POLITECNICO DI TORINO

Corso di Laurea in Ingegneria delle Telecomunicazioni

Tesi di Laurea Magistrale

Privacy e Sicurezza dei Dati Sanitari

Relatore
prof.ssa Monica Visintin

Laureando
Riccardo Artosi
matricola: 084907

Aprile 2025

Ai miei genitori
Ai miei figli

Sommario

Questa tesi di laurea vuole essere il coronamento non solo del percorso di studi, ma anche del percorso lavorativo decennale che nel frattempo il candidato ha maturato in ambito di informatica sanitaria, soffermandosi in maniera particolare verso i sempre più importanti e delicati temi di privacy che l'ambito sanitario porta con sè

Questa tesi è stata composta usando il programma di scrittura scientifica LaTeX ed il pacchetto TOPtesi 6.4.07 - 2025-01-19.

Ringraziamenti

Il ringraziamento più grande lo rivolgo ai miei genitori, a mia madre che purtroppo non c'è più, e so che una delle sue più grandi gioie sarebbe stata essere presente in questo momento, ed a mio padre per la sua incrollabile fiducia e appoggio costante in ogni mia scelta.

Ringrazio la mia relatrice, prof.ssa Monica Visintin, alla quale è bastato pochissimo per capirmi e comprendere le mie necessità di studente-lavoratore, anzi, di lavoratore-studente, mi ha supportato ed aiutato senza indugi, con grande professionalità e preparazione.

Ringrazio il mio responsabile Stefano Giglio, che da sempre considero il mio tutor, maestro e, soprattutto, amico. La sua grande professionalità, organizzazione e tenacia nel raggiungimento degli obiettivi è per me un esempio costante.

Ringrazio Stefano Gamba, che è stato anche lui collega ed è rimasto, cosa ancora più importante, un amico e che sempre, senza esitazione, ha condiviso con me il suo enorme bagaglio di conoscenza ed esperienza.

Infine ringrazio tutti i colleghi con cui ho condiviso, e tuttora condivido, il mio percorso lavorativo e da cui continuo sempre ad imparare.

Questa laurea è un traguardo raggiunto anche grazie a tutti loro.

Indice

Elenco delle tabelle

Elenco delle figure

Lista degli Acronimi

2FA	two factor authentication	35
ADT	Accettazione, Dimissione e Trasferimento	16
AES	Advanced Encryption Standard	43
ANA	Anagrafe Nazionale Assistiti	52
ANPR	Anagrafe Nazionale Popolazione Residente	52
ANSI	American National Standards Institute	65
API	Application Programming Interface	73
ASCII	American Standard Code for Information Interchange	66
AUSL	Azienda Unità Sanitaria Locale	24
BC	Business Continuity	30
BI	Business Intelligence	62
BIA	Business Impact Analysis	30
BTG	Break the Glass	25
CCE	Cartella Clinica Elettronica	16
CIA	Confidentiality, Integrity and Availability	33
CIE	Carta d'Identità Elettronica	61
CSS	Cascading Style Sheets	73
CUP	Centro Unico Prenotazioni	16
DBMS	DataBase Management System	37
DEK	Database Encryption Key	37
DICOM	Digital Imaging and COmmunications in Medicine	64
DoS	denial-of-service	34
DPIA	Data Protection Impact Assessment	30
DPO	Data Protection Officer	27
DSE	Dossier Sanitario Elettronico	16

Capitolo 1

Introduzione

L'argomento "Privacy" ha assunto negli ultimi anni un'importanza sempre maggiore. Questo è ancora più vero se contestualizzato nel mondo della sanità ed, in particolare, al mondo dei dati clinici, considerati dalle normative di tutti gli Stati come i più *delicati* e, quindi, quelli per i quali le Aziende devono spendere più "energie" riguardo la loro protezione da furti o accessi malevoli.

I dati sanitari sono sempre di più oggetto dell'interesse di molteplici soggetti, che purtroppo non sono solo quelli operanti in ambito clinico, e ne abbiamo evidenza dal sempre più alto numero di attacchi informatici che le aziende sanitarie subiscono nei confronti dei loro database [5].

Nel mondo dell'informatica sanitaria, questo vuol dire che **il livello di attenzione** che le tecnologie (così come le persone che queste tecnologie sviluppano o utilizzano) devono sostenere, **deve essere sempre più alto**. Ciò significa anche che **la responsabilità** che sottende a come questi dati vengono gestiti, trattati, condivisi, inviati, archiviati, **è molto alta**, più di quella che normalmente è la percezione non solo di coloro che sono estranei all'ambito della sanità, ma, purtroppo, anche per molti di coloro che in questo ambito tutti i giorni lavorano.

L'ambito della **privacy** e della **sicurezza** in sanità o, più precisamente, **nell'informatica sanitaria** infatti ha acquisito una moltitudine di aspetti e sfaccettature spesso difficili da comprendere o immaginare per chi non è direttamente addentro, anche perché spesso occorre sottostare a normative vigenti di difficile comprensione e di altrettanto difficile applicazione. Queste normative sono state scritte nel modo più preciso possibile ma, al tempo stesso, anche con un'accezione sufficientemente ampia da permettere di poter essere applicata alla moltitudine, eterogenea, dei software sanitari in uso.

Queste norme, che sono quindi state emanate ed aggiornate nel corso degli ultimi 20 anni allo scopo di proteggere questi dati preziosi, hanno implicato, ed implicano tuttora, un grosso sforzo di interpretazione riguardo al come riuscire ad applicarle alle specificità

di ogni software, sia esso già "in produzione"[1] o durante la fase di progettazione o sviluppo (da qui i concetti, che vedremo più avanti, di "privacy by design" e "privacy by default").

Infine, alla base di questa tesi, vi è l'esperienza riguardo a quanto implementato presso l'AUSL della Valle d'Aosta proprio in applicazione delle normative italiane sulla privacy sanitaria. Un lavoro corposo ed in costante adeguamento che abbraccia un arco temporale ormai decennale (l'inizio dello studio dell'applicazione delle regole del DSE[2] è iniziato nella seconda metà del 2015, subito dopo l'emanazione della specifica regolamentazione). In particolare, il software principale in uso, chiamato **TrakCare**[3] (attualmente in versione 2014, ma in fase di progressiva dismissione per la migrazione verso la versione 2024) e prodotto dall'azienda **InterSystems**[4], è stato installato, adattato e ad oggi mantenuto, dal gruppo di lavoro denominato SIO[5] della società inhouse della Regione Valle d'Aosta "INVA S.p.A."

TrakCare è un complesso software clinico che fa parte della categoria dei software cosiddetti HIS[6] o, in italiano SIO, la cui caratteristica principale è quella di essere ad utilizzo "orizzontale" all'interno dell'organizzazione dell'Azienda Sanitaria, il ché vuol dire possedere delle caratteristiche tali per cui esso può essere utilizzato in molteplici ambiti, tra cui, ad esempio, la gestione dell'ADT[7] e delle CCE[8] di reparto, delle sale operatorie, la gestione ambulatoriale (refertazione di visite o esami strumentali), la gestione delle prenotazioni (CUP[9]), la tariffazione delle prestazioni e degli appuntamenti sia in regime "istituzionale" che di LPI[10]. Dato l'uso, appunto, molto esteso che questo software permette, esso diviene di conseguenza un contenitore di una enorme mole di dati clinici digitali i quali, sommandosi a quelli prodotti da altri applicativi, sempre clinici,

[1] Come è facile immaginare, applicare modifiche ad un software già attivo in un ambiente di produzione è tutt'altro che semplice, ancora più delicato è però questo lavoro se il software è utilizzato in ambito clinico dove questo implica una grande delicatezza sia per quel che riguarda l'accurata necessità di non compromettere i dati, di mantenerli sempre disponibili (le interruzioni di servizio sono sempre molto delicate, ma in ambito sanitario, ricordiamoci sempre, abbiamo a che fare con il "rischio clinico" e i problemi assumono un livello decisamente più alto) ma al tempo stesso visibili solo alle giuste condizioni

[2] Dossier Sanitario Elettronico

[3] www.intersystems.com/it/prodotti/trakcare

[4] www.intersystems.com/it

[5] Sistema Informativo Ospedaliero

[6] Hospital Information System

[7] Accettazione, Dimissione e Trasferimento

[8] Cartella Clinica Elettronica

[9] Centro Unico Prenotazioni

[10] Libera Professione Intramoenia

ma più specialistici (che definiamo perciò "verticali"), come ad esempio il RIS[11] dedicato al servizio di Radiologia, o il LIS[12] dedicato alla gestione del Laboratorio Analisi, finisce per diventare il principale punto di produzione e gestione dell'archivio dei dati sanitari dei pazienti, detto, non a caso, DSE e di cui parleremo in maniera approfondita nel paragrafo 2.1.

Questa tesi è strutturata in 5 capitoli:

- il capitolo 2 è dedicato alla normativa vigente in Italia al 2025 in ambito di protezione dei dati, con particolare riferimento a quelli sanitari
- nel capitolo 3 ci soffermiamo sulle tecnologie ad oggi esistenti riguardo la protezione dei database, sia dal punto di vista della cifratura, che serve a proteggere i db da accessi illegittimi, sia dal punto di vista dei backup, che servono a proteggere i db da errori, malfunzionamenti o incidenti che causerebbero la perdita dei dati
- il capitolo 4 tratta dei sistemi sanitari, intesi come applicativi software che mettono a disposizione di una struttura sanitaria le funzionalità informatiche di cui i suoi operatori necessitano. Questi software si occupano anche di interfacciarsi con eventuali apparati medicali e devono possedere funzioni fondamentali di **comunicazione** ed **interscambio** dei dati tra di loro
- il capitolo 5 si occupa proprio dell'interscambio dei dati tra i sistemi sanitari, le cosiddette **integrazioni**, funzionalità fondamentali affinché i dati da essi prodotti e gestiti vengano messi a fattor comune così da offrire l'efficienza che un sistema informatico avanzato come quello di un'azienda sanitaria necessita
- infine, nell'appendice, tratteremo un caso reale di cosa vuol dire e qual è una delle possibili conseguenze dell'accesso non autorizzato ai dati sanitari

[11] Radiology Information System

[12] Laboratory Information System

Capitolo 2

La normativa

Numerose normative sono state emanate dall'autorità legislativa sull'ambito **"privacy"** o dei cosiddetti **"dati sensibili"** a partire già dall'anno 2003. Non è scopo di questa tesi soffermarsi sulle parti più strettamente giuridiche, ma si ritiene comunque necessario descrivere alcune delle più importanti normative emesse a riguardo, visti poi gli impatti diretti che queste hanno avuto, ed hanno tuttora, sul mondo dell'informatica sanitaria. Tali concetti e definizioni sono inoltre utili a comprendere come l'argomento sia trattato, a livello normativo, in modo sempre più esteso ed approfondito, a tutela dei dati dei cittadini.

I **dati personali** sono in grado di identificare in maniera certa ed univoca il soggetto a cui si riferiscono. La categoria dei dati personali si suddivide poi in diverse sottocategorie e, tra queste, una in particolare è quella dei cosiddetti **dati sensibili** (vedi fig. 2.1) o, secondo la nuova definizione del Regolamento (UE) 2016/679 - GDPR , art. 9, par.1, **dati particolari**, che comprende cioè le informazioni che riguardano lo stato di salute fisica o mentale e le eventuali prestazioni che i cittadini ricevono dai servizi sanitari. All'interno di questa sottocategoria possiamo far rientrare anche i **dati genetici** del soggetto. Tutti assieme formano la **storia clinica del soggetto**.

Se nel passato i dati clinici dei cittadini venivano conservati con modalità soprattutto cartacee e non organiche, l'avvento delle tecnologie informatiche ha permesso di gestire moli di dati sempre maggiori in maniera organica, strutturata ed anche aggregata, permettendo così di ottenere grandi vantaggi sotto molteplici aspetti. Tra i vantaggi più evidenti citiamo il poter ricostruire più facilmente la storia clinica di un paziente, il poter confrontare i dati aggiornati di un paziente con i suoi dati pregressi o di altri pazienti in condizioni simili, avere notizie sullo stato di salute anche se il paziente è incosciente o non più in grado di fornire informazioni su se stesso, il poter fare valutazioni a distanza. Ma non solo: oltre a questo vi sono enormi vantaggi anche dal punto di vista statistico in quanto la digitalizzazione dei dati dei pazienti permette di avere un visione allargata riguardo le molteplici indagini che si possono fare sull'incidenza di certe patologie o l'efficacia di certe cure, ecc.

Figura 2.1. Diagramma delle tipologie di dati personali

Vi sono però anche grandi rischi se, come già scritto in precedenza, questi dati non vengono adeguatamente protetti al fine di evitare violazioni dei diritti fondamentali di privacy delle persone.

Gli strumenti che il legislatore ha imposto ai soggetti che gestiscono tali dati sono soprattutto:

- il Codice della privacy (il d.lgs. n. 196 del 30/06/2003, poi modificato dal d.lgs n. 101 del 10/08/2018, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE 2016/679)
- le successive linee guida emanate dal Garante privacy in materia sanitaria, in particolare per il DSE e per il FSE[1]
- il GDPR[2]

2.1 Il Dossier Sanitario Elettronico

Con la deliberazione del 4 giugno del 2015 il Garante della privacy ha adottato le linee guida in materia di **Dossier Sanitario** la cui definizione consiste nell'**insieme dei dati personali derivanti dagli eventi clinici presenti e passati relativamente al**

[1] Fascicolo Sanitario Elettronico

[2] Nuovo Regolamento Generale Europeo sulla Protezione dei Dati Personali - Regolamento UE 2016/679

soggetto interessato, i quali vengono condivisi in maniera logica e connessa tra i vari professionisti sanitari che assistono il paziente presso lo stesso titolare del trattamento. L'interessato (cioè il cittadino/paziente) deve prestare il consenso affinché il titolare del trattamento (in questo caso l'ente o la struttura sanitaria) possa trattare i suoi dati attraverso il dossier. Nel caso in cui l'interessato non presti il consenso, allora il professionista sanitario che fornisce la prestazione di cura potrà avere accesso solo alle informazioni che lo stesso interessato gli fornirà in quel momento ed i dati di cui è egli stesso titolare. Infatti, il professionista (o la struttura/reparto) che ha elaborato (cioè prodotto) tali dati è anch'esso "proprietario" del dato assieme al paziente stesso.

Il paziente, però, non ha solitamente a disposizione un'interfaccia per consultare in autonomia il proprio DSE: questo infatti rappresenta un concetto di aggregazione dei documenti clinici (la "storia clinica" del paziente) a disposizione del medico, reparto, struttura che ha in cura il paziente in un dato momento.

La normativa del Garante prevede che il titolare che implementa il DSE rispetti una serie di concetti che sono a tutela della sicurezza dei dati e della privacy che sono:

- l'autenticazione ed il timeout
- la profilazione
- la profondità dell'accesso
- il concetto di "paziente in cura"
- l'oscuramento e l'oscuramento dell'oscuramento
- le leggi speciali
- l'accesso in deroga
- il logging e la conservazione dei log
- la cifratura
- la separazione dei dati

ed il cui **rispetto**, da parte del titolare, **è fondamentale** per una corretta applicazione del regolamento.

Vediamoli di seguito più nel dettaglio.

L'autenticazione ed il timeout

Si tratta di attivare sistemi di autenticazione che prevedano la sicurezza dell'identificazione univoca della persona fisica che materialmente farà accesso ai dati. Non solo va garantita opportunamente la sicurezza degli accessi (con password, e relative scadenze, che rispettino le norme di sicurezza) ma anche un accesso al DSE privo di attività deve avere un timeout (la scadenza della sessione) che sia "congruo" a prevenire che altri utenti approfittino della momentanea assenza davanti alla postazione dell'operatore che ha fatto accesso all'applicativo. Analogamente deve essere implementata anche un'accurata tracciatura di tutti gli accessi effettuati (data e ora di login, nome utente, identificativo della postazione, data e ora di logoff) allo scopo di poter sempre risalire all'operatore che ha fatto accesso ai dati in caso di controlli o contenziosi.

La profilazione

La corretta profilazione del personale ha lo scopo fondamentale di abilitare la visibilità dei dati, a seconda delle situazioni, ai soli dati "di competenza", a seconda anche del consenso espresso dall'interessato, dello stato "in cura" o meno e dal tipo di profilo/ruolo assegnato all'operatore.

La profondità dell'accesso

La diretta conseguenza della profilazione è quella di permettere altresì una corretta *profondità* di visibilità, così da permettere la giusta ed opportuna visibilità dei dati anche in funzione della tipologia di operatore che si divide, solitamente, in 3 grandi gruppi:

- il personale **medico**, che ha compiti decisionali sulla cura del paziente e che necessita quindi della massima "profondità" di visibilità sui dati presenti e passati del paziente
- il personale **infermieristico** e ostetrico o appartenente ad altre professioni tecnico-sanitarie (quali, ad esempio, tecnico di radiologia, tecnico di laboratorio ecc.), con compiti più operativi nell'immediato e che quindi necessita di una visibilità meno profonda rispetto soprattutto alla storia clinica del paziente
- il personale **amministrativo** che non avendo funzioni legate alla parte "clinica" del paziente necessita ancora meno di una visibilità profonda sulla cura in corso o sulla storia del paziente

Il concetto di "paziente in cura"

Fondamentale, da parte dell'applicativo gestionale che implementa il DSE, **è il concetto** cosiddetto **di "paziente in cura"**. La corretta implementazione ed applicazione di questo concetto ha enormi ripercussioni su quella che è la **visibilità** del Dossier stesso (cioè, in parole povere, della storia clinica passata del paziente) da parte degli operatori sanitari,

ed un'errata gestione può avere conseguenze fortemente negative sia dal punto di vista amministrativo [45] che, soprattutto, clinico.

Essere "in cura", per un paziente, vuol dire avere un episodio[3] attivo (aperto/corrente) presso un certo reparto/ambulatorio/medico (parliamo, in generale, di *specialità medica*) e quindi il personale di quel reparto/ambulatorio deve poter avere accesso almeno a quell'episodio ed ai dati in esso contenuti (referti, anamnesi, esame obiettivo, risultati di laboratorio, ecc.). Se però il paziente ha espresso consenso favorevole alla costituzione del suo Dossier allora il personale (sempre in base anche alla profilazione assegnatagli) potrà vedere e consultare anche i dati degli altri episodi clinici passati, effettuati presso reparti anche diversi dal proprio, che compongono, appunto, il Dossier del paziente. Se però per l'applicativo il paziente non risulta in quel momento "in cura", oppure ha negato il consenso alla costituzione del suo DSE, allora il personale potrà accedere, riguardo la storia del paziente, solo agli episodi passati dello stesso reparto/ambulatorio/specialità di appartenenza, con la conseguenza, potenzialmente grave e pericolosa, di **non poter accedere ad informazioni anche importanti per la somministrazione di un adeguato processo di cura**.

Il concetto di "in cura", quindi, deve attenersi ad una situazione che è temporanea e, alla chiusura dell'episodio, il sistema deve far sì che il personale torni a vedere solo i dati clinici del paziente nel quale sono stati coinvolti per competenza e sempre nel rispetto dei concetti già espressi di profondità dell'accesso (con eventuali deroghe, definite solitamente come "periodo di garanzia", atte a permettere agli operatori una visibilità pari al momento del paziente in cura anche per un periodo di tempo, limitato solitamente ad un massimo di 30 o 60 gg, a seconda dei casi e delle scelte aziendali, utile a permettere agli operatori di poter accedere ad eventuali risultati di esami fatti successivamente all'episodio, ma a questo strettamente legati).

L'oscuramento e l'oscuramento dell'oscuramento

Nel caso in cui il paziente abbia espresso parere favorevole alla costituzione del proprio DSE, egli ha comunque la facoltà di richiedere che alcuni suoi dati clinici non siano resi disponibili all'interno del proprio DSE, siano cioè oscurati. Ricordando che, comunque, i dati clinici sono sempre visibili al reparto/ambulatorio (sempre intesi come "specialità medica") che li ha emessi, l'oscuramento farà sì che, anche durante il periodo di cura del paziente, il medico non potrà vedere i dati oscurati, a meno che non siano afferenti alla sua stessa specialità.

[3] Per *episodio*, o *cartella*, in ambito clinico-informatico, si intende un "contenitore" di dati clinici, siano essi referti di visite ambulatoriali, appuntamenti passati o futuri ancora da eseguire, lettere di dimissione, atti operatori, diari clinici e molto altro ancora, legati ad uno stesso "accesso", cioè un ricovero o un episodio di pronto soccorso o di visita ambulatoriale

In aggiunta a questo, l'operatore non dovrà neanche vedere che un dato è stato oscurato, e cioè non solo egli non dovrà avere evidenza del contenuto del dato oscurato (ad esempio il testo di un referto o di un atto operatorio), ma neanche dovrà avere evidenza dell'**esistenza di quel dato**. Da qui il concetto, che sembra un gioco di parole ma è importantissimo nella salvaguardia della volontà di privacy del paziente, di **"oscuramento dell'oscuramento"**.

Le "leggi speciali"

Come accennato al punto precedente il paziente può richiedere al titolare, in maniera volontaria, l'oscuramento dei dati di cui vuole mantenere un maggiore riserbo. Oltre a questo, però, vi sono alcuni dati clinici soggetti alle cosiddette "leggi speciali", che vanno resi oscurati per impostazione predefinita, quindi anche senza la richiesta esplicita del paziente (il quale, al contrario, può richiederne volontariamente il de-oscuramento). Questi dati rientrano in un concetto, espresso al livello normativo, di *maggior tutela di anonimato* o, appunto, *leggi speciali*, e sono quelli dovuti a:

- atti di violenza sessuale o pedofilia
- soggetti affetti da HIV
- soggetti dipendenti da sostanze stupefacenti o alcooliche
- donne che si sottopongono ad interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato
- dati e documenti riferiti ai servizi offerti dai consultori familiari

Il risultato dell'oscuramento di questi dati è lo stesso di quanto descritto al punto precedente, la differenza sta proprio nel fatto che vanno oscurati senza necessità di richiesta da parte del paziente.

Il logging e la conservazione dei log

La normativa prevede anche che tutte le operazioni effettuate sul DSE siano tracciate. Questa regola comprende, inoltre, che vengano tracciati **tutti gli accessi, anche solo in lettura, al DSE** di un paziente (il quale, lo ricordiamo, ha la facoltà di richiedere al titolare la tracciatura di chi ha fatto accesso al proprio Dossier) e che tali file di log siano conservati per almeno 24 mesi. Più avanti in questa monografia (paragrafo 3.6) si darà evidenza di come questo vada ad impattare, in termini di spazio fisico di archiviazione, a carico di un'azienda sanitaria comunque "piccola" come quella della AUSL[4] della Valle d'Aosta.

[4] Azienda Unità Sanitaria Locale

L'accesso in deroga

La normativa del Garante sul DSE contempla anche la possibilità di ottenere l'accesso al DSE di un paziente (sempre purché il paziente abbia espresso consenso positivo alla costituzione del proprio DSE, altrimenti a livello "logico", il DSE di quel paziente **non esiste**, e quindi non c'è nulla a cui poter fare accesso) per situazioni particolari, soprattutto emergenziali, o comunque in momenti in cui, per l'applicativo, il paziente non risulta "in cura" per quel dato medico. Quindi questa funzione viene ovviamente resa disponibile solo al personale di tipo medico (essendo l'unico coinvolto nel processo "decisionale" della cura del paziente), e necessita di una tracciatura specifica che memorizzi anche la motivazione per cui il medico ha fatto questo accesso detto anche "in deroga" (in TrakCare viene anche definito "BTG[5]"). Vi possono essere anche motivazioni non legate a stati di emergenza, ma comunque lecite, come ad esempio l'accesso ai risultati di esami o visite prescritte dal medico stesso, ma eseguite da altri servizi in tempi successivi ed i cui esiti sono disponibili solo dopo la chiusura/dimissione dell'episodio che ha coinvolto il medico in questione, oppure errori di gestione che fanno sì che l'episodio non sia correttamente aperto nel momento della visita. Tutte motivazioni che rendono lecito (benché scomodo per il medico) l'utilizzo di questa funzionalità.

La cifratura

Un altro obbligo imposto dal Garante della privacy (nelle linee guida per il DSE) è quello di cifrare il database contenente i dati clinici (e come vedremo anche rispetto al GDPR porta vantaggi attuare la cifratura (v. par. 2.3.3). Questo argomento molto importante necessita di uno specifico approfondimento che verrà trattato nel paragrafo 3.1.

La separazione dei dati

Analogamente alla cifratura dei dati del db viene anche richiesto, come ulteriore forma di sicurezza, che i dati presenti nel db siano opportunamente "separati" a livello logico. Anche questo argomento verrà approfondito nello specifico paragrafo 3.4.

2.2 Il Fascicolo Sanitario Elettronico

Secondo la definizione il FSE è l'insieme dei dati e documenti digitali di tipo sanitario e sociosanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito. Si tratta di uno strumento atto a contenere e descrivere l'intera vita del paziente e che viene costantemente alimentato ed implementato nel tempo. A livello normativo esso è stato inizialmente disciplinato dal d.P.C.M. del 29 settembre del 2015, n.178, ed ora quasi

[5] Break the Glass

totalmente abrogato dal Decreto del Ministero della Salute 7 settembre 2023 "Fascicolo Sanitario Elettronico 2.0".

Esso si differenzia dal DSE in quanto:

- il DSE viene costituito da un organismo sanitario, che è il titolare del trattamento, all'interno del quale operano più professionisti (ad esempio un ospedale, una clinica privata, un centro diagnostico, ecc.). Quindi ogni titolare creerà il proprio DSE ad uso e consumo dei professionisti che operano al suo interno.

- il FSE è invece formato dai dati sanitari che provengono da molteplici e distinti titolari del trattamento (che possono essere, ad esempio, ospedali, intere aziende sanitarie, medici di medicina generale e pediatri di libera scelta, strutture private convenzionate, ecc.), e che possono operare anche in ambiti territoriali diversi.

Il FSE quindi si configura come un raccoglitore per certi versi più esteso del DSE, sia in termini di quantità che di tipologie di documenti e informazioni cliniche che può ricevere ed aggregare, oltre che essere disponibile ed accessibile al cittadino/paziente.

Oltre a questo, il FSE ha ricevuto nel tempo importanti aggiornamenti riguardo le funzionalità a cui le Regioni si devono attenere per garantirne la cosiddetta "interoperabilità" atta a far sì che:

- eventuali referti prodotti da strutture geograficamente appartenenti ad una regione diversa da quella di residenza dell'interessato siano comunque resi disponibili nel FSE del cittadino.

- in caso di trasferimento di residenza in un'altra regione i dati eventualmente presenti nel FSE della regione di origine vengano trasferiti nel nuovo FSE della nuova regione di residenza (parliamo, in questo caso, di trasferimento dell'indice del FSE, in quanto fisicamente, i dati restano nell'archivio del FSE della regione dove si sono originati, ma in maniera del tutto trasparente al cittadino, questi vengono resi disponibili anche nel nuovo FSE).

2.3 Il GDPR

Il Regolamento UE 2016/679 (c.d. GDPR) è formato da 3 parti più ulteriori 3 allegati:

- La **Parte prima**: contiene i principi generali, le definizioni e le norme sulla sicurezza dei dati e dei sistemi

- La **Parte seconda**: contiene, tra le altre norme, il capo V, che riguarda il trattamento dei dati in ambito sanitario

- La **Parte terza**: riguarda la tutela dell'interessato e l'apparato sanzionatorio

- Gli **Allegati A, B e C**: tra questi è di fondamentale importanza per il lavoro degli informatici l'**allegato B**, detto "Disciplinare tecnico sulle misure minime di sicurezza" che impone misure di autenticazione, autorizzazione, backup e data recovery dei sistemi informatici

Il GDPR richiede di adeguare le tecnologie informatiche ed i processi aziendali, di fare l'analisi del rischio e di notificare all'autorità di vigilanza le violazioni dei dati personali, come il furto di dati o il "data breach" (vedi par. 2.3.3). Esso introduce il diritto alla "portabilità" dei propri dati personali, per trasferirli da un titolare del trattamento a un altro, ed introduce la *responsabilizzazione* dei titolari del trattamento ("accountability" vedi par. 2.3.1) per garantire un approccio che tenga in maggior considerazione i rischi che un determinato trattamento può comportare per i diritti e le libertà degli interessati. Non a caso il GDPR prevede la creazione della figura del DPO[6], o "Responsabile della protezione dei dati", incaricato di assicurare una gestione corretta dei dati nelle aziende e negli enti e che viene individuato in funzione delle qualità professionali, della conoscenza specialistica, della normativa e della prassi in materia di protezione dati.

Il GDPR prevede pesanti sanzioni a carico dei trasgressori, sanzioni che possono ammontare fino anche a 10 milioni di euro.

2.3.1 Il principio di accountability

La parola inglese "accountability" si può tradurre nella nostra lingua con "responsabilizzazione" e indica, nelle intenzioni del legislatore comunitario del Regolamento, quell'insieme di comportamenti **proattivi** atti a dimostrare di aver messo in essere tutte le misure necessarie previste dal GDPR, da parte di tutti i soggetti coinvolti nel trattamento dati, in particolare il titolare ed il responsabile del trattamento, affinché possano sempre dimostrare la conformità delle attività di trattamento e l'efficacia delle misure intraprese (indipendentemente dall'effettiva perdita di dati). Questo concetto è quindi citato direttamente dal sito del Garante italiano dove, nella sua "*Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali - approccio basato sul rischio e misure di* ***accountability*** *(responsabilizzazione)*"[16], si occupa direttamente di aiutare i titolari del trattamento a passare da una concezione formale di mero adempimento ad una normativa, ad un approccio **attivo** verso la tutela dei dati. In altri termini, non basta adottare delle misure di protezione che inizialmente si rivelino idonee alla necessità, ma è necessario verificare costantemente nel tempo la loro continua adeguatezza e, nel caso in cui tali misure non siano più adeguate con il passare del tempo, il titolare dovrà modificarle per renderle nuovamente adeguate.

[6]Data Protection Officer

2.3.2 Privacy "by default" e "by design"

All'articolo 25 del Regolamento vengono date precise indicazioni al titolare del trattamento di mettere in atto misure tecniche ed organizzative quali:

- la pseudonimizzazione
- la minimizzazione: che vengano, cioè, trattati solo i dati personali strettamente necessari per ogni finalità del trattamento
- che vengano trattati **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento, anche in termini di quantità di dati personali raccolti, periodo di conservazione, accessibilità
- **sempre per impostazione predefinita** che non vengano resi accessibili dati personali ad un numero indefinito di persone fisiche senza l'intervento della persona fisica

Le misure da adottare potranno essere sia **tecniche**, realizzate cioè attraverso sistemi software o hardware, sia **organizzative**, cioè affidate alle pratiche e modalità operative dei soggetti che operano all'interno della struttura del titolare o del responsabile del trattamento.

Questi concetti essenziali introdotti dal GDPR sono quindi applicati attraverso questi due principi cardine:

- **privacy by design**: il concetto che si vuole intendere con questa definizione è quello di impostare un approccio alla protezione dei dati personali che sia **proattivo** e non più **reattivo** affinché vengano tutelate la **riservatezza**, l'**integrità** e la **disponibilità** dei dati. Tutto questo va applicato fin dalla progettazione del software ;
- **privacy by default**: con questo principio si intende che la tutela dei dati deve essere un'**impostazione predefinita** del software, ed i dati raccolti dal titolare siano i **minimi possibili** e soltanto quelli **necessari** per ogni specifica finalità del trattamento.

2.3.3 Il data breach

L'articolo 33 del Regolamento [14] prevede un nuovo ed ulteriore adempimento spettante al titolare del trattamento nel momento in cui egli venga a conoscenza del fatto che si sia verificata una situazione della cosiddetta "data breach" che si traduce in un episodio di distruzione accidentale o illegale, di perdita, di modifica, di rivelazione o di accesso non autorizzato ai dati personali trasmessi, conservati o comunque elaborati dal titolare o dal responsabile del trattamento [25].

In qualunque di questi casi il titolare deve notificare al Garante l'avvenuta violazione e documentarne le circostanze in cui è avvenuta, le sue conseguenze ed i provvedimenti che egli ha adottato per porvi rimedio.

L'articolo 34 del Regolamento [15], in aggiunta a quanto sopra, prevede che il titolare del trattamento notifichi l'avvenuta violazione anche al proprietario dei dati. La comunicazione al proprietario dei dati può non avvenire se *"il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali* ***la cifratura****"*.

2.3.4 Ulteriori misure di sicurezza

L'articolo 32 del Regolamento prevede anche di indicare al titolare del trattamento le misure di sicurezza che devono essere adottate per la protezione dei dati.

Come citato in precedenza queste possono e devono essere sia di natura tecnica che organizzativa e devono essere idonee a garantire il necessario livello di sicurezza in base ai dati trattati.

Questo è un elenco, non esaustivo, fornito dall'articolo:

- la pseudonimizzazione e la cifratura dei dati personali;
- la capacità di assicurare con continuità la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di guasto fisico tecnico ai sistemi informatici;
- una procedura per testare regolarmente l'efficacia delle politiche applicate per garantire la sicurezza del trattamento.

2.4 La normativa ISO 27001:2022

La normativa ISO 27001, in particolare nella sua versione attuale ISO 27001:2022 si integra in modo complementare con il GDPR [19]: in particolare 7 nuovi "controlli"[7] inseriti nell'Annex A e di cui ben sette sono riferiti al dominio tecnologico e si concentrano sulla cancellazione delle informazioni, offuscamento e prevenzione della perdita dei dati con un chiaro richiamo al GDPR sulla configurazione "sicura" di hardware, software,

[7] I controlli sono gli adempimenti a cui l'organizzazione deve ottemperare per dotarsi di un sistema per la sicurezza delle informazioni

servizi e reti nonché sullo sviluppo sicuro del codice per ridurre il numero di potenziali vulnerabilità. Entrambe le normative mirano a proteggere le informazioni sensibili, ma mentre il GDPR si concentra e si applica alla protezione dei dati personali, la ISO 27001 fornisce le indicazioni per gestione della sicurezza delle informazioni in generale, con uno spettro più ampio e da un punto di vista più "aziendale" ma, in un contesto di azienda sanitaria, porre l'accento sulla BC[8] aziendale, ha comunque delle importanti e positive ricadute sulla sicurezza dei dati dei pazienti. Vediamo qualche dettaglio in più di quello che comporta per una azienda ottemperare (cioè certificarsi) alla normativa ISO 27001.

La ISO 27001 richiede una valutazione dei rischi per identificare e gestire le minacce alla sicurezza delle informazioni. Questo è fondamentale anche per il GDPR, che richiede una valutazione d'impatto sulla protezione dei dati (DPIA[9]) in determinate circostanze. Inoltre essa stabilisce controlli e misure di sicurezza che possono aiutare le organizzazioni a conformarsi ai requisiti del GDPR, come la protezione dei dati e la gestione degli accessi.

In un contesto sanitario dove la disponibilità del dato dei pazienti da parte del personale medico può essere un fattore critico (ancora di più se siamo in un ambito di gestione dell'emergenza, come un pronto soccorso ospedaliero) è necessario che a fronte di un problema che impedisca l'accesso ai dati, la "prontezza" che il sistema deve avere nel ripristinare i sistemi sia la più elevata possibile [18].

Ci sono due importanti parametri che vanno presi in considerazione:

- RTO[10]: è il tempo necessario per completare il ripristino di un servizio e ritornare operativi, ovvero è il tempo in cui l'organizzazione può permettersi di avere un certo servizio indisponibile e definisce, quindi, la massima interruzione ammissibile o tollerabile
- RPO[11]: è la percentuale di dati che l'organizzazione è disposta a perdere in caso di disastro, in sintesi misura la quantità di dati non sincronizzati rispetto all'ultimo backup effettuato.

Per poter misurare il livello di "prontezza" che un sistema deve avere è necessario procedere ad una preventiva BIA[12] che permetta di indicare quali devono essere gli RTO e gli RPO di ogni servizio dell'organizzazione, al fine di garantire l'implementazione di quanto necessario per questo controllo della ISO 27001 (v. fig. 2.2).

[8] Business Continuity

[9] Data Protection Impact Assessment

[10] Recovery Time Objective

[11] Recovery Point Objective

[12] Business Impact Analysis

Figura 2.2. Rapporto RTO - RPO

Capitolo 3

La protezione del db

Quando si parla di privacy e sicurezza dei Dati Sanitari bisogna ricordarsi che la protezione non deve solo applicarsi al lato applicativo del software, ma che è fondamentale anche proteggere il database stesso dove questi dati sono archiviati. Allargando ancora il discorso, oltre al database "corrente", allo stesso modo vanno protetti anche i backup.

Il database si può proteggere in vari modi, da usare anche simultaneamente e non in alternativa, vedremo in questo capitolo come farlo ed i relativi pregi e difetti delle diverse tecniche di protezione.

Come per tutti i database, anche per quelli in ambito sanitario è necessario garantire tre proprietà principali, che si raggruppano nella cosiddetta triade CIA[1], e per la quale ogni lettera rappresenta un principio fondamentale della sicurezza informatica:

- **Riservatezza** (C - Confidentiality) è quella che definiamo anche, genericamente, privacy. Ciò vuol dire che un database, così come l'applicativo che ne gestisce i dati, deve essere in grado di proteggerne l'accesso da parte di qualcuno non autorizzato. Un attaccante che dovesse riuscire ad ottenere i privilegi di accesso ad un sistema che ospita un database di dati sanitari, otterrebbe le informazioni sensibili di grande valore nel mondo della criminalità [4, 5]. Nella riservatezza quindi comprendiamo anche una necessaria ed importantissima formazione specifica per tutti gli operatori che, in qualunque modalità ed a qualunque titolo, accedono ai dati di un db (a tal proposito vedere quanto successo presso l'ASL della Valle d'Aosta, appendice A a pag. 79), allo scopo di familiarizzare con i fattori di rischio. Ulteriori aspetti della formazione possono includere password complesse e best practice relative alle password o a fornire la conoscenza sui metodi di ingegneria sociale usati dai malintenzionati, così da cercare di impedire agli utenti il venir meno alle regole di gestione dei dati, fatto a volte con buone intenzioni, ma che porta a risultati potenzialmente disastrosi.

[1] Confidentiality, Integrity and Availability

- **Integrità** (I - Integrity) vuol dire mantenere la coerenza, l'attendibilità e l'accuratezza dei dati durante il loro intero ciclo di vita . I dati devono rimanere invariati durante il transito e devono essere adottate misure per garantire che non possano essere modificati da persone non autorizzate (ad esempio, in violazione della riservatezza). Queste misure includono la gestione delle autorizzazioni per la modifica dei file e controlli di accesso degli utenti. Inoltre, le organizzazioni devono adottare alcuni mezzi per rilevare eventuali modifiche nei dati che potrebbero verificarsi a seguito di eventi non causati dall'uomo come un impulso elettromagnetico (EMP[2]) o un arresto anomalo del server, molto utili sono quindi i cosiddetti **integrity check** del db programmati per essere effettuati a cadenza regolare. Devono poi essere disponibili backup o ridondanze per ripristinare il più in fretta possibile lo stato corretto dei dati interessati.

- **Disponibilità** (A - Availability) significa che le informazioni devono essere facilmente e costantemente accessibili alle parti autorizzate. Questo include la certezza che venga effettuata una corretta manutenzione dell'infrastruttura tecnica, dell'hardware e del software che contengono le informazioni. Ciò è garantito al meglio mantenendo rigorosamente tutto l'hardware, eseguendone le riparazioni immediatamente quando necessario e mantenendo un ambiente del sistema operativo correttamente funzionante e privo di conflitti software. È anche importante tenersi aggiornati con tutti gli update di sistema necessari. Fornire un'adeguata larghezza di banda di comunicazione e prevenire il verificarsi di colli di bottiglia sono tattiche altrettanto importanti. Ridondanza dei sistemi, procedure di failover, uso di supporti di dischi in configurazioni RAID[3], persino cluster ad alta disponibilità, possono mitigare gravi conseguenze quando si verificano problemi hardware. Il ripristino di emergenza rapido e adattivo è essenziale per gli scenari peggiori; tale capacità si basa sull'esistenza di un piano globale di ripristino di emergenza. Le salvaguardie contro la perdita di dati o le interruzioni nelle connessioni devono includere eventi imprevedibili come disastri naturali e incendi. Per prevenire la perdita di dati a causa di tali eventi, una copia di backup può essere archiviata in un luogo geograficamente isolato, forse anche in una cassaforte ignifuga e impermeabile. Dispositivi o software di sicurezza extra come firewall e server proxy possono proteggere dai tempi di inattività e dai dati irraggiungibili bloccati da attacchi DoS[4] dannosi e intrusioni di rete.

Quali sono quindi le pratiche migliori per implementare la triade della CIA? Nell'implementare la triade della CIA, un'organizzazione dovrebbe seguire una serie generale

[2]Electromagnetic Pulse

[3]Redundant Array of Independent Disks

[4]denial-of-service

di cosiddette "best practice". Alcune di queste, suddivise per ciascuna delle tre materie, includono:

- **Riservatezza** I dati devono essere gestiti in base alla privacy richiesta dall'organizzazione o dalle normative che si applicano in base alla tipologia di dati. Se possibile i dati andrebbero protetti utilizzando l'autenticazione a 2 fattori (2FA[5]) e la cifratura. Vanno mantenuti aggiornati gli elenchi di controllo degli accessi e gli altri permessi sui file.

- **Integrità** Assicurarsi che i dipendenti siano a conoscenza della conformità e dei requisiti normativi per ridurre al minimo l'errore umano. Utilizzare software di backup e ripristino. Infine, per garantire l'integrità, utilizzare il controllo della versione, il controllo degli accessi, il controllo della sicurezza, i registri dei dati e i checksum.

- **Disponibilità** Utilizzare misure preventive come ridondanza, failover e RAID. Assicurarsi che i sistemi e le applicazioni rimangano aggiornati. Utilizzare sistemi di monitoraggio della rete o del server. Garantire che sia in atto un piano di ripristino dei dati e continuità aziendale (BC) in caso di perdita di dati.

3.1 La cifratura del db

Nell'ambito della sicurezza dei dati sanitari, è di fondamentale importanza, oltre che obbligatorio per rispettare la normativa (vedi par. 2.3.4), che i dati del db siano protetti con un sistema di cifratura.

Quando si parla di dati, però, non si parla solo di quelli cosiddetti "a riposo" nel db, ma vengono suddivisi in 3 stati:

- Dati **in transito**: si tratta dello stato dei dati nel momento che questi vengono trasmetti dal server dove risiedono, al client che li visualizza, o ad altro server. E' quindi un stato dei dati comunque vulnerabile e che va perciò protetto. Solitamente si usano le tecniche di cifratura TLS[6] [11] o SSH[7] [12].

- Dati **in uso**: si tratta dello stato in cui i dati sono una volta giunti a "destinazione", cioè quindi nel client dove questi possono essere letti e/o elaborati, oppure in un altro server o altro sistema di archiviazione. Anche in questo stato i dati possono essere più o meno attaccabili a seconda delle diverse modalità di caricamento e lettura utilizzate dalle componenti hardware e software del sistema utilizzato.

[5] two factor authentication

[6] Transport Layer Security

[7] Secure Shell Protocol

- Dati **a risposo**: è questo lo stato in cui i dati si trovano quando non sono trasmessi o in uso quindi è lo stato in cui si trovano per la gran parte del tempo la maggioranza dei dati. Tutti i dati memorizzati su qualsiasi unità di archiviazione locale o remota appartengono a questa categoria. E' sui dati in questo stato che vanno applicate le maggiori accortezze riguardanti la loro protezione.

3.2 Cifratura dei dati a riposo

Esistono diverse tecniche per cifrare i dati a riposo di un database, ognuna di queste presenta vantaggi e svantaggi. Le elenchiamo brevemente di seguito, per poi soffermarci meglio su quella che, attualmente, presenta il migliore rapporto dei primi sui secondi che è la cifratura a livello di DBMS Engine e che è la tecnica di maggior diffusione e applicazione in quelli che sono i db relazionali utilizzati nei grandi sistemi aziendali, compresi quindi quelli in uso presso le aziende sanitarie, ed ai quali, come già detto, vanno dedicate particolari attenzioni.

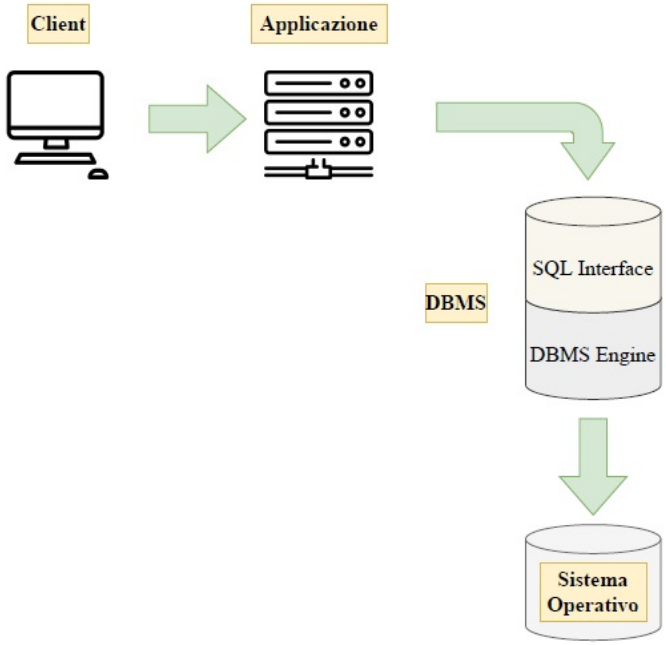

Figura 3.1. Architettura di un DB

3.2.1 Cifratura a livello di *Sistema Operativo*

Con questa tecnica i dati vengono criptati/decriptati direttamente dal sistema operativo durante le operazioni di lettura e scrittura sul disco.

Vantaggi:

- la completa trasparenza delle operazioni ai client ed alle applicazioni, che così non necessitano di essere modificati
- ampie possibilità di personalizzazioni dei controlli tramite l'uso di specifiche policy

Svantaggi:

- gli operatori con privilegi di amministrazione possono leggere i dati cifrati
- la gestione delle chiavi
- poca flessibilità nella scelta della granularità[8] del dato
- la cache del database, che contiene un gran numero di copie di pagine del disco (per aumentare le performance), viene tenuta in chiaro e perciò vulnerabile agli attacchi sui *Dati in Uso*

3.2.2 Cifratura a livello di *DBMS Engine*

Il **DBMS Engine** (o "motore" del database) è il modulo centrale di un DBMS[9] che gestisce le operazioni di input/output e il data storage nel database. Molti DBMS offrono delle funzionalità di cifratura integrate.

Abilitando la cifratura fornita da un DBMS Engine ogni volta che le informazioni vengono inserite o lette nel database queste vengono rispettivamente cifrate o decifrate in modo del tutto automatico. Per questo motivo questa soluzione non comporta nessuna modifica alle applicazioni esistenti.

Come scritto in precedenza (par. 2.3.3) riguardo gli articoli 33 [14] e 34 [15] del GDPR per quanto riguarda la notifica al supervisore e al proprietario dei dai nel caso di *data breach* [25], la comunicazione al proprietario dei dati può non avvenire se il db è cifrato. Visto che il furto dei dati rappresenta un enorme danno per l'azienda, l'utilizzo della cifratura a questo livello (e anche a livello client, v. par 3.2.5) può prevenire questo tipo di problemi.

Come detto sopra, con questa tecnica i dati vengono criptati e decriptati dal DBMS Engine, e questa funzionalità ha, tra i suoi maggiori vantaggi, quella di non richiedere modifiche alle funzionalità delle applicazioni che vi accedono.

La tecnica di cifratura a livello di DB più utilizzata è la TDE[10], la quale permette di cifrare e decifrare dati e file di log. Questa cifratura utilizza una DEK[11] che è una

[8] vedi paragrafo 3.2.6

[9] DataBase Management System

[10] Transparent Data Encryption

[11] Database Encryption Key

chiave simmetrica protetta da un certificato memorizzato nel DBMS. Si tratta di una tecnologia che può essere utilizzata per fornire alti livelli di sicurezza delle colonne, tabelle e tablespace[12].

La TDE cifra i dati prima che questi vengano scritti sul disco e li decifra prima di essere ritornati all'applicazione. I processi di cifratura/decifratura vengono eseguiti nel DBMS Engine in modo completamente trasparente alle applicazioni e agli utenti [27]. Inoltre, assicura che i dati a riposo non possano essere letti da individui malintenzionati che hanno l'intenzione di rubarli fisicamente o che hanno ottenuto i privilegi sulla macchina che ospita il DBMS. Infatti, anche se i file vengono compromessi o rubati, tutti i dati rimangono illeggibili, solo gli utenti autorizzati possono accedervi in chiaro. Quindi solo chi possiede la chiave di cifratura è in grado di comprendere i dati in quanto dati che non possono essere letti sono inutili, andando così a ridurre drasticamente l'incentivo per il furto.

Siccome la TDE effettua operazioni crittografiche a livello I/O all'interno del DBMS Engine è inoltre possibile aggiungere ai dati cifrati del **salt**[13] per evitare attacchi crittografici sul testo cifrato, come gli attacchi a "dizionario" [28, 29]. Un dizionario è una mappa chiave-valore dove la chiave corrisponde ad una stringa (generalmente una password) mentre il valore è l'hash della stringa corrispondente, calcolato con uno specifico algoritmo. Un attacco a dizionario consiste nel prendere come input un hash (corrispondente all'hash di una password) e controllare nel dizionario se esiste una coppia avente come valore l'hash di input, la password corrispondente è la chiave associata a quel valore. Il salt è una sequenza casuale di bit che viene aggiunto ai dati originali prima di calcolare l'hash rendendolo più casuale. Il salt viene generato casualmente ogni volta che viene ricevuto o calcolato un dato. Perciò un attaccante dovrebbe calcolare il dizionario per ogni possibile valore del salt e se questo ha grandi dimensioni rende infattibile questo tipo di attacco.

La maggior parte delle implementazioni permettono di cifrare i dati (a livello colonna o tablespace) utilizzando una chiave chiamata **TDE Encryption Key** mantenuta dal DBMS stesso. Tale chiave viene cifrata utilizzando una **TDE Master Encryption Key** che viene mantenuta in un modulo sicuro esterno.

Vantaggi:

[12] Un tablespace è una struttura di memoria contenente tabelle, indici, LOB (large object) e dati lunghi. Vengono utilizzati per organizzare i dati in un database in raggruppamenti di memoria logici che si riferiscono al punto in cui i dati vengono memorizzati su un sistema. I tablespace vengono memorizzati nei gruppi di partizioni del database.

[13] Letteralmente "sale".

- Non c'è bisogno di creare tabelle ausiliarie, trigger[14] o viste per decifrare i dati per gli utenti autorizzati. I dati vengono decifrati in modo trasparente. Un'applicazione che processa dati sensibili può usare la TDE per fornire una forte cifratura dei dati senza cambiare l'applicativo;
- Essendo i dati decifrati in modo trasparente, gli utenti che utilizzano il database possono non essere consapevoli che i dati a cui stanno accedendo sono memorizzati in forma cifrata;
- Flessibilità nella scelta della granularità del dato da cifrare [20];
- Burocrazia e immagine. Nel caso di *data breach* in cui i dati rubati siano cifrati non c'è bisogno di notificare il cliente, come detto negli articoli 33 e 34 del GDPR citati nel paragrafo 2.3.3.

Svantaggi:

- Key Management (vedi par. 3.3);
- Performance overhead: le operazioni crittografiche aggiungono del calcolo computazionale al DBMS rendendolo tendenzialmente più lento rispetto ad una soluzione che non effettua operazioni crittografiche;
- Storage overhead: la memorizzazione dei dati cifrati ne aumenta anche lo spazio occupato, per cui occorre gestire questo aumento in modo opportuno;
- La crittografia non si applica ai dati in transito, quindi è necessario combinare la TDE con altre tecniche (ad esempio, SSL/TLS).
- Benchè ancora molto utilizzata, la TDE è ormai potenzialmente violabile [21].

3.2.3 Cifratura a livello *SQL Interface*

Questa tecnica fornisce meccanismi, funzioni e librerie per elaborare i dati nel DBMS, come procedure, viste e trigger. Operare a questo livello permette allo sviluppatore di essere totalmente flessibile riguardo le operazioni che deve compiere sui dati. A questo livello è possibile connettere al sistema dei plug-in che permettono di cifrare e decifrare i

[14] Il trigger, nelle basi di dati, è una procedura che viene eseguita in maniera automatica in coincidenza di un determinato evento, come ad esempio la cancellazione, la modifica o la creazione di un record di una tabella. In questo modo si ha a disposizione una tecnica per specificare e mantenere vincoli di integrità anche complessi. I trigger permettono agli utenti di specificare vincoli di integrità più complessi dato che un trigger è essenzialmente una procedura SQL. Tale procedura è quindi associata ad una tabella e viene automaticamente richiamata dal motore del database quando una certa modifica (o evento) avviene all'interno della tabella. Le modifiche sulla tabella possono includere operazioni INSERT, UPDATE, e DELETE.

dati installando un opportuno modulo sul DBMS. Cifrare i dati a questo livello permette al DBMS Engine di ricevere i dati già cifrati e inoltre permette di selezionare la granularità così da migliorarne le prestazioni [22, 23, 24].

Vantaggi

- Performance: soluzioni ad-hoc possono essere adottate per diminuire l'impatto sulle performance delle operazioni crittografiche. Teoricamente si può cercare di ottimizzare la query in modo da ottimizzarne le performance, ma nei casi reali l'effetto migliorativo è trascurabile
- Flessibilità sia su DBMS commerciali che su DBMS open-source. Flessibilità in termini di granularità e gestione delle chiavi. Si possono cifrare dati diversi con diverse chiavi o con la stessa chiave. Massima libertà al programmatore

Svantaggi

- Key Management esplicito. L'utente deve implementare un corretto sistema di Key Management in quanto è lui stesso il proprietario delle chiavi crittografiche inserite nelle query
- Non è completamente trasparente. Infatti si può pensare di utilizzare dei trigger per automatizzare le operazioni crittografiche per i diversi statement SQL, ma la maggior parte dei vendor supportano ciò solo parzialmente
- Aumenta la complessità del codice (aumentando la probabilità di inserire nuove vulnerabilità) in quanto l'utente deve scrivere delle nuove query che contengono le chiamate alle funzioni crittografiche. E' responsabilità dell'utente gestire correttamente le operazioni crittografiche
- La cifratura avviene all'esterno del DBMS Engine e quindi alcuni meccanismi (indexing, foreign keys) potrebbero non funzionare correttamente [23]

3.2.4 Cifratura a livello *Applicazione*

La cifratura a questo livello viene eseguita nell'applicazione che invia (produce) e riceve i dati. Le funzioni di cifratura e decifratura vengono eseguite esternamente al DB senza aggravio computazionale sul gestore DBMS (il database non effettua operazioni di cifratura/decifratura dei dati). Cifrare a questo livello vuol dire quindi che è necessario che siano le applicazioni a dover essere sviluppate (o, eventualmente, modificate) in tal modo da poterlo fare.

Vantaggi:

- separazione delle chiavi di cifratura dai dati cifrati memorizzati nel database, la chiave non esce mai dall'applicazione

- flessibilità nella scelta della granularità dei dati
- flessibilità nella Key Management

Svantaggi:

- innanzitutto vi è un problema di sicurezza dovuto alla granularità che si desidera ottenere: l'applicazione infatti potrebbe aver bisogno di recuperare un insieme di dati più grande di quello effettivamente poi concesso all'utente. In questo modo infatti si lascia all'utente (o qualsiasi aggressore che abbia accesso alla macchina su cui gira l'applicazione) la possibilità di violare l'applicazione stessa per accedere a dati non autorizzati
- adattare alla cifratura applicazioni obsolete, ma che comunque sono e devono restare in uso, cioè le cosiddette applicazioni "legacy", comporta quasi sempre un enorme dispendio di ore lavoro, oltre che un'alta difficoltà, il ché si traduce in un grande impegno economico
- infine, si perde la possibilità di sfruttare i meccanismi del DBMS per l'ottimizzazione delle query, come ad esempio gli indici, molto utili per ottimizzare le operazioni di ricerca e quindi, più in generale, le performance

3.2.5 Cifratura a livello *Client* (Client-side encryption)

E' una modalità di cifratura che consiste nel criptare i dati direttamente nel client prima di essere trasmessi al server dove è attestato il DBMS e dove, quindi, i dati sono archiviati. Questo fa sì che i dati siano inaccessibili al gestore del servizio ed a tutti gli eventuali nodi/server che i dati potrebbero attraversare tra il database di questi ed il client, ed ha quindi grandi vantaggi dal punto di vista della sicurezza, soprattutto in alcuni specifici ambiti come quelli, sempre più in uso, dove i dati vengono gestiti da enti terzi nel cosiddetto "cloud". Questa tecnica di cifratura però non ha solo vantaggi, e per capirne meglio i possibili impatti vi è la necessità di fare alcuni approfondimenti su quello che ne deriva dal suo utilizzo, soprattutto per quel che riguarda gli indici e le operazioni di ricerca. Abbiamo detto che la cifratura avviene nel client, e quindi non è il DBMS Engine a gestirla, ma essendo comunque il DBMS Engine a dover eseguire le operazioni (cioè le query), le dovrà eseguire su dati di cui non ha conoscenza, andando così a perdere le opportunità di ottimizzazione sopracitate (come gli indici), a meno di non applicare specifiche tecniche che possono aggirare questo problema.

Tra le tecniche possibili vogliamo citare la *crittografia omomorfica*. Questa tecnica, teorizzata alla fine degli anni settanta, permette di fare operazioni su dati cifrati, ottenendo un risultato cifrato. Questo apre la strada a un livello di protezione dei dati e della privacy superiore.

Essa si divide a sua volta in:

- crittografia *parzialmente omomorfica* o PHE[15]. Questa, ottempera alla necessità di mantenere al sicuro i dati sensibili, ma consente solo a determinate funzioni matematiche di essere eseguite sui dati cifrati. All'interno di questa tipologia ci possono essere diversi livelli intermedi, se ad esempio l'elaborazione avviene su set diversi di dati cifrati, oppure per sottoinsiemi. Questo implica che solo una porzione delle informazioni, quelle indispensabili ai fini dei calcoli, debbano essere decifrate per ottenere dei risultati che siano conformi, mentre tutte le altre possono rimanere criptate

- crittografia *completamente omomorfica* o FHE[16] che può elaborare tutte le operazioni necessarie, ad esempio le operazioni aritmetiche o le funzioni booleane AND, OR, NOT e consente di mantenere tutti i dati cifrati durante l'elaborazione. Questa tipologia di crittografia è decisamente più ambita dato che garantisce altissimi livelli di privacy, perché consente di tenere le informazioni sempre al sicuro ma totalmente accessibili

Questo sistema crittografico trova la sua naturale applicazione in tutti quei settori altamente regolamentati, proprio come quelli della **sanità digitale**, dove è più forte l'esigenza di un trattamento dei dati sensibili che sia il più sicuro possibile e in grado di eseguire calcoli senza ridurre i livelli di privacy dei pazienti.

Per fare un esempio pratico, sarebbe possibile mantenere criptati tutti i dati personali non indispensabili dei pazienti (nome, cognome, domicilio, numero di telefono, ecc.), ed effettuare calcoli sui soli dati utili ai fini dello studio, come quelli per ottenere statistiche sull'incidenza delle malattie nella popolazione o per valutare l'efficacia dei vari farmaci. Addirittura, così facendo, l'azienda sanitaria potrebbe dare l'accesso ai dati ad un ente esterno specializzato in queste elaborazioni senza la necessità di chiedere il consenso a tutti i pazienti a cui tali dati afferiscono.

La crittografia omomorfa, inoltre, potrà trovare applicazione in moltissimi altri settori in futuro, come ad esempio la mappatura dei flussi di persone in un centro commerciale o lo studio del traffico automobilistico in una città, e potrà riscrivere le dinamiche del trattamento dei dati personali e anche le relative regole di protezione, rendendo obsolete alcune normative come il GDPR e il problema del trasferimento all'estero dei dati sensibili.

Lo svantaggio, ancora piuttosto impattante, di questa tecnica è che richiede un'enorme potenza computazionale da parte dell'hardware, cosa che però, con l'avanzare delle tecnologie, diventa sempre più disponibile ed a costi accettabili.

[15]Partially Homomorphic Encryption

[16]Full Homomorphic Encryption

3.2.6 Granularità nella cifratura dei dati

Abbiamo appena visto come le diverse tecniche di cifratura del db possono avere vantaggi o svantaggi anche dal punto di vista della possibilità di granularità di quello che si va a cifrare.

Per **granularità** intendiamo il dettaglio dei dati del db che si vanno a cifrare e cioè:

- **Intero tablespace**, per cui utilizzando una chiave univoca per ogni tablespace si andrà a cifrare l'intero contenuto di questa. E' una metodologia supportata dalla TDE e dalla client-side encryption, di semplice implementazione e con un basso impatto sulle prestazioni
- **Singola colonna**, per cui con questo metodo si vanno a cifrare singole colonne del db, ognuna con una diversa chiave. E' supportata anche questa dalla TDE e dalla client-side encryption. La cifratura con una granularità a livello colonna ha un più alto impatto sulle prestazioni (proporzionale al numero di colonne cifrate), ma una maggior flessibilità sulla scelta di quali dati (o quali tipologie di dati) andare a cifrare
- **Singolo campo**, vuol dire andare a cifrare una o più specifiche celle del db. Sebbene, in maniera proporzionale alla cifratura a livello colonna, le prestazioni siano ancora più inficiate da questo livello di granularità, essa ha il vantaggio di permettere di cifrare ogni cella con una chiave diversa, quindi con un altissimo livello di protezione, che può essere utile per specifiche esigenze. Viene incontro a questa tecnica, per non perdere troppo a livello di prestazioni, la cifratura a livello client di tipo omomorfico

3.2.7 Scelta dell'algoritmo e della modalità di cifratura

Abbiamo visto nei paragrafi precedenti i diversi livelli di cifratura e di granularità ma, indipendentemente da queste strategie, saranno l'**algoritmo di cifratura** (AES[17] [18], RSA[19] [20], ecc.), la lunghezza, la complessità della chiave e la protezione del db ad avere un peso determinante nella sicurezza finale dei dati. Oltretutto, anche adottando un forte algoritmo (come AES), tecniche evolute di analisi dei dati anche cifrati, possono riuscire a comprometterne il contenuto, se l'algoritmo non viene utilizzato in **modalità sicura**. Ad esempio, se l'algoritmo di crittografia è implementato in modalità ECB[21], blocchi di dati identici vengono cifrati in blocchi che, sebbene appunto, cifrati, saranno comunque

[17] Advanced Encryption Standard

[18] è un algoritmo di cifratura a blocchi a chiave simmetrica [9]

[19] RSA è l'acronimo di Ron Rivest, Adi Shamir e Leonard Adleman

[20] è un algoritmo di cifratura asimmetrica [10]

[21] Electronic Codebook

a loro volta identici, rivelando così schemi ripetitivi che, nell'ambito dei database, sono spesso comuni in quanto molti record potrebbero avere lo stesso contenuto.

É quindi molto importante fare attenzione quando si sceglie la modalità di cifratura. Inoltre, soluzioni semplici che possono funzionare in altri contesti, possono invece non fornire un adeguato grado di protezione nel contesto di un DBMS.

Tutte le specificità del contesto del database dovrebbero essere prese in considerazione per guidare la scelta di un algoritmo di crittografia adeguato e della sua modalità di funzionamento. Inoltre, la protezione dovrebbe essere abbastanza forte poiché è molto comune che i dati debbano essere gestiti e mantenuti per un periodo di tempo molto lungo (molti anni, anche decine) e quindi va fatta una valutazione molto accorta al fine di scegliere un algoritmo di crittografia e modalità di funzionamento che siano il più possibile all'avanguardia [6].

3.3 Key Management

Come si sarà notato nei precedenti paragrafi, la *Key Management* è una problematica comune a tutte le varie tecniche di cifratura descritte.

Per Key Management si indica il processo, a carico del DBMS Engine, di memorizzazione, scambio e ciclo di vita delle chiavi crittografiche. Se questo processo non funziona correttamente tutto il contenuto del database rischia di venire, sostanzialmente, perso, ed è per questo quindi che la gestione delle chiavi è una problematica da prendere seriamente in considerazione.

Affinchè un KMS[22] sia considerato valido, è importante che esso riesca a gestire correttamente questi 4 aspetti [26]:

- **Ciclo di vita delle chiavi**: è composto da 5 fasi, dalla creazione alla distruzione

    1. Pre-operatività: quando le chiavi non sono ancora disponibili per le operazioni di crittografia ma vengono create per un sistema configurato ed inizializzato in modo sicuro;
    2. Attivazione: la chiave può essere attivata subito dopo la sua creazione o dopo un lasso di tempo in modo automatico o manuale;
    3. Operatività e scadenza: quando le chiavi sono disponibili ed in uso per tutto il periodo definito della loro validità;
    4. Post-operatività: quando le non sono più in uso ma esistono ancora ed è possibile accedervi (ad esempio per recuperare vecchi backup cifrati con chiavi scadute);

[22] Key Management System

5. Distruzione: quando le chiavi non più disponibili. In caso di compromissione o semplicemente per inutilizzo, si può scegliere di eliminare definitivamente una chiave. Questa opzione impedisce definitivamente il ripristino di dati cifrati con quella chiave.

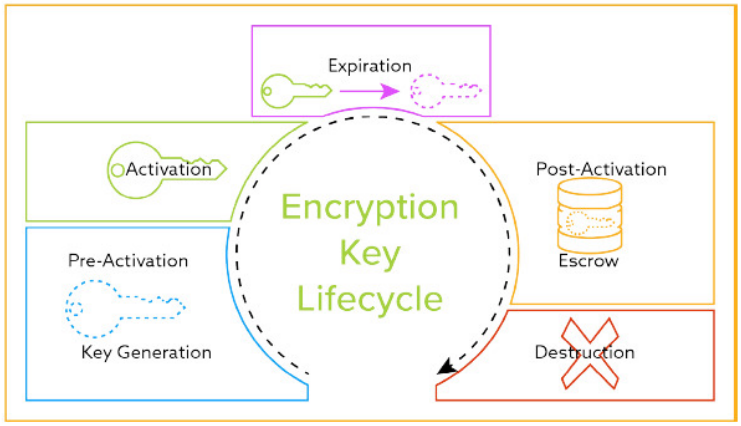

Figura 3.2. Ciclo di vita delle chiavi crittografiche

- **Accesso fisico alla chiave**: con questo si vuole intendere tutte le protezioni che il sistema fisico che ospita il KMS siano adeguate ed operative. Controllo dell'accesso fisico ai sistemi hardware, comprese le porte e le interfacce, sicurezza antincendio, integrità strutturale degli ambienti, gestione delle utenze (elettricità, aria condizionata, riscaldamento e relativi sistemi di backup), intercettazione dei dati, politiche di gestione degli accessi in remoto, protezione fisica specifica dei moduli crittografici hardware

- **Accesso logico alla chiave**: con questo si intende la separazione logica dei diversi componenti crittografici che ospitano le chiavi dal resto dei dati del DBMS

- **Determinazione degli utenti e ruoli che possono accedere alla chiave**: come ultimo punto abbiamo che il concetto fondamentale di riguardo gli utenti/ruoli è quello di "privilegio minimo", dove si limitano i privilegi di accesso del personale autorizzato (ad esempio, privilegi di esecuzione del programma, privilegi di modifica dei file) al minimo necessario per svolgere il proprio lavoro

Per quel che riguarda la gestione delle chiavi e, in particolare per il mondo della sanità digitale, esistono diverse normative emanate dalle principali nazioni che si sono preoccupate di normare la gestione della protezione dei database. In particolare, per quel che riguarda le normative che hanno specifici riferimenti alla protezione dei dati sanitari, abbiamo:

- HIPAA[23] e HITECH[24]: si tratta di 2 leggi statunitensi emesse con lo scopo di cercare una maggiore adozione ed un uso significativo della Key Management specificatamente per la **protezione delle informazioni sanitarie**. Esse sono state emesse al fine di stabilire dei *regolamenti*, anche allo scopo di avere la funzione di *linee guida*, per una corretta gestione della sicurezza dei dati e degli ePHI[25] [31]. La conformità alle HIPAA Security Rules e alle HITECH Privacy Rules per ePHI richiedono l'uso di tecnologie e best practices per dimostrare una forte adozione di misure di sicurezza per la Key Management [32]

- **GDPR**: il già citato regolamento europeo, negli articoli 32 e 34, va a definire un alto livello di priorità che le istituzioni devono assegnare nella protezione dei dati a riposo attraverso la cifratura. Siccome la gestione della Key Management è parte integrante della strategia di cifratura, deve avere anch'essa un'alta priorità affinché sia conforme alle leggi dell'Unione Europea [13]

3.4 La separazione dei dati nel db

Analogamente alla cifratura dei dati del db viene anche richiesto, come ulteriore forma di sicurezza, che i dati presenti nel db siano opportunamente "separati" a livello logico. Questo vuol dire, ad esempio, che le tabelle contenenti i dati clinici/sensibili, non devono avere "in chiaro" il nominativo della persona a cui appartengono ma solo un "riferimento" numerico (dr) alla/e tabella/e che contengono i dati anagrafici. In questo modo, se anche si riuscisse ad avere accesso in maniera fraudolenta ad alcuni di questi dati non si riuscirebbe a risalire alle persone a cui questi appartengono.

In un database "relazionale", ottenere la separazione dei dati è semplice e quasi "scontato". Ciò che in aggiunta a questo è sempre consigliabile è suddividere ulteriormente il db in diversi spazi di tabelle[26], così da ottenere un db meglio organizzato e strutturato, utile soprattutto quando si ha a che fare con db grandi e complessi come tendenzialmente sono i db che contengono grandi moli di dati sanitari, suddivisi tra dati anagrafici, dati clinici, ed un ulteriore ventaglio molto ampio di tutti quei dati che vanno a comporre un HIS.

[23] Health Insurance Portability and Accountability Act

[24] Health Information Technology for Economic and Clinical Health

[25] Electronic Protected Health Information

[26] Un spazio da tavolo è una struttura di archiviazione contenente tabelle, indici, oggetti di grandi dimensioni e dati lunghi. Vengono utilizzati per organizzare i dati in un database in raggruppamenti di memorie logiche che si riferiscono a dove i dati vengono memorizzati su un sistema. Gli spazi della tabella sono memorizzati nei gruppi di partizione del database. Nell'ecosistema Intersystems TrakCare vengono detti "namespace"

3.5 Anonimizzazione degli ambienti non di produzione

In un sistema complesso come quello sanitario atto a gestire , ad esempio, una intera ASL, si rende sempre necessario avere diversi "ambienti",. Oltre a quello solitamente detto di "produzione" o "live" vengono creati solitamente almeno altri 2 ambienti quasi del tutto gemelli di quello di produzione, che servono ad una moltitudine di scopi. Innanzitutto per "ambiente" vogliamo indicare tutti i server e relativi applicativi e db che compongono l'ecosistema di un'azienda sanitaria, HIS, LIS, RIS, ecc. come vedremo nel dettaglio nel capitolo 4.

Replicare quindi un intero ambiente, fatto da diversi applicativi i quali, a loro volta, possono necessitare di svariati server (il solo TrakCare di produzione ha bisogno di almeno 5 server: uno per il db, 2 cosiddetti "applicator" per la parte web in configurazione di high-avaibility, un server "shadow" dove viene copiato in tempo reale il db di produzione, uno o due server per gestire le integrazioni, un server per la produzione dei report e delle stampe. Questi server possono ovviamente essere virtualizzati, ma occupano comunque una quantità di risorse computazionali, di memoria e di spazio disco non indifferente, integrarli tra di loro e manutenerli è anch'essa un'attività onerosa, ma con molteplici vantaggi a seconda di come e quali server di un ambiente vengono replicati.

Ad esempio si può fare un ambiente gemello di quello di produzione ma "parziale", con solo i sistemi principali (come quelli appena citati), tralasciando piccoli sistemi "verticali" meno utili ai fini che descriveremo a breve.

Gli ambienti così creati possono avere svariate funzioni, vediamo alcuni esempi:

- CLONE: è un ambiente che come dice il nome, è la copia di quello di produzione, che viene replicato con procedure automatiche solitamente quotidianamente ed ha lo scopo di mettere a disposizione dei tenici una copia costantemente aggiornata, utile a poter sopperire ad eventuali modifiche o problemi inaspettati dovuti ad errate configurazioni, utilizzandola come punto dove poter rivedere la configurazione o i dati precedenti alla modifica non voluta;

- TRAINING: è un ambiente che, come dice il nome, viene solitamente utilizzato per la formazione degli operatori, o per testare le modifiche prima di metterle in produzione. Viene solitamente replicato, sempre a partire da quello di produzione, con una frequenza non molto elevata, nell'ordine di qualche mese;

- SVILUPPO: è un ambiente utilizzato dai tecnici per, appunto, sviluppare o implementare le modifiche importanti o del tutto nuove all'applicativo. Viene replicato con una bassa frequenza perché nel farlo senza le dovute accortezze si andrebbero a perdere eventuali sviluppi non ancora salvati o portati in produzione.

A livello di sicurezza dei dati, però, tutti questi ambienti soffrono di un difetto intrinseco. Esso consiste nel fatto che, pur essendo ambienti fatti solo per test, per sviluppi o per avere una copia facilmente accessibile delle configurazioni senza andare ad utilizzare l'ambiente di produzione, ci sono comunque tutti i dati "veri" di tutti i pazienti. Cosa

in realtà solitamente inutile in questi contesti, oltre che "pericolosa". Per sopperire a questo si usa allora applicare dopo ogni clonazione di questi ambienti, una procedura di "scrambling" delle anagrafiche. Questa procedura va, come dice il nome, a scambiare in maniera casuale i principali dati anagrafici delle anagrafi presenti, nomi, cognomi, date di nascita, codici fiscali, mentre per altri dati meno importanti rispetto alla loro univocità, (indirizzi o numeri di telefono, stato civile, ...) li va direttamente a cancellare o sostituire con testi fissi.

Una volta applicata la procedura di scrambling i dati presenti in questi ambienti sono completamente anonimi e così da poter essere utilizzati per gli scopi suddetti senza pericolo di incorrere in violazioni dei dati non volute.

3.6 Le politiche di backup

Quando si parla di sicurezza dei dati, non ci si deve fermare esclusivamente all'ambito della potenziale minaccia dovuta all'accesso fraudolento ad un database, ma bisogna anche considerare la perdita più o meno accidentale dei dati, e quindi la necessità primaria di un loro backup costante, e sicuro, al fine di poter tempestivamente recuperarne il contenuto.

Ci sono diverse metodologie per il backup dei dati di un database, alcune di queste non sono esclusive tra loro ma possono, e molto spesso devono, essere usate in concomitanza tra loro.

Sottoporre un database ad un costante backup è il primo passo, ma va considerata anche la procedura di "restore" dei dati che, in caso di necessità, può risultare un'operazione lunga e tutt'altro che scontata in termini di successo. A tal proposito infatti, il tempo di ripristino dei dati è un fattore critico in un ambiente, come quello sanitario, dove il personale si può facilmente trovare a lavorare in un contesto di emergenza dove anche lì, ormai, si è sempre più dipendenti dall'informatica, e la possibilità di avere accesso ai dati clinici di un paziente (siano essi passati, cioè la sua "storia clinica", ma siano anche essi quelli presenti, come i risultati di esami del sangue o di immagini radiologiche appena effettuate), possono essere fondamentali in un processo di cura in un momento di emergenza. Ecco perchè, come accennato prima, è bene utilizzare più metodi di backup in concomitanza tra loro, così da avere più possibilità di ripristino a seconda della situazione e di che tipo di problema ne ha causato la perdita o anche solo la temporanea indisponibilità.

Infine, non si deve sottovalutare che i backup occupano anch'essi, e più ancora del database stesso, una quantità di spazio che le Aziende non possono ignorare nella gestione complessiva di un sistema informativo.

3.6.1 I log (o tracciatura) e la retention dei dati

Forse non si possono formalmente considerare un sistema di backup, ma per certe situazioni essi sono il primo punto di accesso per capire cosa è successo a determinati dati.

La tracciatura dei dati consiste nel mettere determinate tabelle, o campi di essere, o interi tablespace costantemente sotto "audit" tracciando in appositi file di log tutte le modifiche, che consistono in inserimenti, aggiornamenti o cancellazioni ai dati che si è scelto di mettere sotto tracciatura. In aggiunta a questo, la normativa in ambito di DSE prevede che siano tracciati anche i soli accessi in lettura ai dati clinici dei pazienti.

Tutto assieme questo "costa" moltissimo in termini di spazio occupato da questi file di log, almeno fino a quando li si deve archiviati. La normativa prevede comunque un tempo minimo per cui un'azienda è obbligata a tenerli (solitamente 2 anni) dopodiché è facoltà dell'azienda decidere se cancellare quelli più vecchi.

Per dare un'idea dello spazio che la tracciatura delle attività in un database occupa, dobbiamo dividere quella che è l'occupazione data dalle attività normali di un applicativo HIS e che comprende quindi la crescita dovuta all'inserimento dei dati che ogni giorno viene fatta dagli operatori, rispetto all'occupazione dovuto al mantenimento della "tracciatura" di ciò che gli operatori fanno anche solo "guardando" i dati. Come accennato infatti in 2.1 anche il solo dover mantenere disponibile il log di quanto gli operatori non solo "fanno" (cioè inseriscono o modificano sul database) ma anche solo "guardano" comporta un'occupazione di spazio non indifferente. A titolo di esempio, nell'installazione TrakCare presso l'ASL della Valle d'Aosta i dati di log hanno una crescita di circa 85mb al giorno, che vogliono dire quindi 2.5GB/mese circa. Viene da sè va sempre accuratamente pianificata e monitorata l'occupazione di spazio fisico sui dischi dei server e lo spazio disponibile.

3.6.2 I "journal" e lo "shadow"

Siccome i backup di un database sono delle "fotografie" fatte ad intervalli regolari (ogni ora, ogni giorno, ogni settimana, ecc. . .), in caso di perdita improvvisa del database ci si perderebbe quanto fatto dal momento dell'ultimo backup fino al momento della perdita del database. Un modo specifico di alcuni DBMS per mantenere un traccia costante delle modifiche che avvengono è quello di scrivere in appositi file, detti appunto "journal", tutte le transazioni che avvengono sul database. In caso di perdita del database è praticamente possibile ricostruirne uno gemello a partire dall'ultimo backup e applicandoci il file di journal creato da quel momento in poi.

Sfruttando i "journal", poi, è possibile implementare un sistema gemello, che per ovvie ragioni è bene sia dislocato fisicamente in un posto diverso dal database originale, che leggendo costantemente il file di journal ricrea in tempo quasi-reale un database uguale all'originale e detto, appunto, "shadow".

3.6.3 I backup su NAS o SAN e poi su nastri

Il backup classico di un database è quello che viene effettuato ad intervalli regolari (ogni ora, ogni giorno, ogni settimana, ecc. . .) su sistemi NAS[27] o SAN[28] affinché possa essere disponibile in maniera abbastanza rapida per un eventuale "restore". Questi file di backup sono conservato per un tempo deciso a livello aziendale in base anche allo spazio disponibile nei NAS o nelle SAN che ovviamente non è "infinito" e quindi bisogna giungere a dei compromessi tra la scelta "ideale" di conservare tutti i backup per sempre su sistemi di rapido accesso e quella "reale" in ci si deve confrontare con una disponibilità di spazio che è comunque sempre limitata.

Un compromesso alle necessità di archiviazione dei backup a lungo termine e, nondimeno, come ulteriore misura di sicurezza, questi backup o alcuni di essi, vengono salvati su sistemi di **backup a nastro** i quali, benché lenti nel loro eventuale ripristino, garantiscono un sistema sicuro di archiviazione dei dati nel lungo periodo (purché i nastri siano conservati in luoghi idonei e sicuri).

[27] Network Attached Storage

[28] Storage Area Network

Capitolo 4

I sistemi sanitari ed il passaggio delle informazioni tra essi

Finora abbiamo citato, in particolare, l'HIS, un software sanitario che, sebbene sia quello che possiamo senza dubbio identificare come **centrale** per importanza all'interno di un'azienda sanitaria, non è però, ovviamente, l'unico presente.

Infatti, sebbene l'HIS sia l'applicativo sanitario aziendale più diffuso o cosiddetto "trasversale", esistono all'interno di un'azienda ospedaliera una moltitudine di reparti, uffici, servizi, che hanno necessità specifiche che un software "orizzontale" non è detto che riesca fornire, perché non nasce per coprire esigenze troppo "specifiche" e che vengono quindi espletate da altri e più specifici software che vengono quindi genericamente definiti come "verticali". Alle volte questi verticali possono anche essere definiti applicativi **"dipartimentali"**, in quanto utilizzati per funzioni necessarie solo a singoli dipartimenti, come ad esempio il RIS che viene utilizzato essenzialmente solo presso i reparti (o dipartimenti) di **Radiologia** (più propriamente di definiscono "Diagnostica per immagini") o il LIS per il dipartimento di **Laboratorio Analisi**. Altri verticali non è detto che siano però anche dipartimentali, in quanto magari usati da servizi più "diffusi" come il CUP.

Tutti insieme questi applicativi vanno a comporre un SIS[1], cioè un insieme ordinato di elementi che raccolgono, elaborano, scambiano, ed archiviano i dati con lo scopo di fornire informazioni alle persone che svolgono attività legate alla salute umana. I SIS trattano quindi principalmente dati sanitari, ma non solo; trattano infatti anche dati amministrativi, contabili, finanziari e tecnici necessari a far funzionare l'azienda sanitaria nel suo complesso.

Questi applicativi che sono oggi a disposizione consentono di assolvere alla maggior parte dei bisogni informativi delle aziende sanitarie. I dipartimenti informatici delle

[1] Sistema Informativo Sanitario

aziende sanitarie (e le persone che vi lavorano) hanno acquisito negli anni un ruolo sempre più importante all'interno dell'infrastruttura aziendale in quanto hanno l'onere di gestire un insieme di software molto eterogenei, realizzati in tempi diversi, da ditte diverse, con tecnologie differenti e per sistemi operativi non più sul mercato (o, perlomeno, in versioni non più supportate dalle case produttrici).

Prima di affrontare nel prossimo capitolo come questi sistemi dialogano tra loro, e come quindi viene affrontato l'aspetto della sicurezza, vediamo una breve disamina dei principali tipi di applicativi in uso presso un'azienda sanitaria. Come già scritto, mentre alcuni di questi servono a specifiche esigenze, ad esempio della diagnostica (radiologia, laboratorio analisi) altri sono usati più trasversalmente con l'**anagrafica centrale** o, come già detto, l'HIS. Al di fuori delle mura aziendali ci sono poi sistemi usati su scala regionale (come il già citato FSE) o nazionale, come i sistemi Sogei/SistemaTS, che espletano funzioni quali le ricette dematerializzate, o ANA[2] e ANPR[3] per l'anagrafe nazionale.

Non bisogna poi trascurare l'aspetto della **disponibilità** di questi sistemi dai quali dipendono le scelte che un operatore sanitario (tipicamente un medico) può o non può fare per la cura e, potenzialmente, per la vita di un paziente (soprattutto in contesti "emergenziali"). E' perciò di primaria importanza dotare l'hardware, le reti elettriche, le reti informatiche di sistemi di ridondanza che si affiancano ai sistemi primari e che, nelle emergenze, ne assumano le funzionalità. Al giorno d'oggi perciò la disponibilità dei sistemi non è più un requisito aggiuntivo, ma una caratteristica che deve essere intrinseca in ogni sistema informatico fin dalla sua progettazione (privacy by design) e, oltre alla ridondanza delle apparecchiature e hardware e software, ai sistemi di backup citati in precedenza, devono essere redatti piani di Disaster Recovery e Continuità Operativa.

Oltre alla disponibilità dei dati questi sistemi devono garantire l'**integrità dei dati**, che consiste nel mettere in campo più azioni e a vari livelli. Parlando di database anagrafici l'uso di archivi centralizzati e normalizzati permette di effettuare sia controlli interni che esterni all'azienda. Per controlli *interni* intendiamo ad esempio gli incroci di dati per trovare record duplicati, record anonimi, o incongruenze di altro tipo che vanno corrette, funzionalità solitamente presenti negli applicativi MPI[4] (v. par. 4.2) . I controlli *esterni* invece si fanno, ad esempio, incrociando la base dati anagrafica con i corrispondenti archivi anagrafici presenti sulla ANPR, con l'anagrafe dell'Agenzia delle Entrate, con gli archivi comunali. L'integrità consiste anche nel tracciare tutte le azioni di modifica, inserimento o anche solo lettura dei dati compresi l'autore, la data e l'ora, salvando tutto su appositi file di log conservati per un periodo opportuno di tempo (solitamente non inferiore a 24 mesi).

[2] Anagrafe Nazionale Assistiti

[3] Anagrafe Nazionale Popolazione Residente

[4] Master Patient Index

L'integrità dei dati è una responsabilità che è in capo al Titolare del trattamento il quale, opportunamente, consentirà l'accesso ai dati dell'Azienda solo al personale opportunamente autorizzato tramite una procedura di autenticazione. Anche gli accessi devono essere salvati in specifici file di log completi di tutti i dati necessari per risalire a chi, quando e da che postazione ha fatto accesso. Spesso vengono salvati anche i tentativi di accesso falliti, allo scopo di intercettare eventuali tentativi fraudolenti da parte di persone (o, sempre più spesso, di sistemi automatici) non autorizzate.

Vediamo ora quali sono i principali software applicativi sanitari che, integrati tra di loro, vanno a comporre un SIS.

4.1 HIS

Alle volte, in alcuni contesti, si tende a considerare l'HIS come l'insieme dei singoli software "verticali" o "dipartimentali", confondendolo, cioè, con il SIS. Nell'esperienza di chi scrive, invece, l'HIS in uso per l'Azienda USL della Valle d'Aosta (ma anche presso numerose altre Aziende Sanitarie italiane, come Città della Salute a Torino, o presso l'Azienda Ospedaliera Universitaria di Verona), espleta funzionalità trasversali ad una moltitudine di dipartimenti e servizi tra le quali: ADT, Order Entry, Order Filler, CUP, EPR[5], CCE, DSE, gestione Pronto Soccorso, OBI[6], gestione sale operatorie, terapia farmacologica, refertazione ambulatoriale, gestione letti ospedalieri, statistiche ed elaborazione dati, produzione di report ed etichette.

Uno spettro così ampio di funzionalità implica un'alta complessità fin dalla sua creazione e altrettanto nella sua manutenzione ordinaria e straordinaria e nel suo bisogno costante di "adattamento" a delle necessità che cambiano rapidamente in un contesto sanitario, sia per questioni di **evoluzioni normative** ma anche per evoluzioni e modifiche che costantemente un ospedale ha al proprio interno come modifiche e aggiornamenti alla struttura dei reparti, delle sale operatorie, l'aggiunta di funzionalità evolute come ad esempio la farmacoterapia, la firma digitale dei referti o degli altri documenti clinici prodotti, estensioni dei servizi di prenotazione che consentono ai cittadini di prenotarsi in autonomia alcune prestazioni (magari attraverso il proprio FSE), e tanto altro. Questo si traduce in una continua necessità di evoluzioni ed adattamenti che i tecnici devono fare al software.

Conseguentemente, vi è la necessità di personale esperto il quale ha bisogno di un lungo periodo di apprendistato per padroneggiarne tutte le funzionalità. Si tratta infatti di un percorso che difficilmente un tecnico informatico può aver intrapreso e maturato in altre esperienze lavorative se diverse dal mondo sanitario, in quando si tratta di applicativi

[5]Electronic Patient Record

[6]Osservazione Breve Intensiva

impiegati in quella che, alla fine, è una "nicchia" del mondo informatico e che si definisce "informatica sanitaria".

Vediamo un pochino più nel dettaglio alcune delle principali funzionalità di un HIS (come TrakCare):

- **CUP**: le funzionalità di "prenotazione" implicano la preventiva creazione di "agende", fatte da sessioni e slot in cui poter prenotare set di prestazioni affini, gestione dei cataloghi di prestazioni, emissione di stampe di appuntamenti e cedole di pagamento. Solitamente questa funzionalità si integra a sua volta con sistemi automatici di pagamento, i cosiddetti "totem" o con il nodo di pagamento nazionale "PagoPA", con il FSE del cittadino, o con sistemi automatici per l'invio di mail ed sms per ricordare all'interessato l'appuntamento. Spesso poi in una regione con più Aziende Sanitarie, i singoli CUP "aziendali", si integrano tra di loro attraverso un "sovra-CUP" regionale, allo scopo di ottimizzare meglio e mettere a fattor comune le risorse e le "disponibilità" di ogni Azienda o, sempre più spesso ormai, anche di realtà sanitarie private a cui le aziende pubbliche si appoggiano convenzionandole per espletare le prestazioni in cui sono carenti di disponibilità rispetto alle richieste;

- **ADT**: le funzionalità di ADT riguardano principalmente la gestione dei ricoverati ("degenti" o "pazienti interni") e consentono di gestirne la posizione "fisica" all'interno di un ospedale (reparto/corsi/camera/letto) i dati principali di ricovero, soprattutto quelli amministrativi utili alla gestione economica e fiscale dell'episodio;

- **Order Entry/Order Placer**: con questo termine si indica la gestione informatica delle richieste di prestazioni, siano esse di esami di laboratorio ma anche di visite, consulenze, esami strumentali o altro. Dietro ad una richiesta di prestazioni viene gestito tutto l'iter autorizzativo (a seconda del ruolo dell'operatore si può permettere o meno di richiedere certe categorie di prestazioni, e l'eventuale stampa automatica di etichette da applicare sulle provette o fogli accompagnatori alla richiesta, così come le note o il quesito clinico ad essa associata). L'uso di un sistema informatico permettere agevolmente di tenere traccia delle richieste e dei relativi conteggi, statistiche, calcolo dei costi,ecc. Detto molto semplicemente si tratta della funzionalità di poter richiedere (o "ordinare") delle prestazioni che, a seguire, dovranno essere ricevute dall'applicativo stesso o, tramite integrazione, da un altro applicativo dove poi un operatore (medico, tecnico, ecc...) o un apparato (analizzatore di laboratorio, strumento per gli ECG[7], ecc...) le dovrà eseguire e dovrà produrre un referto o dei risultati;

- **Order Filler**: è la funzionalità di un applicativo di produrre un referto, o un risultato proveniente da uno strumento, relativo alla prestazione che è stata richiesta

[7] Elettrocardiogramma

attraverso l'Order Entry, e renderla disponibile. Alcuni applicativi, come, appunto, l'HIS possono svolgere contemporaneamente entrambe le funzioni;

- **CCE**: fondamentale nel processo di diagnosi e cura del paziente, la CCE non rappresenta una semplice trasposizione in digitale di quella che una volta era la Cartella Clinica Cartacea, ma una vera e propria evoluzione nella quale si concentrano tutte le informazioni cliniche riguardanti un episodio di ricovero di un paziente. Viene anche detta EMR[8] o EPR, e viene aperta al momento dell'accettazione del ricovero e si chiude, solitamente, alla dimissione di questo[9]. A livello legale è normata la possibilità per una struttura sanitaria di conservare le CCE esclusivamente in forma digitale, scansionando eventualmente quei documenti ancora solo cartacei (si parla in questo caso di Cartella Clinica "ibrida") anche se è ovviamente preferibile che tutto ciò che compone la Cartella Clinica sia "nativamente" digitale. La CCE non raccoglie solo le informazioni cliniche dell'episodio, ad uso del personale medico e infermieristico, ma anche alcune informazioni amministrative come il piano di pagamento o la convenzione con cui l'episodio viene registrato e che potrà dare luogo, eventualmente, ad una fattura verso un ente terzo (ad esempio un'assicurazione del quale un paziente potrebbe essere dotato). Alla chiusura della cartella vengono solitamente emessi 2 ulteriori documenti:
  - LDO[10]: che rappresenta la sintesi di tutto quanto avvenuto durante il ricovero e le prescrizioni per il paziente per il post-ricovero
  - SDO[11]: che viene "calcolata" attraverso uno specifico software (denominato "Grouper") richiamato, in maniera trasparente per l'operatore (il medico) che la compila e che, in base alle diverse informazioni presenti nella cartella (durata del ricovero, diagnosi e procedure eseguite, . . .), calcola un "codice" (numerico) che rappresenta sostanzialmente il "costo" di quel ricovero
- **DSE**: se ne è parlato in maniera approfondita nel par. 2.1 per via delle forti implicazioni che questo strumento ha nei confronti del rispetto della privacy, ed è l'insieme di tutti gli episodi clinici passati di un paziente presenti presso la struttura. Esso rappresenta per il medico uno strumento che, forse più degli altri, è utilissimo, per non dire fondamentale, per poter avere in un unico punto una visione d'insieme della storia clinica del paziente. Paziente che alle volte può non ricordarsi esattamente

[8] Electronic Medical Record

[9] C'è un'eccezione a questo dovuta al fatto che alle volte, sopratutto a seguito di episodi di ricovero che hanno implicato una procedura chirurgica, alcuni esami, in particolare quelli di Anatomia Patologica, impiegano svariati giorni, o settimane, per elaborarne i risultati, comportando questo la necessità "virtuale" di tenere aperta la CCE del paziente anche oltre la sua dimissione, fino all'arrivo dei risultati mancanti, fondamentali spesso per il medico per poter decidere sull'eventuale proseguo di altre cure

[10] Lettera di Dimissione Ospedaliera

[11] Scheda di Dimissione Ospedaliera

cosa e quando ha avuto un certo evento clinico, oppure può essere incosciente o non in grado di esprimersi al momento del ricovero.

- **Pronto Soccorso e OBI**: all'interno di un HIS può esserci[12] la gestione specifica del flusso detto anche EMUR[13] che comprende la possibilità di accettare e gestire attraverso percorsi specifici gli accessi in Pronto Soccorso (che può essere "generale" oppure specifico come il Pronto Soccorso Ostetrico-Ginecologico, il Pronto Soccorso Pediatrico, il Pronto Soccorso Psichiatrico, . . .), assegnando ad esempio i codici colori in base alla gravità del paziente o percorsi rapidi per specifici tipi di problemi. Un accesso in Pronto Soccorso si può concludere in vari modi tra cui, in particolare un episodio di tipo OBI per poter monitorare per un breve tempo un paziente prima di decidere se dimetterlo al domicilio o ricoverarlo.

- **Blocco Operatorio**: la gestione del blocco operatorio prevede tutta una serie di elementi tra cui una vera e propria "agenda" per le prenotazioni delle varie sale da parte dei diversi reparti chirurgici in base ai tipi di intervento, della diverse tipologie di operatori che ogni intervento richiede e della loro disponibilità, e anche in base ai diversi tempi di occupazione (che possono essere sempre e solo stimati). Alla fine di ogni intervento chirurgico, che deve essere censito con specifiche numerazioni univoche, date le ovvie implicazioni anche legali che ogni intervento porta con sè, il chirurgo "principale" redige uno specifico referto denominato VAO[14]. Mentre il medico anestesista compila la Cartella Anestesiologica. Entrambi sono documenti che verranno a far parte della CCE dell'episodio.

4.2 MPI

Si tratta di un applicativo anch'esso trasversale e non dipartimentale **estremamente importante** all'interno di un'Azienda Sanitaria. Questo software si colloca sostanzialmente come "centro stella" di tutti gli interscambi anagrafici e riveste un ruolo di fondamentale importanza nella **sicurezza del dato anagrafico**. Bisogna considerare infatti che praticamente tutti gli applicativi clinici, che si occupano cioè di gestire nei diversi modi i dati dei pazienti, funzionano in modalità "paziente-centrica". Questo termine è usato per indicare che la prima cosa che solitamente un operatore fa nel suo flusso di lavoro è quella di individuare *con certezza* l'anagrafica del paziente su cui deve "lavorare". Operazione questa tutt'altro che scontata in un sistema dove, con molta facilità, si trovano centinaia di migliaia di record anagrafici, compresi tantissimi record "sporchi", cioè errati, finti, anonimi, non riconosciuti o, anche, molto spesso **duplicati**.

[12] ma esistono anche applicativi verticali specifici che fanno solo quello

[13] Emergenza-Urgenza

[14] Verbale di Atto Operatorio

Scopo di un MPI è quindi quello di censire e, costantemente, tenere aggiornate ed allineate tutte le basi dati anagrafiche locali che ogni applicativo che fa parte del SIS contiene al proprio interno. E lo fa funzionando innanzitutto come archivio centrale di tutte le anagrafiche che, nel tempo, transitano in un'Azienda Sanitaria. Esso lavora poi come router verso gli altri applicativi per ogni nuovo inserimento o modifica di record anagrafico. Trattandosi innanzitutto di un archivio, il MPI assegna ad ogni record anagrafico un identificativo univoco (ID-MPI), diverso dal codice fiscale, e lo comunica, insieme a tutti gli altri dati che compongono il record, agli altri applicativi, i quali recepiranno il record (nuovo o modificato) ed i suoi altri dati ad esso connessi[15] (o almeno quelli di interesse) lo inseriranno all'interno del loro archivio ed useranno l'ID-MPI per comunicare informazioni riguardo quell'anagrafica tra di loro (ad esempio la richiesta di una prestazione, o l'invio di un referto).

Ma non solo: esso deve contenere al suo interno alcune **funzioni evolute** atte a rilevare le **anagrafiche duplicate**, in quanto palesemente doppie o anche solo "simili", inserite cioè più di una volta ma riconducibili alla stessa persona. L'individuazione delle anagrafiche duplicate (operazione detta di "swiffer", "spazzolatore"), **soprattutto se simili ma non esattamente uguali**, è un'attività tutt'altro che semplice, che si avvale di algoritmi matematici come l'algoritmo di "distanza di **Levenshtein**"[16], che permette di rilevare quei record presumibilmente creati doppi a causa di errori di battitura degli operatori grazie a delle "assonanze". Una volta che lo spazzolatore ha individuato le anagrafiche duplicate (che per via del costante allineamento che MPI fa verso tutti gli altri applicativi saranno duplicate anche in questi), indicandone la probabilità con la quale due o più anagrafiche sono in realtà la stessa, queste andranno "fuse" (l'operazione è detta "merge") ma solo dopo un ulteriore ed accurata valutazione fatta anche dal personale umano (esiste solitamente un apposito "Ufficio Anagrafe" che ha, insieme a molti altri, anche questo compito), in quanto la delicatezza è estrema dato che l'operazione di merge fa unificare anche tutti gli eventuali dati clinici (referti di visite, di atti operatori, allergie o malattie possedute, ecc...) verso l'unica anagrafica valida restante. Il rischio, in caso di errore, cioè in caso in cui quei 2 record non erano comunque in realtà della stessa persona, è quello che vedere sparire i dati dell'anagrafica "slave" e che l'anagrafica "master" si ritrovi associati referti, o comunque dati personali sensibili altrui.

---

[15] Un record anagrafico è, come minimo, composto dai 5 dati fondamentali che, assieme, vanno a comporre il codice fiscale e che sono cognome, nome, luogo e data di nascita, sesso. Vi sono poi i dati di residenza, eventuale domicilio, se ha l'assistenza sanitaria e di quale ASL, il Medico di Medicina Generale (MMG) o il Pediatra di Libera Scelta (PLS) associato, altri identificativi anagrafici specifici di altri software o nazionali, come il prossimo ID-ANA, oppure dati di altro tipo, come le esenzioni di patologia, condizione o reddito, i consensi prestati, se l'anagrafica è deceduta, lo stato civile, il grado di istruzione, la condizione lavorativa, ecc.

[16] Questo metodo valuta la differenza alfabetica tra due stringhe, così da valutare quanto due stringhe come, ad esempio, due cognomi, due nomi, 2 date di nascita, due codici fiscali, sono simili. Il risultato del confronto tra queste stringhe produrrà un valore compreso tra 0 e 1, dove, se 1 vuol dire che i due campi sono esattamente uguali

Di per sè, quindi, il MPI contiene soprattutto dati anagrafici, ma potenzialmente anche dati sensibili (vedi, ad esempio, le esenzioni di un paziente che, ad esempio quelle per patologia, o malattia rara, rappresentano un'informazione appunto "sensibile" sullo stato di salute) e dalla certezza dei suoi dati dipende poi la sicurezza di tutti gli altri dati (quindi soprattutto quelli sensibili) che alle anagrafiche sono collegati. E' perciò un elemento fondamentale per tutti i software che fanno parte di un SIS.

4.3 LIS

Il LIS è quel software deputato alla gestione delle attività del laboratorio analisi. Queste attività vanno dal momento del prelievo dei campioni, alla loro analisi, fino alla generazione, firma, stampa, conservazione e condivisione dei referti. Il LIS lavora in stretta sinergia con il HIS che svolge la funzione di *order entry* (o di *order placer*, v. par. 4.1), mentre il LIS è, naturalmente, l'*order filler* (v. par 4.1). I dati che un LIS tratta rientrano ampiamente nella categoria dei **dati particolari** e vanno predisposte tutte le misure necessarie alla loro protezione. Ci sono poi dei casi specifici in cui i dati (cioè, in questo caso, i risultati/referti) devono essere prodotti con i "metadati" specifici per la loro protezione, affinchè tutti i "consumer" (cioè i software che andranno a "leggere" quei referti), ne tengano opportunamente conto nelle logiche di autorizzazione verso chi può andarli a visualizzare. Ad esempio, i referti degli esami per individuare la sieropositività andranno sempre prodotti con i metadati di "oscuramento ex-lege" (v. par. 2.1), e questo deve essere fatto a prescindere dal risultato (positivo o negativo che sia) per l'ovvio motivo per cui se si oscurassero solo gli esiti "positivi" questo sarebbe già un'indicazione dell'esito stesso.

4.4 RIS e PACS

Il RIS ed il PACS[17] sono 2 software che lavorano in stretta sinergia dedicati in particolare ai cosiddetti reparti di Diagnostica per Immagini (un volta si diceva semplicemente "Radiologia"). I 2 sistemi vivono in simbiosi e sono fortemente integrati tra di loro attraverso gli standard HL7 e DICOM, tant'è che spesso ci si riferisce al "RIS-PACS" come un unico elemento.

Andando un po' più nel dettaglio, il RIS è un verticale specifico per la gestione dell'ambito della diagnostica per immagini, si integra con l'HIS per la ricezione delle richieste di prestazioni radiologiche e con gli strumenti radiologici (dette "modalità diagnostiche") come gli strumenti per le radiografie (RX), le TC[18] (ancora adesso chiamate comunemente TAC[19] anche se si sono evolute in, appunto, TC, in quanto le immagini

[17] Picture Archiving and Communication System

[18] Tomografia Computerizzata

[19] Tomografia Assiale Computerizzata

prodotte non sono più solo "assiali" ma permettono una ricostruzione tridimensionale), le RM[20], gli ecografi, le PET[21], i macchinari per le scintigrafie, e si occupa poi di gestire la refertazione degli esiti/immagini prodotte dalle modalità e di renderne infine disponibili le consuntivazioni (cioè la comunicazione all'order placer dello stato delle prestazioni richieste, che passerà quindi dallo stato "ordinato" allo stato "eseguito" e poi "refertato" o definizioni simili).

Il RIS, insieme al LIS quando operano all'interno di un ospedale dotato di pronto soccorso, deve occuparsi anche dell'attività emergenziale e non solo elettiva[22] e per questo è necessario che anch'esso abbia le funzionalità per trattare i dati, come order filler, con le opportune e necessarie informazioni di oscuramento ex-lege (v. par. 2.1) nel caso in cui questo si renda necessario.

Il PACS è un software dedicato alla trasmissione, visualizzazione ed archiviazione delle immagini digitali prodotte dalle modalità diagnostiche e dalle stazioni di refertazione. Come facilmente intuibile deve avere una grande capacità di archiviazione, visto il "peso" sempre crescente delle immagini con l'avanzare della tecnologia che permette un dettaglio sempre crescente, e deve rendere disponibile queste immagini in tempo quasi-reale anche per lungo tempo (si immagini ad esempio l'esigenza, molto comune e frequente, di un medico di poter confrontare un esame appena fatto con le immagini dello stesso esame fatto magari alcuni anni prima per vedere se un certo problema ha avuto un'evoluzione). Non si può quindi pensare di archiviare su sistemi "lenti" (come i nastri) immagini che devono essere rese disponibili in qualunque momento. Fanno parte del PACS anche le stazioni di refertazione, i robot che stampano/masterizzano i CD/DVD contenenti le immagini

4.5 Anatomia Patologica

Un altro software fondamentale in un'azienda sanitaria è quello che si occupa dell'ambito della Anatomia Patologica, che corrisponde a quella branca della medicina che studia gli organi a livello macroscopico e i tessuti e le cellule a livello microscopico. All'interno di un contesto clinico l'anatomia patologica svolge un ruolo fondamentale nell'individuazione delle malattie che colpiscono le cellule (o gli organi) per poter pianificare le terapie mediche o chirurgiche. Similmente a quanto avviene con un LIS anche il software di anatomia patologica prevede la ricezione della richiesta di esame, il campione, la sua analisi e la produzione del relativo referto corredato, eventualmente, da immagini (in questo quindi è affine anche al RIS).

[20] Risonanza Magnetica

[21] Tomografia a Emissione di Positroni

[22] Con il termine attività "elettiva" (o "di elezione") in ambito clinico si intendono le attività pianificate, mentre le attività urgenti o emergenziali, per loro natura, non sono ovviamente pianificabili

4.6 Centro Trasfusionale

Ancora, tra i software che gestiscono da estremamente sensibili e delicati c'è l'applicativo della gestione del Centro Trasfusionale. Esso si occupa di erogare prestazioni che si dividono in attività di medicina trasfusionale (comprese le donazioni sanguigne), attività di laboratorio (al pari del LIS può avere strumenti dedicati a specifiche analisi ematiche direttamente integrati) ed attività consulenza per i pazienti che devono essere o sono stati trasfusi.

La conseguente gestione della banca dati ematica che l'applicativo deve fare, spesso contiene anche dati genetici che sono particolarmente tutelati dalla legge sulla privacy, e vanno di conseguenza protetti con tutte le migliori tecnologie a disposizione.

Immaginiamo, inoltre, la gravità di un'accidentale corruzione dei dati o anche solo un accidentale errore di tracciamento ed identificazione dei campioni ematici o delle sacche di sangue.

4.7 Sistema Informativo Territoriale

Il SIRTE[23] è l'applicativo che ha permesso la digitalizzazione dei servizi di Cure Domiciliari e Cure Domiciliari Palliative, dei Consultori, delle strutture residenziali ad alta intensità assistenziale (denominate R2) direttamente gestite dall'AUSL, dei Centri Alzheimer e dell'Hospice, migliorando notevolmente la gestione e l'efficacia dei servizi sanitari in queste aree. Le potenzialità di questo applicativo sono molteplici ed in continua evoluzione e si estenderà anche verso la Continuità Assistenziale, gli Ospedali di Comunità, il Ser.D[24] e il DSM[25].

Vista la moltitudine di attori potenzialmente coinvolti nella gestione dei pazienti sul territorio questo software nasce allo scopo di agevolarne la collaborazione, integrandosi anch'esso con gli altri sistemi informativi aziendali e, in particolare, attraverso l'order entry del sistema SIO è possibile comunicare con il LIS e il RIS, così da agevolare la richiesta di prestazioni e la consultazione dei dati diagnostici, migliorando il processo di cura e di presa in carico del paziente.

Questo applicativo si deve poi integrare con il sistema di televisita, teleconsulto e telemonitoraggio per agevolare la gestione a distanza del cittadino. Il SIRTE consente di velocizzare l'erogazione dei servizi e contribuisce a eliminare o ridurre l'uso della documentazione cartacea che, sul territorio, è più difficile da eliminare. Infatti, sono state digitalizzate le Schede Valutative e i Referti in ambito territoriale mettendo a disposizione

[23] Sistema Informativo Territoriale

[24] Servizio per le Dipendenze

[25] Dipartimento di Salute Mentale

del **Repository aziendale** e della **Conservazione a norma** i documenti elettronici firmati digitalmente. In ambito progettuale è previsto anche che il cittadino possa ricevere sul suo FSE quanto prodotto dai servizi territoriali.

4.8 Altri software (Screening, SSO, BI, . . .)

All'interno di un'azienda ospedaliera, come già detto, esistono molti altri software "verticali", oltre a quelli esposti sopra, che possiamo considerare, come ambito di attività, mole di attività, e criticità rispetto alle loro funzioni, "minori". Non per questo essi sono meno importanti o un'azienda può pensare di farne a meno. Solo che, operando in un contesto più "ristretto" e, soprattutto, che non comprende ambiti "emergenziali", un eventuale loro disservizio è meno impattante, ed anche i dati che essi possono contenere hanno caratteristiche che li rendono meno "sensibili".

Tra i più importanti possiamo annoverare:

- **Screening**: le campagne di prevenzione che una AUSL può condurre sul territorio necessitano di una gestione specifica per la finalità a cui queste sono dedicate.

  Ci possono essere campagne dedicate a specifiche categorie della popolazione, a seconda dell'età o del sesso, e servono quindi specifici applicativi in grado di integrarsi con l'anagrafica aziendale, ma anche con i laboratori analisi o i servizi radiologici gestendone le campagne di reclutamento e di eventuale richiamo in caso di positività.

- **SSO**: vista la proliferazione di software in uso in un'Azienda sanitaria, ed a cui gli operatori devono costantemente autenticarsi, molto utili sono gli applicativi che permettono di gestire le credenziali di autenticazione in maniera centralizzata ed univoca, detti cioè di SSO[26], permettendo così agli operatori di doversi ricordare una sola combinazione utente/password per tutti gli applicativi aziendali. Anche il cambio password, che per policy di sicurezza deve avvenire ogni 3 o 6 mesi è così centralizzato. Negli anni il protocollo che più si è affermato è LDAP[27], ed ormai la stragrande maggioranza degli applicativi è compatibile con esso. Una volta che l'utente si è autenticato nell'applicativo, sarà cura dell'applicativo stesso assegnargli poi le dovute autorizzazioni in base al suo profilo.

  Ad un livello più grande, la pubblica amministrazione ha messo a disposizione dei cittadini il sistema SPID[28] e, più recentemente, l'autenticazione tramite CIE[29],

[26] Single Sign On

[27] Lightweight Directory Access Protocol

[28] Sistema Pubblico di Identità Digitale

[29] Carta d'Identità Elettronica

entrambi con lo scopo di supportare i cittadini fornendo un unico modo di accesso e login a tutti i servizi della pubblica amministrazione (FSE, ANPR, . . .).

- **BI**: i programmi di BI[30] si stanno diffondendo sempre più nelle aziende sanitarie perché consentono di supportare il processo decisionale, sia quello gestionale che quello direzionale, in ambito amministrativo ma anche clinico. Grazie al suo supporto si possono automatizzare i processi di misurazione, controllo, analisi dei risultati, e delle performance attraverso sistemi di reporting e vari tipi di visualizzazioni, compresi allarmi su valori fuori norma.

[30] Business Intelligence

Capitolo 5

Le integrazioni tra i sistemi sanitari

Tutti gli applicativi descritti fino qui e che vanno a comporre un ambiente informativo sanitario, gestiscono dati, li elaborano e li archiviano, ma mentre fino a qualche anno fa questi operavano come delle scatole (o isole) chiuse (parliamo dei sistemi informativi degli anni ’90), senza preoccuparsi di dover inviare (o ricevere) dati da altri applicativi.

L’evoluzione delle tecnologie ha permesso un salto di qualità, con evidenti vantaggi (ma anche con qualche svantaggio), facendo sì che ora nessun applicativo verrebbe mai acquistato ed utilizzato da un’azienda sanitaria senza che esso abbia la capacità di "integrarsi" (è questo il termine con cui si indica il fatto che applicativi diversi "dialoghino" tra loro) con gli altri software già presenti ed attivi. Esistono infatti specifiche normative del Ministero della Salute che impongono lo sviluppo della metodologia HTA[1].

Le "integrazioni" hanno sempre un grado di complessità piuttosto alto, sia nel loro sviluppo che nella loro gestione e manutenzione, dovuto al fatto che ogni software comunque è generalmente "proprietario" e sono tra di loro eterogenei, ma lo scambio dei dati deve avvenire in modalità che sia il più possibile standard e si ottiene grazie a linguaggi, protocolli, regole e formati standard che stabiliscono:

- le modalità di trasmissione e ricezione dei dati
- la rappresentazione e le regole di scrittura dei dati (sintassi)
- il significato dei termini (semantica)

A tal fine esistono infatti numerosi **linguaggi per l’integrazione** dei dati, alcuni di questi creati esplicitamente per l’utilizzo con i dati sanitari come l’HL7[2], nelle sue varie

[1] Health Tecnology Assessment

[2] Health Level 7

versioni, fino al FHIR[3], il DICOM[4] per lo scambio di immagini sanitarie e molti altri. Lo scopo naturale di questi standard è quello di facilitare i vari produttori di software nel poter permettere la condivisione delle informazioni attraverso un linguaggio comune, facilitando ma, soprattutto, rendendo più sicura la trasmissione senza errori di questi che, abbiamo capito, sono dati molto "delicati".

5.1 Le comunicazioni all'interno della rete ASL

I software che fanno parte di un SIS, abbiamo visto in precedenza, sono molteplici, molto diversi tra loro in quanto, benché si tratti sempre di ambito sanitario, hanno scopi e ruoli diversi, alcuni trasversali a tutta l'azienda o a buona parte di essa, altri "verticali" con funzionalità specifiche per un singolo servizio. Tutti però devono scambiare informazioni tra di loro, nonostante siano probabilmente stati sviluppati ed installati anche in momenti temporalmente piuttosto distanti tra loro. Solitamente ormai la stragrande maggioranza degli applicativi (ma non tutti!) usano una tecnologia web-based per offrire agli operatori la propria interfaccia attraverso l'accesso tramite un semplice browser, senza necessità di installare uno specifico software su ogni client dell'azienda. Tra gli innumerevoli vantaggi di questa scelta c'è il fatto che si può usare la cifratura https nello scambio di dati con il server. Ovviamente il prerequisito, scontato ormai, è che tutti i pc/client di un'azienda siano in rete tra di loro e le comunicazioni tra client e server siano "gestite" attraverso un'opportuna regolamentazione e filtrazione fatta attraverso i firewall affinché non si possa accedere ai dati dei server da reti non inserite tra quelle autorizzate. Solitamente poi i server su cui sono installati questi software non sono accessibili dall'esterno, e, nel caso in cui questo si renda necessario, come vedremo nei prossimi paragrafi, si dovranno utilizzare delle specifiche tecnologie allo scopo di proteggere il più possibile queste comunicazioni.

5.1.1 IHE

IHE[5] è un'iniziativa che non ha scopo di lucro ed è nata per promuovere l'integrazione tra i sistemi informativi sanitari, ed è stata fondata dalla HIMSS[6] e dalla RSNA[7] nel 1998.

Come si vedrà nei prossimi paragrafi, gli standard di integrazione ad oggi in uso sono numerosi ma, nonostante ciò, i molteplici ed eterogenei sistemi informatici clinici spesso non riescono a scambiarsi dati tra di loro in maniera efficiente a causa delle diverse

[3]Fast Healthcare Interoperability Resources

[4]Digital Imaging and COmmunications in Medicine

[5]Integrating the Healthcare Enterprise

[6]Healthcare Information and Management Systems Society

[7]Radiological Society of Notrh America

interpretazioni nell'uso degli standard, la notevole complessità dei sistemi stessi, e anche per la troppo ampia scelta di opzioni che gli standard consentono. IHE analizza questi standard già in uso, senza proporne di nuovi, ma allo scopo di definire in maniera chiara come utilizzarli nel modo migliore e più efficace, in particolare per gli standard HL7, DICOM e LOINC, emettendo delle *linee guide* dette **profili di integrazione** (o *Technical Framework*).

Anche in Italia abbiamo il gruppo "IHE Italia" [35] che raccoglie gli attori che vogliono contribuire a questa iniziativa la quale, grazie alla qualità ed all'utilità del lavoro svolto, è diventata un framework per i problemi di integrazione, per i formati dati, per le integrazioni di strumenti medicali.

I profili di integrazione che IHE emette, vengono revisionati ed aggiornati annualmente e sono fatti con filosofia *open source* e perciò liberamente scaricabili da internet. Quelli di maggiore interesse sono:

- XDS[8] che descrive le linee guida per lo scambio di documenti clinici tra studi medici, reparti, aziende sanitarie pubbliche o istituti di cura privati. Ogni organizzazione deve appartenere (o "adottare") uno o più **Affinity Domain**[9]
- XCA[10] interroga e recupera le cartelle cliniche elettroniche dei pazienti conservate da attori ad un livello superiore a quello ospedaliero. Viene definito il concetto quindi di *Community* come un insieme di strutture sanitarie che adottano delle policies e dei protocolli comuni per l'interscambio della documentazione clinica
- PIR[11] coordina la riconciliazione della cartella clinica del paziente quando vengono acquisite immagini di pazienti non identificati (ad esempio, traumi) o identificati erroneamente.

5.1.2 HL7

HL7 International è un'organizzazione senza scopo di lucro, accreditata ANSI[12], che si occupa di sviluppare formati standard che possano fornire un quadro completo per lo scambio, l'integrazione, la condivisione e il recupero di informazioni sanitarie elettroniche a supporto della pratica clinica e della gestione, erogazione e valutazione dei servizi sanitari [33]. A questa associazione fanno capo oltre cinquanta gruppi di lavoro provenienti da tutto il mondo ed i cui membri rappresentano operatori sanitari, enti governativi,

[8] Cross enterprise Document Sharing

[9] L'Affinity Domain è un insieme di regole per garantire interoperabilità dei dati tra aziende sanitarie atte a definire come tutti gli attori di un dominio XDS debbano popolare e scambiarsi messaggi. Lo stesso FSE italiano adotta un Affinity Domain "nazionale" [36]

[10] Cross-Community Access

[11] Patient Information Reconciliation

[12] American National Standards Institute

specialisti informatici del mondo clinico, aziende farmaceutiche e sanitarie, società di consulenza e fornitori di sistemi medicali.

In Italia è stato creato il gruppo HL7 Italia, formato nel 2003 come parte di HL7 International ed è responsabile della localizzazione dello standard nella realtà italiana e, più in generale, ha l'obiettivo di stimolare e convogliare i contributi regionali e nazionali allo sviluppo dello standard e favorire la modernizzazione del IT sanitario italiano [34].

Il linguaggio sviluppato dall'associazione porta lo stesso nome e si è affermato ormai come uno standard adottato a livello internazionale per l'integrazione tra i software e apparati sanitari per i messaggi elettronici relativi ai dati sanitari permettendo ai diversi apparati software e hardware di condividere diverse tipologie di dati. Il numero 7 nel nome sta ad indicare che esso è stato scritto per lavorare al livello 7 del modello ISO/OSI[13].

Il linguaggio HL7 prevede perciò diverse tipologie di messaggi, legate ai diversi "eventi", come l'accettazione di un episodio, la richiesta di un esame di laboratorio o di una visita, l'emissione di un referto o la comunicazione di avvenuta esecuzione di una prestazione (e quindi di calcolo della tariffa), l'inserimento di una nuova anagrafica, ecc. . .

Attualmente sono in uso due principali versioni dello standard HL7, la v2, basata su messaggi di testo in formato ASCII[14], e la v3, basata su oggetti XML[15].

La v2, nonostante possa considerarsi "obsoleta" come tecnologia, resta tuttora la più diffusa per via della sua adozione da più tempo che ne ha permesso un'ampia diffusione, e per via della difficoltà e dei costi che gli aggiornamenti portano in ambito sanitario e per cui, alla fine, si tende a mantenere una tecnologia che benché "vecchia" è ben conosciuta dai tecnici, ben supportata dalle aziende e, in fondo, funzionale allo scopo per cui è stata creata.

Vediamole un pochino più nel dettaglio con degli esempi.

HL7 versione 2

Come già scritto lo standard HL7 v2 utilizza per le comunicazioni messaggi scritti in formato ASCII che vengono creati e trasmessi a seguito di un evento.

Il più diffuso delle v2, attualmente, è quello in particolare in versione 2.5, emesso ormai nel lontano 2003 ma ancora particolarmente usato[16].

---

[13] Il livello 7 della pila, denominato "Applicazione", è quello più vicino all'uomo

[14] American Standard Code for Information Interchange

[15] eXtensible Markup Language

[16] Infatti è quello attualmente utilizzato ancora nella maggior parte delle integrazioni all'interno dell'USL della Valle d'Aosta

Ogni messaggio è composto da diversi segmenti, non tutti obbligatori e non tutti sempre presenti (ce ne sono circa 150). Il segmento di testa, questo sì obbligatorio, si chiama MSH[17] ed identifica il tipo di messaggio e, quindi, l'evento che lo ha scatenato. Altri segmenti molto comuni sono:

- PID[18] che include le informazioni anagrafiche principali del paziente e, soprattutto, i suoi identificativi univoci (v. par. 4.2)
- ADT usato, come dice l'acronimo, per accettazioni, dimissioni e trasferimenti, ma anche per le gestioni "anagrafiche" di inserimento, modifica, riconduzione (merge) di record anagrafici
- PV1[19] include informazioni quali ad esempio il medico che ha richiesto una visita, o il posto letto assegnato
- OBR[20] include le informazioni relative a visite o esami

Ogni segmento è fatto di più campi, separati dal carattere **|** ("pipe") e possono a loro volta essere divisi in sottocampi separati dal carattere **&**, **^** o **~**.

Molto importante è il fatto che questo linguaggio ha una **semantica posizionale**, cioè il significato dei campi dipende dalla posizione in cui si trovano all'interno del segmento.

Il vantaggio di questo linguaggio è quello di essere piuttosto leggibile da parte dell'uomo. Bisogna però definirne bene la sintassi in quanto, pur definendo questo linguaggio "standard", la lunghezza variabile dei campi, la mancanza di un significato univoco di questi, la mancanza di una definizione precisa del modello di dati, fa sì che in realtà il linguaggio HL7 v2 sia "poco standard" e deve sempre essere accompagnato da tabelle dove vengono definiti con precisione i messaggi in uso ed il loro contenuto. Questo va fatto per ogni integrazione che essendo solitamente punto-punto (per esempio tra HIS e LIS o tra HIS e RIS) o punto-multipunto (per esempio tra MPI e HIS, LIS, RIS, . . .) va comunque concordata di volta in volta tra almeno 2 attori.

A tal proposito HL7 v2 permette anche la creazione di segmenti "personalizzati", definiti **Z-segment**, che si possono creare quando nessuno dei segmenti standard risponde alle esigenze di contenuto necessarie. Anche se dovrebbero essere usati con "parsimonia" sono uno dei motivi che hanno decretato il successo e la longevità di questo linguaggio.

Un altro dei maggiori pregi riguardo questo standard è la sicurezza delle comunicazioni. Sicurezza che è dovuta al ciclo che i messaggi devono rispettare e prevede che

[17] Message Header Segment

[18] Patient IDentifier

[19] Patient Visit Information

[20] Observation Request

ogni messaggio dalla sorgente al destinatario, per considerarlo inviato con successo, deve ricevere in senso inverso un messaggio di ACK positivo (con all'interno la sigla AA, Application Accept) che ne indica la corretta ricezione. Viceversa, in caso di errori, il destinatario invia un messaggio di NACK a cui, la sorgente, potrà rispondere con un reinvio o altre azioni concordate tra gli attori. Oppure un ACK con AE (Application Error) ad indicare che benché il messaggio sia stato formalmente ricevuto correttamente, il destinatario non ne ha comunque accettato il contenuto e, solitamente, sempre in questo messaggio di risposta, viene riportato un codice o un testo che dovrebbe descrivere cosa non andava bene nel contenuto del messaggio.

Vediamo alcuni esempi, presi dall'ambiente reale in uso presso la ASL della Valle d'Aosta ma, naturalmente, opportunamente "anonimizzati" dei dati che riconducono ai pazienti.

Nell'ambito della gestione dei record anagrafici i 3 messaggi principali che vengono utilizzati sono:

- A28: per l'inserimento di un nuovo record anagrafico (esempio in tab. 5.1)
- A31: per l'aggiornamento di un record anagrafico già presente
- A40: per il "merge" (unione) di 2 record anagrafici già presenti, di uno, quello che deve rimanere valido, sarà indicato nel messaggio in appositi campi e viene detto "master" e l'altro, indicato in altri campi ooportuni, "slave" (esempio in tab. 5.2)

Request
MSH|^~_&|MPI|.|TRAK|.|20111221163629|.|ADT^A28^ADT_A05| uB111221153629410458|P|2.5
EVN|A05|20111221163629|.|.|.|20111221163629
PID|.|.|204587^^^^MPI~^^^^TRAK~PZNPRV22B02E379N^^^^CF~^^^^SSN ~123456789 ^^^^TEAM^^^20120131 |.|PAZIENTEMPI^PROVA009|.|19220202 |M|.|.|^^IVREA^^^^N^^001125~via Roma ^^AOSTA^100^11100^^L^^007003 ~^^^^^^C|.|0161887766|333 8877990^^^paziente@prova.com|.|1|.|.|.|.|.|.|.|.| 100^ITALIA
PD1|.|.|.|.|.|.|.|.|.|.|.|.|Y|20090914
CON|1|092^Consenso al DSE^DSE|.|.|Potesta' genitoriale|CognomeMadre NomeMadre|.|Y|V|Y|.|.|20170405

Tabella 5.1. Esempio di messaggio HL7 v 2.5 di tipo ADT^A28

L'esempio riportato in tab. 5.1 (si tratta di un unico messaggio dove ogni riga è un segmento del messaggio stesso) rappresenta un messaggio di tipo "A28" che viene inviato (request) dal master per le anagrafiche MPI (indicato nel segmento MSH posizione 3)

verso l'applicativo TrakCare (MSH pos. 5) atto ad "ordinargli" di inserire una nuova anagrafica nel suo database. I dati di questa anagrafica sono riportati nel segmento EVN ed in ogni posizione è presente una certa informazione.

Molto simile (per non dire identico) è il messaggio di tipo "A31" per l'aggiornamento di un record anagrafico già presente. In questo caso il ricevente, una volta verificata l'effettiva presenza nel suo database di quel record identificato dai principali "id", deve provvedere ad aggiornarne i dati con quanto presente nel messaggio.

Diverso e molto più delicato è il discorso per il cosiddetto "merge" di 2 record anagrafici. Esso si rende necessario quando vengono individuate 2 anagrafiche che corrispondono in realtà alla stessa persona (v. pag. 56). L'applicativo master per le anagrafiche ha di solito un'interfaccia per effettuare questa operazione in modo "visivo" così da mettere a confronto i dati principali dei 2 record e far sì che l'operatore abbia ben chiaro quale mantenere attiva (master) e quali disattivare (slave). L'anagrafica che viene disattivata (non si cancella mai un record, ma esso viene "solo" disattivato) potrebbe anch'essa contenere dei dati clinici (è un caso assolutamente frequente) ed essi non devono andare persi, ma devono essere spostati verso l'anagrafica master (o meglio, vengono fatti "ripuntare" verso l'anagrafica master). L'operazione che ogni applicativo deve compiere sul proprio database anagrafico è la medesima, ma invece che dover essere fatta manualmente da un operatore viene eseguita internamente alla ricezione del comando corrispondente al messaggio "A40" (v. tab. 5.2). Nella fig. 5.1 si può vedere un esempio di interfaccia di "merge" a disposizione dell'operatore (tratta dall'applicativo MPI in uso presso l'ASL della Valle d'Aosta) ed il relativo interscambio con il messaggio "A40" di "request" che viene scaturito ed inviato agli applicativi integrati i quali risponderanno con un messaggio "response". L'interfaccia deve proporre chiaramente quale anagrafica è quella che verrà mantenuta (lato sinistro) e quale verrà "disattivata" (lato destro), affinché l'operatore che compie tale atto abbia ben visibili i dati essenziali di una e dell'altra anagrafica così da ridurre al minimo l'errore umano che sempre ci può essere.

Si noti nel messaggio A40 (tab. 5.2) il segmento denominato MGR, che contiene l'indicazione dell'identificativo (ID_MPI) dell'anagrafica "slave" che dovrà essere disattivata ed i cui eventuali dati clinici andranno fatti "migrare" sull'anagrafica "master".

Nella response, invece, è importante notare il parametro "AA" oltre al "ACK", dove "AA" sta per "Application Accept", ad indicare che, oltre alla ricezione positiva "ACK" del messaggio, anche a livello applicativo il comando è stato eseguito correttamente.

Vediamo ancora invece un messaggio di "ordine" (o "richiesta") di prestazione (tab. 5.3). Nell'esempio vogliamo mostrare una richiesta di radiografie, le quali possono essere raggruppate in un unico messaggio composto dai vari segmenti in cui, ognuno, è una singola radiografia che verranno però eseguite in un unico momento. In questo caso, ogni prestazione richiesta è formata da una "tripletta" di 3 segmenti, ORC, OBR e FT1 in cui vengono inserite tutte le informazioni utili all'esecutore (sia il sw applicativo esecutore che la persona fisica, operatore amministrativo, tecnico, medico, esecutore) per organizzare ed eseguire al meglio la/le prestazioni richieste.

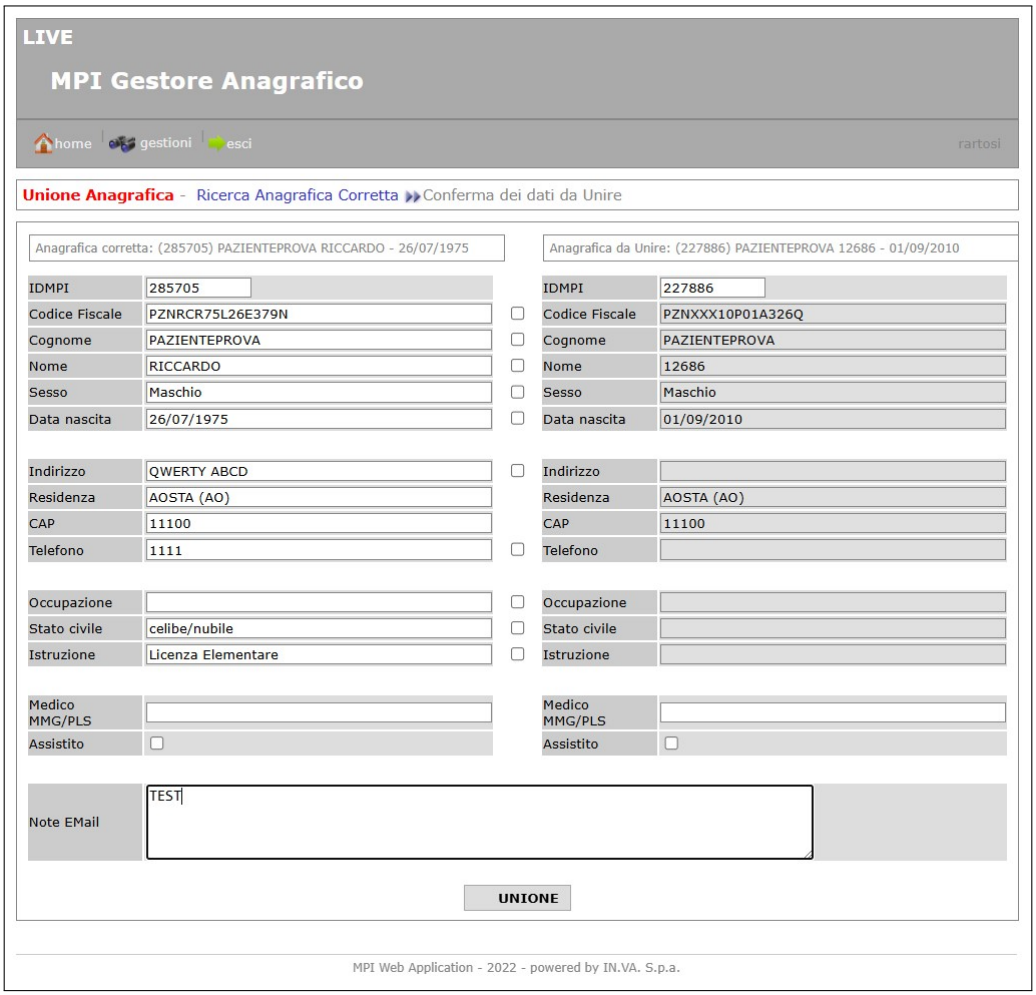

Figura 5.1. Maschera per effettuare merge anagrafici

HL7 versione 3

Nato come evoluzione del HL7 v2 utilizza un framework "Object Oriented" ed un modello di riferimento che pone regole precise e ben più stringenti di quelle adottate nella v2.

Come nel v2 anche nel nel v3 i messaggi sono testuali e cominciano con un Header, ma sono scritti in XML, che risulta facilmente intellegibile ed è uno standard semplice e, soprattutto, aperto. Qui la semantica non è posizionale come nel v2 ma basata sui TAG dell'XML che si esprimono in una struttura nidificata.

Vediamo in tab. 5.4 un esempio di messaggio HL7 v3.

Lo standard HL7 v3 è più "ricco" del v2, gestendo un maggior numero di eventi ed una maggiore varietà di costruttori. In altre parole, il principale vantaggio di HL7 v3 rispetto a HL7 v2 risiede nella sua flessibilità semantica e nell'approccio modellato, progettato

Request
MSH|^~_&|MPI|MPI|TRAK|TRAK|20250126172728|.|ADT^A40^ADT_A05| uB111221153629410458|P|2.5
EVN|A40|20250126172728|.|.|.|20250126172728
PID|.|.|285705^^^^MPI~307573^^^^TRAK~PZNRCR75L26E379N^^^^CF ~02V01424136^^^^SSN~12121212^^^^TEAM^^^20221231|.|PAZIENTEPROVA ^RICCARDO|.|19750726|M|.|.|^^IVREA^^^^N^^001125~QWERTY ABCD ^^AOSTA^^11100^^L^^007003~~^^^^^C|.|1111|.|.|1|1^Licenza Elementare| 12121212^3^^IT^^500001^^20221231|.|.|.|.|.|.|100^ITALIA|.|.|.|N|.|N~N~N
PD1|.|.|^^^^^^ASLASS
MRG|227886^^^^MPI
Response
MSH|^~_&|TRAK|TRAK|MPI|MPI|202501261726|.|ACK^A40 |UR250126162728438245|P|2.5
MSA|AA|UR250126162728438245|

Tabella 5.2. Esempio di messaggio HL7 v2.5 di tipo ADT^A40 e relativa risposta

per superare le limitazioni dei campi fissi e della struttura rigida di HL7 v2. HL7 v3 si basa sul RIM[21], che è un modello concettuale progettato per rappresentare in modo uniforme qualsiasi aspetto delle informazioni sanitarie.

Nonostante i numerosi vantaggi che, sulla carta, HL7 v3 ha rispetto a HL7 v2 il suo utilizzo è rimasto limitato per diversi motivi:

- Complessità eccessiva: HL7 v3 richiede una profonda comprensione del RIM, un modello complesso e astratto che ha reso difficile l'implementazione e l'adozione. I messaggi XML generati sono lunghi, difficili da leggere e gestire rispetto a HL7 v2.

- Costo di implementazione: La transizione da HL7 v2 a HL7 v3 è stata onerosa in termini di costi e tempo. Molte organizzazioni hanno preferito continuare con HL7 v2, già consolidato.

- Interoperabilità limitata: Nonostante l'obiettivo di standardizzare lo scambio di dati, HL7 v3 spesso richiedeva personalizzazioni specifiche per ogni implementazione, compromettendo l'interoperabilità.

[21] Reference Information Model

<table>
<tr><td>Request</td></tr>
<tr><td>MSH|^~_&|TRAKCARE|TRAKCARE|ELEFANTE|AGFA|20250201103653|.|ORM^O01 |Dh250201093653154630|P|2.5|574148</td></tr>
<tr><td>PID|.|.|123123^^^^TRAK~321321^^^^MPI~ABCDEF00S11D537K^^^^CF~ 80380000000000000000^^^^TEAM^^^20271123|.|PAZIENTEPROVA^TEST||20001124| M|.|.|^^FENIS^^^^N^^007027~LOC. NAVE 99^^FENIS^AO^11020^^L^^007027~ LOC. NAVE 99^^FENIS^AO^1212^^H^^007027~^^^^^^C|.|333 123123|.|.|2| 1^Licenza Elementare|.|.|.|.|.|.|.|.|100^Italia|.|.|.|N|.|Y~Y|.|.|.|.|Y</td></tr>
<tr><td>PD1|.|.|.|.|.|.|.|.|.|.|.|.|N</td></tr>
<tr><td>PV1|1|O|6902^^^^^^^^Radiologia V.LE GINEVRA|.|14582672|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|. |.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|P|.|.|20250201103600</td></tr>
<tr><td>ORC|NW|570117|.|RAD01499770|.|.|1^^^20250201103600^^NORM|.|202502011036| ^Operatore1^INF7^Amministrativo|.|.|6902^^^^^^^^Radiologia V.LE GINEVRA|.|.|.| 6902^Radiologia V.LE GINEVRA|.|.|.|.|.|.|.|.|.|.|.|N^Normal^ConfidentialityCode</td></tr>
<tr><td>OBR|1|570117||69324^MANO (SIN)^6905|.|20250201|20250201103600|.|.|.|.|.|ESENTE |.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|6902^Radiologia V.LE GINEVRA|.|.|QUE^TRAUMA DELLA MANO, ESCLUSE LE DITA - SX</td></tr>
<tr><td>FT1|1|.|.|20250130|.|D|.|U|.|.|.|.|.|E01^Esente per eta e reddito|.|.|.|SSN|^^^^TRAUMA DELLA MANO, ESCLUSE LE DITA - SX |.|28004W|.|.|.|.|.|.|.|.|0200A4020012345</td></tr>
<tr><td>ORC|NW|570118|.|RAD01499770|.|.|1^^^20250201103600^^NORM|.|202502011036| ^Operatore1^INF7^Amministrativo|.|.|6902^^^^^^^^Radiologia V.LE GINEVRA|.|.|.| 6902^Radiologia V.LE GINEVRA|.|.|.|.|.|.|.|.|.|.|.|N^Normal^ConfidentialityCode</td></tr>
<tr><td>OBR|2|570118||69323^POLSO (SIN)^6905|.|20250201|20250201103600|.|.|.|.|.|ESENTE |.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|.|6902^Radiologia V.LE GINEVRA|.|.|QUE^TRAUMA DELLA MANO, ESCLUSE LE DITA - SX</td></tr>
<tr><td>FT1|2|.|.|20250130|.|D||U|.|.|.|.|.|E01^Esente per eta e reddito|.|.|.|SSN|^^^^TRAUMA DELLA MANO, ESCLUSE LE DITA - SX |.|28004W|.|.|.|.|.|.|.|.|0200A4020012345</td></tr>
<tr><td>Response</td></tr>
<tr><td>MSH|^~_&|ELEFANTE|AGFA|TRAKCARE|TRAKCARE|20250201103700||ACK^O01 ^ORR_O02|c5f7c2416b599dd|P|2.5.1|.|.|.|.|.|8859/1</td></tr>
<tr><td>MSA|AA|Dh250201093653154630|Insert/Update Request: RAD01499770 OK</td></tr>
</table>

Tabella 5.3. Esempio di messaggio HL7 v2.5 di tipo ORM^O01 e relativa risposta

- Accettazione globale scarsa: HL7 v3 non è mai stato universalmente accettato come HL7 v2. Molti paesi e organizzazioni hanno mantenuto HL7 v2 o sono passati direttamente a FHIR.

```
<MSH>
<MSH.2>Azienda USL VdA</MSH.2>
<MSH.3>Accettazione</MSH.3>
<MSH.4>2020-06-10</MSH.3>
<MSH.9>
<C.1>ADT</C.1>
<C.2>A01</C.2>
</MSH.9>
</MSH>
```

Tabella 5.4. Esempio di messaggio HL7 v3 di tipo ADT^A01

HL7 FHIR

Come detto nel paragrafo precedente l'HL7 v3 non ha avuto la diffusione che ci si aspettava quando è stato creato perché gli sviluppatori e le aziende hanno preferito continuare ad utilizzare HL7 v2 perché le sue caratteristiche ne garantivano semplicità, velocità e grande flessibilità. Non vi era alcun vantaggio concreto che rendesse conveniente modificare gli applicativi in uso per andare a sostituire l'HL7 v2 con l'HL7 v3, più rigida e con un modello di riferimento complesso come il RIM. E così, anche per le integrazioni ex-novo si è continuato ad usare l'HL7 v2 (le integrazioni tuttora attive nell'ecosistema dell'AUSL della Valle d'Aosta ne sono un esempio).

Vista la lezione maturata sul campo grazie ai successi e agli insuccessi dei precedenti standard l'associazione HL7 ha deciso di realizzare un linguaggio per standardizzare lo scambio dei dati sanitari di tutti i pazienti che entrano negli ecosistemi sanitari digitali EPR o nei FSE, ed è nato così lo standard HL7 FHIR (che si legge "fire" ed ha il simbolo di una fiamma come visibile in fig. 5.2), ora giunto già alla versione 5 delle specifiche (al momento in cui si scrive questa monografia la versione 6 è in "draft"), e che si prefigge di essere più facile da implementare, più aperto e più estensibile rispetto alle versioni HL7 v2 o v3. Esso sfrutta una moderna suite di tecnologia API[22] basata sul Web, tra cui un protocollo RESTful [38] basato su HTTP[23], HTML[24] e CSS[25] per l'integrazione dell'interfaccia utente, una scelta di JSON[26] o XML per la rappresentazione dei dati, OAuth [39] per l'autorizzazione e ATOM per i risultati delle query. Lo scopo

[22] Application Programming Interface

[23] Hypertext Transfer Protocol

[24] HyperText Markup Language

[25] Cascading Style Sheets

[26] JavaScript Object Notation

principale dello standard FHIR è garantire l'interoperabilità tra diversi sistemi informatici. Definisce il formato dei dati e il protocollo per lo scambio di informazioni mediche, indipendentemente da come vengono archiviate in questi sistemi.

Figura 5.2. Logo dello standard HL7 FHIR

L'elemento base che va a comporre un messaggio di tipo FHIR si chiama "Resource", tutti i dati scambiabili sono quindi "risorse", sono descritte in XML o JSON ed hanno queste caratteristiche:

- sono rappresentate in modo univoco e condiviso
- sono costruite attraverso dei data type condivisi
- possiedono dei metadati condivisi
- come per l'HL7 sono abbastanza leggibili dall'essere umano

Nella tipologia di comunicazioni dello standard HL7 v2 o v3 ogni sistema invia le informazioni in suo possesso agli altri sistemi che potrebbero averne bisogno seguendo una logica di tipo "push". I riceventi, poi, memorizzano il contenuto dei messaggi affinché possano successivamente utilizzarne i dati o aggiornarli. In questo modo, si assiste alla generazione e allo scambio di un'elevata quantità di messaggi, che rischiano di far diventare la rete sottostante un vero e proprio collo di bottiglia. La logica FHIR è invece all'opposto: il sistema struttura sintatticamente e semanticamente le informazioni attraverso le suddette entità denominate "risorse" e, quando un sistema ha bisogno di un'informazione fa una richiesta direttamente ai sistemi che la possiedono. Le informazioni sono accessibili e disponibili a chi le richiede o ne ha bisogno attraverso API, la logica, in questo caso, è di tipo "pull" [40] verso un server che, accessibile mediante una URL[27], permette operazioni di lettura e scrittura mediante dei **metodi standard**:

- **Create** = POST `https://example.com/path/{resourceType}`

[27] Uniform Resource Locator

- **Read** = GET `https://example.com/path/{resourceType}/{id}`
- **Update** = PUT `https://example.com/path/{resourceType}/{id}`
- **Delete** = DELETE `https://example.com/path/{resourceType}/{id}`
- **Search** = GET `https://example.com/path/{resourceType}?search_parameters...`
- **History** = GET `https://example.com/path/{resourceType}/{id}_history`
- **Transaction** = POST `https://example.com/path/` (POST a transaction bundle to the system)
- **Operation** = GET `https://example.com/path/{resourceType}/{id}/${opname}`

Le risorse sono organizzate in moduli. Ognuno di questi rappresenta una diversa area funzionale e contiene:

- **Ambito e indice**: una descrizione del contenuto coperto dal modulo e un indice del contenuto
- **Casi d'uso**: la guida per gli usi comuni del modulo, e come affrontarli
- **Sicurezza / Privacy**: informazioni su questi aspetti
- **Roadmap**: lo stato di definizione del modulo

I moduli poi sono generalmente organizzati, a loro volta, in 3 gruppi e poi in livelli [41] (vedi fig. 5.3):

- Infrastruttura (livelli 1 e 2)
- Contenuto (livelli 3 e 4)
- Ragionamento (livello 5)

All'interno delle specifiche del nuovo ecosistema nazionale FSE 2.0 ampio spazio è stato dato a questa tecnologia nella quale vengono riposte grandi speranze affinché non succeda quanto accaduto con HL7 v3 [42].

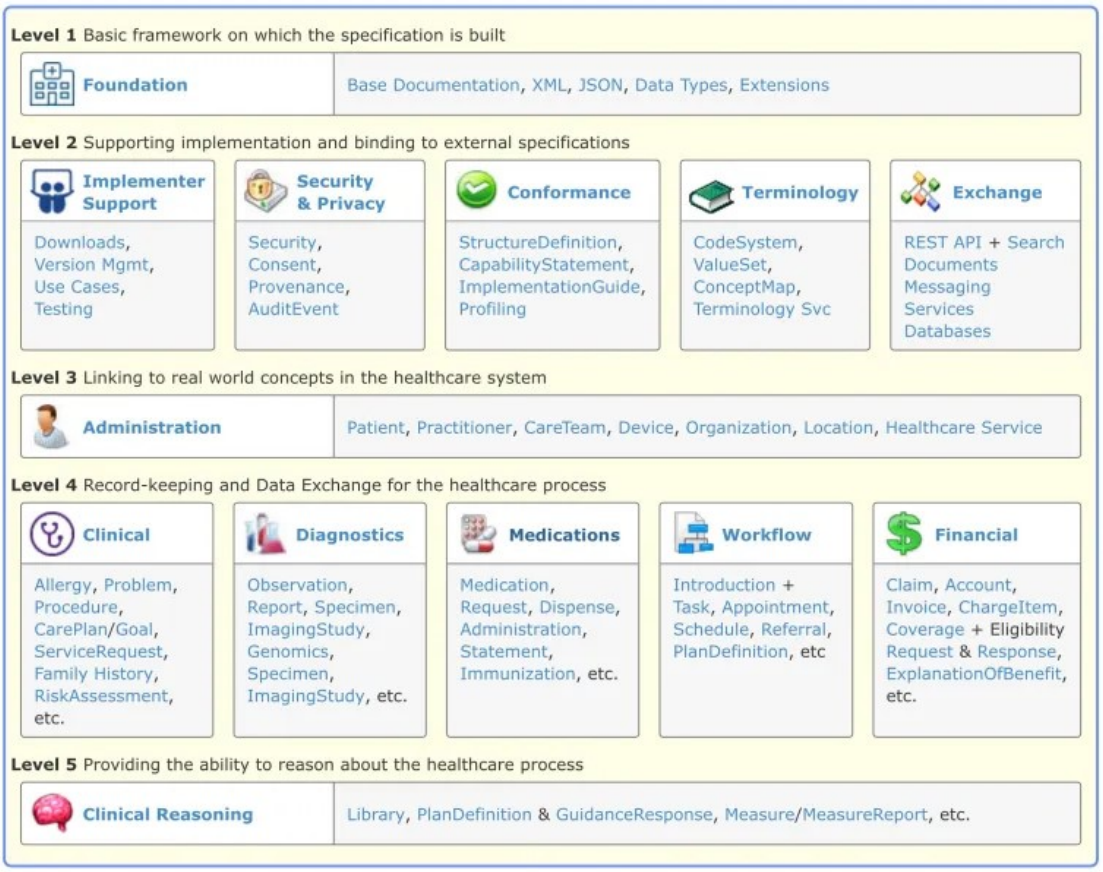

Figura 5.3. Livelli, moduli e risorse HL7 FHIR

5.2 Le comunicazioni con l'esterno

Come ormai in quasi tutti i contesti aziendali, ed una rete aziendale sanitaria non fa eccezione, sempre più spesso c'è la necessità di "integrarsi", scambiare dati, non solo tra software o apparati che sono fisicamente all'interno dell'azienda stessa, e che quindi possono beneficiare delle tecnologie di protezione ivi presenti, ma anche con software, applicativi, servizi fisicamente dislocati all'esterno di una ASL. Questo avviene per i più disparati motivi e lo scambio dei dati può essere sia in uscita che in entrata. Vediamo alcuni casi a titolo esemplificativo:

- applicativi sanitari (solitamente "verticali" più o meno piccoli) installati in "server farm" esterne all'azienda ma che devono funzionare come se fossero interni

- servizi di scambio file per molteplici necessità (rendicontazioni attività, costi, materiali verso servizi ragionali o nazionali)

- accesso a servizi nazionali per invio o interrogazione di dati demografici, di reddito, di patologie

Da questo elenco, non esaustivo ma esemplificativo, emerge la continua necessità di implementare forme di comunicazione sicure verso l'esterno della rete aziendale, sempre allo scopo principale di garantire la dovuta sicurezza in un ambito che, come già detto, resta uno dei più delicati riguardo gli aspetti di privacy dei cittadini.

Vediamo quali sono alcuni delle principali tecnologie oggi in uso che permettono di garantire la necessaria sicurezza dei dati interscambiati.

5.2.1 Le VPN

Le VPN[28] sono ormai un metodo assolutamente consolidato che permette di rendere un applicativo esterno parte integrante di una rete privata aziendale, come quella di una USL, in maniera, praticamente, trasparente. Grazie ad esse si possono integrare i software che restano fisicamente attestati su server esterni (spesso ormai, a loro volta, virtuali) utilizzando qualunque tecnologia vista prima (in special modo HL7) come se fossero interni alla rete aziendale. La sicurezza intrinseca che una VPN oggi permette, fornisce le garanzie necessarie e sufficienti a rendere anche questi servizi sicuri dal punto di vista dell'interscambio dei delicati dati clinici.

5.2.2 I Webservices

Sebbene se ne voglia parlare come servizio per scambiare i dati verso l'esterno, la tecnologia dei "webservices" è, in realtà, trasversale ed utilizzabile sia tra applicativi assestati all'interno della stessa rete (aziendale) che tra applicativi che comunicano da o verso l'esterno.

Normalmente, se utilizzata tra applicativi che non fanno parte della stessa rete, è necessario implementare preventivamente un collegamento sicuro tra i sistemi (usando quindi un collegamento opportunamente protetto da una VPN) ed è il caso, ad esempio, di un applicativo "verticale" che scambia dati con il HIS. Altresì, si può proteggere l'accesso ai webservices tramite un sistema di cifratura che preveda l'utilizzo di certificati di sicurezza specifici e chiavi, come ad esempio i nuovi servizi messi a disposizione delle Regioni e delle ASL da Sogei per l'avvio, ormai prossimo, di ANA [43] i quali seguono le Linee Guida Modello di Interoperabilità definite da AgID [44].

I webservices quindi possono essere utilizzati in entrambe le "direzioni", sia per consultare (leggere, ma anche inserire) dati presenti in servizi esterni all'Azienda, oppure per far sì che applicativi attestati all'esterno possano accedere (di nuovo: sia inserire che anche solo leggere) a dati presenti in applicativi interni alla rete aziendale.

[28] Virtual Private Network

I principali vantaggi dell'utilizzo di questa modalità rispetto ad un'integrazione "sincrona" come quella HL7 risiedono nel fare "minor traffico" o, per meglio dire, generare traffico in maniera che possiamo definire più "puntuale", cioè solo per i dati di stretto interesse. Facciamo un esempio: un'integrazione HL7 per l'interscambio dei dati anagrafici da un server MPI verso un servizio qualunque invia costantemente tutti gli inserimenti di nuove anagrafiche, aggiornamenti di quelle esistenti ed eventuali "merge" tra di essi, con un traffico continuo che arriva tranquillamente a circa 50.000 movimentazioni giornaliere nella sola "piccola" ASL della Valle d'Aosta, anche se comunque questo può essere sicuramente utile in un contesto in cui vige la necessità di tenere costantemente allineati i database anagrafici dei diversi servizi, così da essere anche "ridondati" e non necessitare del servizio master in caso di interruzione della rete o indisponibilità dello stesso.

Un altro servizio invece, che possiamo definire meno "critico", può non avere necessità di essere tenuto costantemente aggiornato su tutto il database anagrafico dell'Azienda, ma di avere al suo interno solo un ridotto sottoinsieme di questo, comprensivo delle sole anagrafiche di cui il servizio necessita, ad esempio l'applicativo delle protesi e ausili che fornisce servizi alla sola popolazione che ne ha necessità. In questo caso, attraverso l'interrogazione da parte di questo servizio verso MPI, effettuata via webservice, delle sole anagrafiche di interesse permette una drastica riduzione del traffico, dell'occupazione di spazio fisico sul database del verticale e, infine, di ottimizzazione senza intaccare le reali necessità di aggiornamento del verticale.

5.2.3 Gli SFTP

Sebbene possa considerarsi una tecnologia obsoleta, teoricamente in via di progressiva dismissione, ma, praticamente, ancora molto utilizzata per specifici "flussi" sanitari, quello dello *scambio file* resta infatti una pratica tutt'altro che dismessa. Essa prevede che vengano generati file testuali secondo specifici "tracciati", solitamente di tipo "csv" o "txt" dentro cui vengono inseriti dati riguardanti solitamente record di attività erogate (come per esempio i ricoveri effettuati da un ospedale in un trimestre e tutti i dettagli relativi, oppure le esenzioni). A tale scopo vengono così utilizzati sistemi di trasferimento file come il protocollo SFTP[29] o altri servizi proprietari attestati direttamente sui siti web dei gestori interessati (tra i quali ad esempio, le Regioni, o il sistema nazionale gestito da Sogei denominato **SistemaTS**).

[29] SSH File Transfer Protocol

Appendice A

Il caso della sanzione alla AUSL della Valle d'Aosta

Nel novembre del 2022 all'Azienda Sanitaria della Valle d'Aosta, è stata comminata una sanzione [45, 46] a causa di un denuncia di un utente dipendente dell'AUSL che aveva rilevato accessi ai propri dati da parte di un altro utente anch'esso dipendente dell'AUSL nonostante che:

- l'utente/paziente avesse negato il consenso alla costituzione del proprio DSE
- l'utente/paziente non fosse "in cura" presso altri operatori

La causa di questa denuncia ha origine da una scelta dell'Azienda, presa poco dopo l'inizio della pandemia di **Covid19**, di *allentare* i filtri privacy del principale applicativo sanitario in uso presso l'azienda, TrakCare versione 2014, che assume, vista l'estensione delle sue funzionalità (anche se non è l'unico software clinico in uso[1]), il ruolo di DSE dell'Azienda USL della Valle d'Aosta.

La sanzione comminata dal Garante alla AUSL è stata di 40.000€ ed è stata presa in considerazione, oltre alla violazione sopra descritta, anche la mancanza di specifici "alert" che avrebbero dovuto rendere evidenti violazioni di questo e di altri tipi.

La AUSL, certa della correttezza della propria decisione presa in momento eccezionale ed allo scopo di garantire ai cittadini, durante la pandemia, il miglior accesso alle cure, ha fatto ricorso verso la sentenza e, a seguire, appello in Cassazione, per la quale è ancora attesa, nel momento in cui viene scritto questo testo, l'emanazione della sentenza definitiva.

---

[1] A voler essere precisi, dato che TrakCare funge sia da "producer" di documenti clinici che da "consumer" di questi, ma **non è l'unico a farlo**, non è TrakCare il DSE Aziendale, ma ne è una parte preponderante. Infatti il concetto (logico) di DSE Aziendale consiste nell'insieme dei dati clinici prodotti da tutti gli applicativi aziendali, come anche il RIS, il LIS, e svariati altri (vedi par. 2.1)

Bibliografia

[1] Pier Paolo Muià, "LA TUTELA DELLA PRIVACY IN AMBITO SANITARIO", Maggioli Editore, 2018

[2] L. Degani, A. Lopez, S. Familiari, "L'APPLICAZIONE DEL GDPR PRIVACY NEI SERVIZI SOCIOSANITARI", Maggioli Editore, 2018

[3] A. Rossotti, "INFORMATICA MEDICA", McGraw Hill, 2021

[4] Agenzia per la cybersicurezza nazionale, "Cyber Attacchi in crescita nel settore sanitario", https://www.acn.gov.it/portale/w/cyberattacchi-in-crescita\-nel-settore-sanitario-dati-digitali-nel-mirino-degli-hacker

[5] cybersecurity360, "La sanità è sotto attacco", https://www.cybersecurity360.it/nuove-minacce/la-sanita-e-sotto-attacco-soluzioni-e-best-practice-per\-metterla-in-sicurezza/

[6] L. Bouganim and Y. Guo, DATABASE ENCRYPTION, Hal, 2011 https://hal.archives-ouvertes.fr/hal-00623915/document

[7] HL7 Italia, http://www.hl7italia.it/hl7italia_D7/

[8] Crittografia omomorfica, https://it.wikipedia.org/wiki/Crittografia_omomorfica

[9] Advanced Encryption Standard, https://it.wikipedia.org/wiki/Advanced_Encryption_Standard

[10] Crittografia RSA, https://it.wikipedia.org/wiki/RSA_(crittografia)

[11] Cifratura TLS, https://it.wikipedia.org/wiki/Transport_Layer_Security

[12] Cifratura SSL, https://it.wikipedia.org/wiki/Secure_Shell

[13] GDPR, https://gdpr-info.eu/

[14] GDPR, "Articolo 33", https://gdpr-info.eu/art-33-gdpr/

[15] GDPR, “Articolo 34”,
https://gdpr-info.eu/art-34-gdpr/

[16] Garante della privacy, "Guida all’applicazione del Regolamento europeo in materia di protezione dei dati personali - approccio basato sul rischio e misure di accountability (responsabilizzazione)",
https://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di\accountability-responsabilizzazione-di-titolari-e-responsabili

[17] Garante della privacy, "Data Protection by Design e Data Protection by Default",
https://www.garanteprivacy.it/regolamentoue/data-protection-by-design-e-data-protection-by-default

[18] cybersecurity360, "Business continuity e disaster recovery, ecco le strategie a prova di emergenza",
https://www.agendadigitale.eu/sicurezza/business-continuity-e-disaster-recovery-ecco-le-strategie\-a-prova-di-emergenza

[19] cybersecurity360, "Nuova ISO 27001:2022: cosa cambia, i punti di accordo col GDPR e come adeguarsi",
https://www.cybersecurity360.it/legal/nuova-iso-270012022-cosa\-cambia-i-punti-di-accordo-col-gdpr-e-come-adeguarsi

[20] Luc Bouganim, Yanli Guo, "Database encryption",
https://hal.archives-ouvertes.fr/hal-00623915/document

[21] The Anatomy and (In)Security of Microsoft SQL Server Transparent Data Encryption (TDE) or How to Break TDE,
https://medium.com/@s.mcauliffe_17464/the-anatomy-and-in\-security-of-microsoft-sql-server-transparent-data-encryption\-tde-or-how-to-d164eb08564

[22] C. Fiandrino, "Descrizione della Query Optimization",
http://claudiofiandrino.altervista.org/Masterdegree/Databasemanagementsystem/queryoptimization.pdf

[23] E. Shmueli, R. Vaisenberg, and E. Gudes, "Implementing a database encryption solution, design and implementation issues",
https://www.sciencedirect.com/science/article/pii/S0167404814000509

[24] MyDiamo, "Types of Database Encryption methods",
https://mydiamo.com/types-of-database-encryption-methods

[25] G. della privacy, “Definizione Data Breach”,
https://www.garanteprivacy.it/regolamentoue/databreach

[26] T. Security, “The Definitive Guide To Encryption Key Management Fundamentals”,
https://info.townsendsecurity.com/definitive-guide-to-encryption\-key-managementfundamentals

[27] A.Deshmukh and R. Qureshi, "Transparent data encryption- solution for security of database contents", International Journal of Advanced Computer Science and Applications, vol. 2, March 2011, https://arxiv.org/ftp/arxiv/papers/1303/1303.0418.pdf

[28] L. Bouganim and Y. Guo, "Database encryption", Hal, September 2011, DOI 10.1007/978- 1-4419-5906-5 677, https://hal.archives-ouvertes.fr/hal-00623915/document

[29] Thales, "Database Encryption Approaches", https://cpl.thalesgroup.com/encryption/selecting-right-encryption\-approach

[30] Vito Lavecchia, "Differenza tra DAC e MAC in informatica", https://vitolavecchia.altervista.org/differenza-tra-dac-e-mac\-in-informatica/

[31] C. Group, "Descrizione di un ePHI", https://compliancy-group.com/hipaa-ephi-electronic-protected\-health-information/

[32] H. Journal, "HIPAA and HITECH", https://www.hipaajournal.com/hipaa-and-hitech/

[33] HL7 Sito ufficiale, https://www.hl7.org

[34] HL7 Sito ufficiale italiano, https://www.hl7.it

[35] IHE Sito ufficiale italiano, https://www.ihe-italia.net/home-page

[36] Affinity Domain Italia, https://www.fascicolosanitario.gov.it/affinity-domain.html

[37] Standard HL7, https://moodle2.units.it/pluginfile.php/745634/mod_resource/content/1/13-FIM-STANDARDHL7.pdf

[38] REST - Representational State Transfer, a new approach to systems architecture and a lightweight alternative to web services, http://rest.elkstein.org/2008/02/what-is-rest.html

[39] OAuth, https://it.wikipedia.org/wiki/OAuth

[40] HL7 FHIR, https://www.aidainformazioni.it/index.php/aidainformazioni/article/view/302/57

[41] Alla scoperta di FHIR, https://salutedigitale.blog/2022/03/08/alla-scoperta-di-fhir/

[42] Uso FHIR in FSE 2.0, https://www.agendadigitale.eu/sanita/fascicolo-sanitario\-elettronico-2-0-cosi-sara-vera-svolta-per-sanita-e-cittadini/

[43] Anagrafe Nazionale Assistiti,
https://sistemats1.sanita.finanze.it/portale/
anagrafe-nazionale-assistiti-ana-

[44] Linee Guida per l'interoperabilità,
https://docs.italia.it/media/pdf/lg-modellointeroperabilita-docs/
vintra-work/lg-modellointeroperabilita-docs.pdf

[45] Garante per la protezione dei dati personale, "Ordinanza ingiunzione nei confronti di Azienda USL Valle d'Aosta",
https://www.garanteprivacy.it/web/guest/home/docweb/-/
docweb-display/docweb/9819792

[46] M. Mangia, "Nessuna deroga per l'emergenza covid",
https://salutedigitale.blog/2022/11/30/privacy-nessuna-deroga\
-per-lemergenza-covid-il-garante-sanziona-la-asl-valle-daosta\
-per-il-dossier-sanitario/