come XML.

2.4.6 OGDI

Open Government Data Initiative (OGDI) è un'iniziativa guidata da Microsoft Public Sector Developer Evangelism team. OGDI utilizza la piattaforma Windows Azure per facilitare la pubblicazione e l'utilizzo di un'ampia varietà di dati pubblici degli enti governativi. OGDI è una soluzione open source "starter kit" che può essere utilizzato per pubblicare i dati su Internet in formati Web tramite API aperte e facili da utilizzare. È possibile accedere all'interfaccia applicativa OGDI da una varietà di tecnologie client come Silverlight, Flash, JavaScript, PHP, Python, Ruby, etc.

2.4.7 *Interrogare il servizio dati*

Il servizio espone i dati in modalità REST. La sintassi base di una query al servizio è la seguente http://***[project]***.cloudapp.net/v1/***[container]***/***[dataset]***?***[query]***, dove:

- *project* è il nome del progetto esposto su Azure (es. etriage)
- *container* è il nome del contenitore dei dati (per esempio, "ICD9CM" per i dataset riguardanti il sistema di classificazione ICD9-CM).
- *dataset* è il nome del dataset (per esempio, "Diagnosi" per il dataset delle Diagnosi appartenente al contenitore di eTriage).
- *query* è l'insieme dei parametri di interrogazione, espressi utilizzando un sottoinsieme della sintassi WCF Data Services query syntax.

Il servizio dati supporta unicamente i parametri di interrogazione $filter e $top.

Formato dati

AtomPub
Per default, il servizio dati restituisce i dati nel formato Open Data Protocol (OData) . Questo formato estende il formato Atom Publishing Protocol largamente adottato, e può essere facilmente letto da diverse piattaforme, incluse Microsoft .NET, Java, Ruby, PHP, e Python.

JSON
Il servizio dati può restituire dati in formato JavaScript Object Notation (JSON) , facilmente interrogabile attraverso JavaScript e altre tecnologie. Per restituire i dati

nel formato JSON, aggiungere nella query string il parametro format=json. Ad esempio:

http://etriage.cloudapp.net/v1/ICD9CM/Diagnosi/?$filter=name eq 'Colera' &format=json

RDF

Il servizio dati può restituire i dati in formato RDF (Resource Description Framework). RDF modello a grafo per descrivere formalmente le risorse web e le loro associazioni. Sviluppato da W3C, RDF si basa su un linguaggio semantico pensato per il Web. Per restituire i dati in formato RDF, aggiungere il parametro format=rdf alla query string:

http://etriage.cloudapp.net/v1/ ICD9CM /Diagnosi/?$filter=name eq 'Colera' &format=rdf

CONCLUSIONI DI POLICY

A conclusione dell'analisi condotta nella parte legale, e alla luce del confronto con il team medico e informatico, e in particolare in seguito all'analisi del documento di lavoro dal titolo *"Requisiti funzionali e specifiche del sistema eTriage"*, si rende necessario sviluppare alcune brevi considerazioni finali, che sintetizzino i punti di arrivo del progetto.

Partendo dalla scelta dell'anonimato, va detto che essa ha ricevuto conferma dai team che hanno coordinato questo lavoro di esame preparatorio sul progetto. Si può quindi acquisire tale scelta come definitiva. Trova altresì conferma la scelta di rendere irreversibile il dato reso anonimo: non si potrà cioè tornare a ricostruire un dato personale a partire da un'informazione dissociata dalla componente identificativa. Del resto sarebbe improprio, in caso diverso, parlare di anonimato.

Le conseguenze di queste due scelte sono precise e di rilievo, in termini giuridici. Si rimanda per un'analisi dettagliata a quanto detto nella parte generale.

Posizioni più approfondite e di dettaglio sulle modalità e i protocolli da seguire da parte delle strutture partecipanti al progetto per la trasformazione dei dati sanitari in anonimi non risultano essere state invece ancora affrontate. In realtà, la fase attuale ha visto concentrare le energie sulla messa a punto dei concetti principali da adottare per le specifiche informatiche e mediche relative al formato dei dati e alla loro trasmissione.

Si tratta dei requisiti della piattaforma informatica da utilizzare in concreto. In proposito, la scelta è caduta su interfacce web service, API Restful, con ricorso al noto formato XML/JSON, in attesa di definizioni di maggior dettaglio sugli aspetti operativi. Si è altresì concordato sul protocollo da utilizzare per lo scambio di dati tra i vari partecipanti al progetto, individuato nello standard HL7, assai diffuso in ambito clinico. Quanto all'architettura del cloud che ospiterà il progetto, ci si è orientati sul servizio Microsoft SQL Azure. Infine, il formato da utilizzare per la codificazione dei

dati sanitari è stato individuato nello standard ICD-9-CM, per ragioni ampiamente spiegate nel documento *Requisiti funzionali*, *cit.*, che qui si intendono richiamate.

In definitiva, perciò, orientandosi il lavoro di approfondimento fin qui condotto sugli aspetti più strettamente medici e informatici legati al funzionamento globale del progetto, la definizione di dettaglio delle procedure da adottare nella anonimizzazione dei dati da parte delle singole strutture sanitarie è stata per il momento rimessa ad una fase più concretamente operativa e futura del progetto.

Ciò comporta, naturalmente, che al momento non sia possibile formulare sul punto alcun tipo di considerazione giuridica.

Al più si può ribadire che appare corretta e apprezzabile la scelta di procedere, in ogni caso, a una dissociazione (automatica o manuale) tra informazione ed elemento identificativo del paziente. Come indicato a pag. 3 del documento *Requisiti funzionali, cit.: "Il sistema sarà alimentato dalle fonti Triage dell'attuale sistema sanitario. Le fonti dovranno pilotare l'inserimento dei dati nel sistema eTriage attraverso delle interfacce di accesso ai dati dei pazienti depersonalizzati… Il dato sanitario è residente negli archivi dei data provider e non può essere condiviso liberamente unitamente all'associazione anagrafica"*[7].

Una delle conseguenze dell'utilizzo di dati anonimi riguarda anche evidentemente l'osservanza delle prescrizioni dettate dal Codice privacy in materia di misure di sicurezza, posto che le disposizioni del Codice trovano applicazione solo con riferimento a dati personali. Non si rende cioè necessaria l'adozione di misure minime e idonee.

Resta comunque la considerazione che l'adozione di misure di sicurezza, specie ove esse siano di tipo ormai acquisito allo stato della tecnica, costituisce una scelta senz'altro opportuna, anche soltanto al fine di assicurare il rispetto dell'integrità e non manomissione delle informazioni. Su questa linea prudenziale si sono mossi i team che hanno elaborato questo primo disegno del progetto, i quali hanno espresso

[7] La scelta è ribadita anche successivamente nel documento citato, cfr. p. 12: *"… Localmente rimangono confinate le identità personali dei pazienti che hanno subito trattamenti ospedalieri. In tal modo sarà disaccoppiato il concetto di identità personale da quello di paziente di una struttura ospedaliera"*.

l'intenzione di adottare stringenti standard di sicurezza, come emerge dal già citato documento *Requisiti funzionali ecc.*. Si legge a pagina 2 che saranno implementati requisiti di sicurezza *"che debbono proteggere l'applicazione da modifiche, usi indesiderati, accessi dolosi o accidentali. Tra gli esempi ci saranno l'utilizzo di tecniche crittografiche, restrizioni delle comunicazioni, integrità dei dati, etc."*.

In materia di adozione di misure di sicurezza, va poi richiamata l'attenzione alla fase assai delicata della trasformazione dei dati sanitari in dati anonimi. Vi è cioè un momento, iniziale rispetto al progetto vero e proprio, nel quale avviene la dissociazione tra componente identificativa e informativa e in cui perciò i dati si trovano – almeno per un passaggio – ancora nella forma di dati personali. È assolutamente necessario, in tale limitata fase, assicurare che il processo dissociativo si svolga con l'assistenza delle misure di sicurezza minime e idonee prescritte dal Codice.

Va in proposito brevemente ricordato che la normativa applicabile prevede per gli enti pubblici (art. 22, co. 7 Codice) l'obbligo della separazione dei dati sanitari da altri dati personali. I dati sanitari, inoltre, come del resto tutti i dati sensibili trattati con strumenti elettronici (art. 22, co. 6 Codice), sono sottoposti a tecniche di cifratura o all'utilizzo di codici identificativi o di altre soluzioni che li rendano temporaneamente inintelligibili, anche per chi è autorizzato ad accedervi, e permettano di identificare gli interessati solo in caso di necessità. Tale misura si trova ribadita, per i dati idonei a rivelare lo stato di salute trattati da organismi sanitari, dall'art. 34, co. 1, lett. h) Codice e dal punto n. 24 dell'Allegato B al Codice.

Uno spunto interessante emerso, circa la destinazione dei dati anonimi di progetto, è quello della possibilità di un loro riutilizzo da parte dei soggetti pubblici coinvolti. Nessun divieto di riutilizzo si pone in concreto, in quanto i dati sono resi anonimi e non rientrano nelle limitate ipotesi di divieto di riutilizzo previste dalla normativa. Il riutilizzo di informazioni pubbliche, pur non assurgendo a un dovere per le pubbliche amministrazioni (cfr. art. 1, co. 2 d.lgs. 24 gennaio 2006, n. 36), rappresenta

comunque una scelta incoraggiata dal legislatore, come reso chiaro dall'art. 1, co. 4 d.lgs. 36/2006.

Esso può avvenire sia a fini commerciali sia a fini non commerciali. Del resto, come emerge anche dal recente Vickery study del 2011[8], promosso dalla Commissione europea, le informazioni raccolte ed elaborate dalle pubbliche amministrazioni della UE, le cosiddette PSI (*Public Sector Information*), registrerebbero un impatto economico, in termini diretti e indiretti, dell'ordine di 140 miliardi di euro. Si tratta di un capitale del quale si impone certamente un efficiente impiego, anche in ossequio al principio costituzionale del buon andamento della pubblica amministrazione, sancito all'art. 97, co. 1 Cost., che certamente si declina anche nel senso di una ricerca di ottimizzazione nelle risorse. In altri termini, la prospettiva che è stata aperta appare sotto molti profili come connotata di interesse e utilità.

Su questa particolare angolatura dell'analisi ci si deve fermare purtroppo fermare a questa prima prospettazione di massima, in quanto i team che hanno partecipato alla definizione delle linee essenziali dell'eTriage non hanno al momento effettuato approfondimenti più specifici che permettano di chiarire se e in quali termini la strada del riutilizzo sia percorribile. C'è anche da considerare che tra le strutture sanitarie che parteciperanno al progetto ci saranno strutture private, i cui rapporti con i soggetti pubblici che faranno parte del progetto andranno definiti nel caso si faccia la scelta del riuso dei dati.

È stata in ogni caso ventilata dal team medico-informatico la possibilità di rendere pubblicamente accessibile una parte dei dati di progetto (open data), studiando la possibilità di cederli con licenze "creative commons" (cfr. *Requisiti funzionali, cit.*, p. 4), anche non appare ancora chiaro come articolare queste ultime né quale parte dei dati rendere pubblicamente accessibile e in base a quali criteri.

[8] Cfr. Graham Vickery, *Review of recent studies on psi re-use and related market developments*, 2011, url: http://ec.europa.eu/information_society/policy/psi/docs/pdfs/report/psi_final_version_formatted.docx, pag. 3: *"PSI-related information can be used in a very wide range of direct and indirect applications across the economy. The aggregate direct and indirect economic impacts from PSI applications and use across the whole EU27 economy are estimated to be of the order of EUR 140 billion annually"*.

Un'ultima considerazione può forse essere sviluppata, in chiave di chiusura del presente lavoro. La scelta di utilizzare dati anonimi ha certamente semplificato e per così dire "ridotto all'osso" le questioni giuridiche sollevate nella prima parte di questo lavoro. Tuttavia, ove i team scientifici non avessero optato per l'anonimizzazione, ad esempio in quanto non percorribile a causa di particolari esigenze mediche o scientifiche, i problemi giuridici che ne sarebbero scaturiti avrebbero registrato una dimensione di particolare difficoltà solutiva. Si sarebbe infatti delineata una situazione caratterizzata non solo dall'interazione tra strutture pubbliche e private ma anche da una duplice finalità di cura e amministrativa nel trattamento di dati sanitari. Ciò avrebbe determinato il richiamo a una disciplina giuridica caratterizzata dalla sovrapposizione e dall'incrocio di schemi diversi, per i quali si rimanda a quanto già notato nella parte generale del presente documento.

Alla luce di quanto osservato, appare allora certamente opportuna una regolamentazione specifica di quei servizi sanitari (e il triage non è certamente l'unico) che si collocano all'intersezione di finalità diverse e coinvolgono organismi sanitari sia pubblici sia privati. Sarebbe anche desiderabile l'enunciazione, in via di possibile alternativa, di criteri generali che permettano di individuare una finalità prevalente nei casi di confine, così da indicare l'applicazione di una disciplina più chiara.