Fascicolo Sanitario Elettronico:

il ruolo della tecnologia nella tutela della privacy e della sicurezza

INDICE

Introduzione

In questo documento si trovano le considerazioni di un gruppo di lavoro relativamente alle implicazioni tecnologiche e di sicurezza del recente provvedimento del Garante della Privacy in merito al Fascicolo Sanitario Elettronico (FSE).

L'autore del documento è un soggetto collettivo costituito dai rappresentanti di aziende di informatica appartenenti alla Community di partner Oracle, specializzato nella sicurezza dell'informazione, che si qualifica per la competenza nella progettazione, realizzazione e gestione di soluzioni di sicurezza sotto il profilo tecnologico ed organizzativo.

La Community for Security è un'organizzazione che affronta il tema della sicurezza dell'informazione e che raccoglie le più importanti aziende di informatica italiane ed internazionali nell'ecosistema dei partner Oracle. Essa vede tra i suoi partecipanti anche le più significative associazioni professionali dedicate alla sicurezza, all'auditing ed all'informatica quali Clusit, AIEA ed Aused. La lista dei partecipanti si può trovare nel link: www.oracle.com/global/it/security/partner.html.

È stato costituito da alcuni mesi, all'interno di tale organizzazione, un gruppo di lavoro (GdL) strettamente dedicato al tema del recente provvedimento sul FSE, allo scopo di creare cultura e conoscenza e di integrare la proposizione di valore verso il mercato. Al GdL hanno aderito le seguenti aziende / associazioni: AIEA, CLUSIT, Deloitte, Gruppo Terasystem, Kelyan, KPMG, Mediaservice, Oracle, Present, Protiviti, Spike Reply, Sinfo One, Studio Legale Abeti, Tech Gap e Zeropiu.

Il GdL ha condiviso le proprie esperienze e competenze per analizzare il provvedimento relativo l'FSE e per valutarne le implicazioni in ragione della sicurezza dell'informazione e della relativa fruizione. Non si è, peraltro, posto l'obiettivo di affrontare gli aspetti funzionali ed applicativi, ma ha deciso di focalizzarsi sulle proprie competenze di base che riguardano la sicurezza.

La scelta di indirizzare una specifica architettura di sicurezza rappresenta, rispetto al tradizionale approccio applicativo, un'evoluzione resa necessaria dalla complessità delle soluzioni richieste e dalla continua evoluzione della tecnologia.

Il contributo originale che il documento intende dare riguarda l'utilizzo, nello specifico contesto del FSE, del know how di sicurezza informatica accumulato dalle aziende che hanno contribuito alla sua redazione. Gli interlocutori di questo documento sono le strutture sanitarie, gli enti regionali, le società in house coinvolte nella realizzazione del FSE e gli attori dell'offerta di applicazioni e servizi professionali che contribuiscono alla soluzione degli aspetti applicativi e gestionali.

Il documento è articolato in sezioni, ognuna delle quali affronta in modo sintetico, ma allo stesso tempo esaustivo, gli aspetti che caratterizzano il tema della sicurezza applicato al FSE.

La Customer experience il cittadino al centro del sistema

La Customer Experience viene definita in letteratura come l'insieme di tutti gli aspetti di interazione tra il cliente, l'organizzazione ed i suoi servizi (Seybold, 2001; Berry et alt., 2002; Schmitt, 2003; Lasalle et alt., 2003).

Il modo e la misura in cui il cliente percepisce il valore che un'azienda gli vuole fornire è un fattore chiave di successo per l'azienda stessa.

La "customer experience" è una modalità manageriale che permette di valutare le relazioni cliente-azienda in modo maggiormente accurato e, quindi, in grado di comprendere anticipatamente le esigenze ed i bisogni dei propri clienti in modo da predirne la soddisfazione adottando, di conseguenza, soluzioni strategiche ed organizzative che ne consentano la sostenibilità

Comprendere i propri clienti, capire ad esempio quali sono i diversi segmenti di clienti, quali bisogni (espressi ed inespressi) etc. significa sviluppare un'offerta in grado di soddisfare il proprio mercato di riferimento veicolandola al meglio attraverso tutti i canali che oggi sono disponibili.

Partendo da questa considerazione si sviluppa il concetto di "cittadino-paziente" cioè il cliente del sistema sanitario ed il rapporto che crea con quanto di più vicino gli può essere, dal punto di vista informatico, nel gestire il proprio rapporto con la salute: il Fascicolo Elettronico Sanitario.

Il FSE è costituito dall'insieme di dati derivati non solo da diversi sistemi informativi sanitari - tra cui la Cartella clinica -, ma anche dai nuovi sistemi di cura domiciliare. Inoltre non si possono trascurare tutte quelle informazioni prodotte dal paziente in quella che potremmo definire la gestione "consapevole" della propria salute.

Molti sono gli argomenti e gli aspetti da trattare e vi è chi lo fa sicuramente con maggior appropriatezza; nel presente documento abbiamo voluto prendere **decidere cosa ed a chi rendere visibili i (propri) dati sanitari",** in altri termini la sicurezza nella gestione e nella fruizione delle informazioni che costituiscono il FSE.

Il documento tratta questi aspetti partendo dalle indicazioni del Garante della Privacy sia per quanto riguarda la scelta del paziente nel costituire o meno il proprio FSE e se costituirlo con tutte o una parte delle informazioni. Affronta, inoltre, gli aspetti legati agli obblighi imposti dal **Dlgs 196/03** relativamente ai requisiti di riservatezza dei dati sensibili che possono essere soggetti ad un uso improprio e scorretto, sia per quanto concerne i dati visibili sia per quanto eventualmente il paziente voglia oscurare successivamente.

Prende, quindi, in esame gli aspetti relativi a chi può fruire le informazioni gestite dall'FSE e con quali strumenti e modalità le può consultare.

In questo senso, viene fortemente sentito dalle aziende sanitarie ed a maggior ragione da chi eroga i servizi relativi al FSE la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei cittadini pazienti, sistemi di controllo tesi a prevenire quegli usi scorretti che, oltre ad esporre l'azienda stessa a rischi (tanto patrimoniali quanto penali), possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

Riprendendo i temi legati alla User Experience, questa dovrà essere sicura in termini di protezione dell'informazione sia per quanto concerne l'information lifecycle management (ovvero quell'insieme di pratiche che proteggono il dato informatico nella sua banca dati) sia per quanto riguarda le informazioni gestite nei repository di cartella clinica (gestione documentale & archiviazione sostitutiva).

Dovranno essere sicuri i sistemi di acquisizione dei dati, tipicamente basati su web services e tecnologie di integrazione attraverso i quali le informazioni che costituiscono il FSE vengono acquisite e scambiate tra i diversi attori della catena (AO/ASL, Medici di medicina generale, medici specialistici, case di riabilitazione, case di cura, i pazienti etc,).

Dovrà essere altresi` sicura la fruizione della banca dati in cui è custodito il FSE relativo al singolo paziente affinchè questi sia protetto da azioni fraudolente che possono essere operate da parte degli operatori, degli hacker, degli amministratori di sistema e, più in generale, da tutti quei soggetti che possono trarre vantaggio dall'acquisire informazioni sensibili sulla persona.

La gestione del FSE ed a maggior ragione gli aspetti legati all'utilizzo delle tecnologie informatiche che ne permettono la fruizione devono garantire la semplicità dell'uso, evitando richieste multiple di accreditamento al sistema o l'utilizzo di tecnologie troppo sofisticate - e spesso costose - che inibirebbero la maggior parte dei pazienti all'uso in quanto essi sono, appunto, pazienti e non tecnici informatici.

Dovrà essere multicanale, dovrà, cioè, permettere al cittadino non solo di fruire dell'FSE attraverso il "tradizionale" browser web, ma anche essere aperto a tecnologie come i chioschi informatici ed a nuove tecnologie di fruizione quali ed esempio gli smart phone e più in generale ai device mobili. È una notazione commerciale, ma negli Stati Uniti le vendite di libri cartacei sono state superate dagli smart reader elettronici, uno dei potenziali strumenti di fruizione del FSE.

Oltre alla multicanalità dovrà essere curata l'ergonomia, in funzione dell'utilizzo da parte di persone diversamente abili, secondo gli standard in vigore a livello nazionale ed europeo.

Deve essere funzionale sul piano della gestione con l'utilizzo di sistemi di self provisioning ovvero con soluzioni informatiche che permettano facilmente al cittadino di cambiare la password, recuperarla se perduta o rigenerarla nel momento in cui sono scaduti i termini di validità.

Dovrà essere multilingua: gli italiani oggi sono parte dell'Unione Europea ed il diritto alla salute contempla i paesi membri dell'Unione; più in generale oggi i cittadini Italiani viaggiano e lavorano in tutti e cinque i continenti, pertanto è impensabile che il FSE non contempli meccanismi di fruizione multilingua che comprendano almeno le prime cinque lingue più diffuse al mondo.

Essendo uno strumento utilizzato dai cittadini/pazienti e dovendo, quindi, rispondere al tema della User Experience, dovrà essere dotato strumenti di monitoraggio non solo per verificarne il costante e corretto funzionamento ma anche e soprattutto per comprendere l'utilizzo dei servizi esposti, arricchirli e migliorarli sul piano funzionale e qualitativo.

Ovviamente non pretendiamo di aver trattato in modo esaustivo tutti gli aspetti della questione, è però vero che attraverso questa lettura potranno emergere quegli aspetti specificatamente legati alla **sicurezza** nel trattamento dei dati contenuti nel FSE, sia che essi riguardino più direttamente i dati del cittadino/paziente sia che essi riguardino l' "azienda" che eroga il servizio.

Profili legali del Fascicolo Sanitario Elettronico

Il presente documento intende fornire una panoramica sui contenuti delle Linee guida approvate dall'Autorità Garante il 16 luglio 2009 in materia di Fascicolo Sanitario Elettronico.

Le linee guida, pur non costituendo normativa cogente, individuano un insieme di misure ed accorgimenti di natura tecnica ed organizzativa che non possono essere né eluse né ignorate, stanti i possibili impatti sotto diversi profili di responsabilità.

Confrontandosi sul tema del FSE con colleghi e clienti emergono in modo ricorrente alcune questioni alle quali in questo documento si è deciso di provare a rispondere, non limitandosi a parafrasare quanto sostenuto dall'Autorità nei propri provvedimenti.

Questi in sintesi i punti sviscerati nei seguenti capitoli del documento:

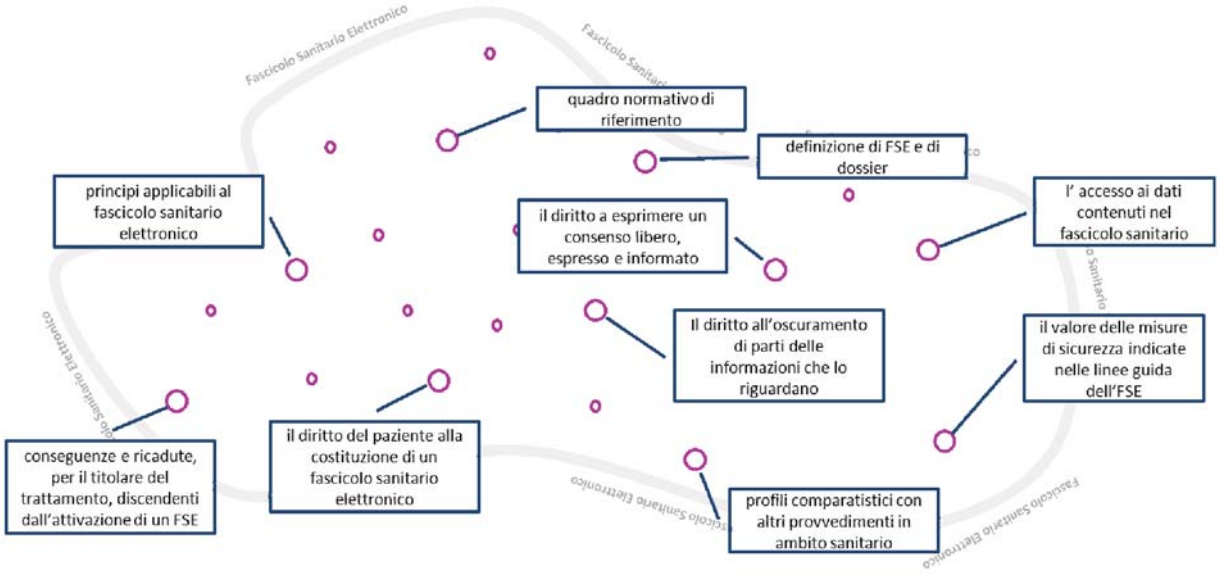


Fig. 1 - Normative e linee guida

Quadro normativo di riferimento

In Italia non esiste un quadro normativo che disciplini espressamente il Fascicolo Sanitario Elettronico. Tuttavia l'adozione del fascicolo si basa su presupposti normativi chiaramente definiti: il diritto alla salute sancito dalla Costituzione, la legge istitutiva del Servizio Sanitario Nazionale, i decreti legislativi 502 del 1992 e 517 del 1993 (c.d. seconda riforma sanitaria), la modifica dell'art. 117 della Costituzione ad opera della Legge Costituzionale 18 ottobre 2001, n. 3.

3.1 Presupposti costituzionali

L'art. 32 della Costituzione sancisce che:

> *"La Repubblica tutela la salute come fondamentale diritto dell'individuo e interesse della collettività e garantisce cure gratuite agli indigenti".*

In pratica per dare attuazione al dettato costituzionale occorre che siano poste in essere misure che tengano conto del fatto che il mantenimento di uno stato di benessere (sia psico-fisico che sociale) è diritto dell'individuo (ad esempio: a ricevere le cure opportune oppure a ricevere sostegno in caso di situazioni di disagio sociale) e interesse della collettività (si pensi, ad esempio, al danno derivante dai giorni di malattia di un lavoratore).

Questa norma sottende una duplice lettura:

- da un lato, con il suo valore programmatico, impegna il legislatore su diversi fronti: la ricerca, la sperimentazione, la riduzione dei tempi d'attesa delle prestazioni sanitarie e in molti altri ambiti, al fine di attuare un sistema di tutela adeguato alle esigenze sociali;
- dall'altro, con la propria valenza precettiva, pone il cittadino, nella posizione di poter vantare, nei confronti dello Stato, un vero e proprio diritto soggettivo nei diversi ambiti in cui questo esplica i suoi effetti.

Sul piano degli interventi finalizzati al governo della sanità ed alla tutela della salute nel tempo si è ricorsi a diversi sistemi a seconda della interpretazione data all'art. 32 della Costituzione Italiana.

3.2 L'istituzione del Servizio Nazionale

Fino al 1978 vi erano in Italia molti enti che svolgevano attività di assistenza sanitaria ed ospedaliera secondo un meccanismo simile a quello previdenziale (per cui gli assistiti erano obbligati a versare parte del loro reddito a tali istituti, i quali con questi fondi, se del caso integrati da trasferimenti dello Stato, assicuravano cure mediche e ricoveri ospedalieri gratuiti agli assistiti che ne avevano bisogno): in luogo di tutti questi enti che sono stati disciolti, L. n° 833/78 ha istituito il Servizio Sanitario Nazionale.

I principi informatori di tale Servizio sono i seguenti:

1. tutti hanno il diritto di ottenere gratuitamente (o pagando un parziale rimborso, il c.d. ticket), in condizioni di eguaglianza, le prestazioni mediche e ospedaliere che il servizio è in grado di offrire;
2. tutti i cittadini debbono contribuire obbligatoriamente, secondo i criteri e nei modi previsti dalle leggi, al finanziamento di tale Servizio, e quindi versare le somme dovute allo Stato;
3. In tutto il territorio nazionale le leggi regionali, in base a criteri delle leggi statali, debbono istituire Unità sanitarie locali (USL o anche UUSSLL), e cioè strutture unificate di base che svolgono compiti di prevenzione e assicurino assistenza medica, farmaceutica e ospedaliera a vantaggio della popolazione ricompresa in ciascuna USL.
4. Il funzionamento del Servizio sanitario nazionale (SSN) è assicurato da un fondo nazionale iscritto nel bilancio dello Stato, che lo Stato ripartisce tra le Regioni, le quali a loro volta ripartiscono le loro quote tra le USL.
5. Le spese, gli investimenti, le iniziative ecc. delle diverse componenti del Servizio (ministero della sanità, regioni, USL ecc.) dovrebbero avvenire secondo un Piano Sanitario Nazionale, approvato dal Parlamento, e secondo Piani Sanitari Regionali in attuazione del Piano Nazionale.
6. Le prestazioni del SSN vengono assicurate o da soggetti privati (medici, cliniche private, ecc.) mediante convenzioni con il Servizio oppure direttamente dalle USL con personale e strutture proprie.

3.3 La seconda riforma sanitaria

Alcuni anni dopo, le spinte riformatrici portarono ad una diversa interpretazione dell'art. 32, ritenendo che il principio enunciato fosse relativamente precettivo nel senso che il cittadino vantasse pur sempre un diritto alla tutela della salute destinate.

Questa "nuova" interpretazione portò, fermi restando i principi ispiratori della prima riforma (generalità, globalità ed eguaglianza), alla revisione del S.S.N. (attraverso i Decreti Legislativi n° 502/1992 e n°229 del 1999) il cui assetto organizzativo venne innovato con l'aziendalizzazione delle UU.SS.LL e dotando le nuove strutture di:

- personalità giuridica pubblica,
- autonomia imprenditoriale,
- strumenti operativi innovativi largamente mutuati dal settore privato (gestione per obiettivi, contabilità economica, contabilità analitica per centri di costo e di responsabilità, controllo di gestione, rilevazione e misurazione dei costi e dei risultati),

e improntando la gestione delle risorse economiche, strumentali ed umane all'uopo destinate a criteri di efficienza, efficacia ed economicità.

Le vecchie UU.SS.LL. vennero sostituite dalle "aziende" con la distinzione delle stesse in Aziende Sanitarie Locali ed Aziende Ospedaliere. In particolare, le Aziende Sanitarie Locali furono chiamate ad erogare prestazioni in un contesto territoriale definito dalle rispettive Regioni e Province Autonome.

3.4 La Legge Costituzionale 18 ottobre 2001, n. 3

Questa legge(riforma del Titolo V della Costituzione) ha "modificato" la ripartizione delle competenze legislative tra lo Stato e le Regioni.
Con essa le competenze di organizzazione sanitaria sono state demandate alle Regioni.
In altre parole, mentre lo Stato ha la responsabilità di assicurare a tutti i cittadini il diritto alla salute mediante un forte sistema di garanzie, attraverso i Livelli essenziali di assistenza (c.d. LEA), le Regioni e Province autonome hanno la responsabilità diretta della realizzazione del governo e della spesa per il raggiungimento degli obiettivi di salute del Paese. Inoltre, alle Regioni viene riconosciuta competenza esclusiva nella regolamentazione ed organizzazione di servizi e di attività destinate alla tutela della salute e dei criteri di finanziamento delle Aziende sanitarie locali e delle aziende ospedaliere (anche mediante: controllo di gestione e valutazione della qualità delle prestazioni sanitarie nel rispetto dei principi generali fissati dalle leggi dello Stato).

3.5 Le linee guida del Garante

In questo quadro normativo si inserisce il provvedimento dell'Autorità Garante, del 16 luglio 2009.

L'Autorità, in seguito alle segnalazioni, ai confronti con gli operatori e alle proprie attività di approfondimento, constata l'esistenza di alcune iniziative

> *volte ad archiviare, mediante nuove tecniche, la svariata documentazione di cui gli organismi sanitari si avvalgono a diverso titolo nei processi di cura dei pazienti come, ad esempio, le più recenti esperienze di informatizzazione della cartella clinica, documento sanitario che pure è regolato da specifiche disposizioni normative*

Accanto ad esse si fa avanti un altro tipo di attività finalizzata a modernizzare la "realtà sanitaria".

Mentre per la dematerializzazione della documentazione (tecnica, amministrativa, …) trattata in ambito sanitario esiste già un quadro specifico e un espresso riferimento è previsto all'interno del decreto legislativo 30 giugno 2003, n. 196, per quel che attiene

> *la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari riguardanti un medesimo individuo e, in prospettiva, l'intera sua storia clinical'intera sua storia clinica*

Non essendo, ad oggi, disponibile un preciso quadro volto a regolamentare quest'aspetto della "modernizzazione", il Garante ha ritenuto opportuno individuare un primo quadro di cautele, al fine di delineare per tempo specifiche garanzie e responsabilità, nonché alcuni diritti connessi.

3.6 Lo schema di disegno di legge su «Sperimentazione clinica e altre disposizioni in materia sanitaria»

Nel corso del mese di luglio è stato presentato al Consiglio dei Ministri un disegno di legge che si pone diversi obiettivi tra cui quello di fornire un presupposto di natura normativa primaria, per l'istituzione del FSE.

In esso si fornisce la definizione di FSE e si espandono le finalità del FSE, oggi (secondo la lettura del quadro normativo data dall'Autorità) limitate a quella di "prevenzione, diagnosi, cura e riabilitazione", estendendole a quelle di:

- studio e ricerca scientifica in campo medico, biomedico ed epidemiologico
- programmazione, gestione, controllo e valutazione dell'assistenza sanitaria.

In esso, il legislatore prendendo atto dell'attuale frammentarietà delle iniziative in merito alla costituzione del FSE, prova a fornire un'impostazione che nasca con una radice comune in modo da circoscrivere il numero di soggetti che possa, nel prossimo futuro avviare iniziative in tema di FSE e auspicare una interoperabilità che nel contesto attuale (in cui possono essere avviate iniziative di FSE differenti da una ASL all'altra e da una Regione all'altra) è piuttosto improbabile. A questo proposito ai commi 3 e 4 dell'articolo 15, del disegno di legge di cui trattasi, si fa riferimento al fatto che

> *il fascicolo sanitario elettronico è alimentato in maniera continuativa dai soggetti che prendono in cura l'assistito nell'ambito del Servizio sanitario nazionale e dei servizi socio-sanitari regionali.*
> *Il fascicolo sanitario elettronico è istituito dalle Regioni e Province autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali.*

Le linee guida su FSE e gli altri provvedimenti in materia sanitaria: profili comparatistici.

Il tema del trattamento di dati in ambito sanitario è emerso in altre pronunce dell'Autorità Garante. In particolare si segnalano per importanza i seguenti Provvedimenti a carattere generale che hanno diversi elementi in comune, sia nell'impostazione generale sia per quanto riguarda la necessità di adozione di misure di sicurezza in grado di contrastare efficacemente i rischi connessi a questo tipo di trattamento:

- le *Linee guida in tema di referti on-line* del 19 novembre 2009;
- le *Linee guida per i trattamenti di dati personali nell'ambito delle sperimentazioni cliniche di medicinali* del 24 luglio 2008;
- le linee guida in tema di *Referti on-line* prevedono due modalità di realizzazione;
- l'invio del referto presso la casella di posta elettronica del soggetto interessato;
- la disponibilità del referto su un sito Internet al fine di poterlo visualizzare/scaricare in locale.

Il Garante ha evidenziato la facoltatività dei servizi di *e-availability* precisando, al pari di quanto indicato per l'FSE, che devono essere considerati i seguenti aspetti:

- il rilascio dell'informativa e la raccolta del consenso;
- il rispetto dell'art. 84 del codice privacy (intermediazione di personale medico o esercente professioni sanitarie) a fronte del quale si può accompagnare la disponibilità del referto on-line con "un giudizio scritto e la disponibilità del medico di fornire ulteriori indicazioni su richiesta dell'interessato";
- l'attuale impraticabilità di rendere disponibili referti on-line che attengano, ad esempio, a test genetici;
- la necessità di adempiere le Linee guida in tema di FSE nel caso si creino degli "archivi dei referti";
- l'adozione di determinate misure di sicurezza.

Le linee guida in tema di sperimentazioni cliniche sono state approvate per far fronte, come si può dedurre dalla lettura della presentazione del Provvedimento per far fronte alle *numerose criticità emerse a seguito di accertamenti e verifiche presso società farmaceutiche e enti di ricerca. I test clinici sui farmaci, infatti, comportano un rilevante flusso di dati sanitari tra numerosi soggetti: case farmaceutiche, centri di sperimentazione, laboratori di analisi, organizzazioni di ricerca che si occupano del monitoraggio dello studio e dell'analisi statistica.*

Atteso che le questioni aperte sono molteplici, grande attenzione viene dedicata a:

- Differenze tra consenso informato ai fini della sperimentazione e consenso al trattamento;
- Revocabilità del consenso prestato anche in tempi e momenti diversi della sperimentazione;

- Caratteristiche specifiche dell'Informativa sul trattamento da rilasciare al paziente sottoposto a sperimentazione;
- Natura dei dati personali dei pazienti sottoposti alla sperimentazione (non già anonimo ma che rende identificabile indirettamente il paziente)
- Riduzione dei tempi di conservazione dei dati trattati nel corso della sperimentazione
- Regole nel caso di flussi di dati verso paesi terzi attivate nell'ambito di studi promossi da promotori che operano in gruppi multinazionali.

Tenuto conto dei diversi momenti temporali di approvazione dei provvedimenti (postumo per i referti on line e anteriore per le sperimentazioni cliniche), emerge con chiarezza un filo rosso che unisce e raccorda le regole di trattamento espresse nei vari interventi e che, sostanzialmente, si rifanno ai medesimi principi ispiratori.

A titolo meramente esemplificativo si fornisce un estratto delle misure di sicurezza presenti nei tre provvedimenti riferite ai concetti di autenticazione ed autorizzazione.

TIPO DI MISURA	FSE/DOSSIER	PROVVEDIMENTO REFERTI ON LINE	SPERIMENTAZIONI CLINICHE
Sistemi di autenticazione	*Idonei sistemi di autenticazione e di autorizzazione*	*Utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di strong authentication;*	*Idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento.*
Sistemi di autorizzazione	*L'adozione di procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati*	*Idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati), prevedendo il ricorso alla strong authentication con utilizzo di caratteristiche biometriche nel caso del trattamento di dati idonei a rivelare l'identità genetica di un individuo.*	*Procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati del trattamento;*

Fig. 2 -

Fascicolo sanitario e dossier sanitario

Nell'ottica di informatizzazione della sanità, il sistema di gestione della cartella clinica elettronica deve essere contestualizzato e adattato al livello evolutivo sia dal punto di vista regolamentare che tecnologico.

La diffusione delle reti telematiche e degli standard sulla comunicazione sanitaria permettono di importare documentazione generata da autori diversi in località diverse.

In quest'ottica sono state individuate due soluzioni opposte all'interno dei sistemi informativi clinici:

- la "cartella clinica elettronica locale", limitata ad una singola struttura sanitaria (Electronic Patient Record);
- il "Fascicolo Sanitario Personale", le forme più complete di servizio che prevedono una qualche modalità di integrazione e di accesso in rete su dati provenienti da applicazioni cliniche eterogenee (Electronic Health Record).

Quest'ultimo livello di servizio può essere implementato in diverse forme, ma richiede comunque un alto grado di armonizzazione di funzionalità e strutture-dati (a livello regionale o nazionale).

In linea teorica, le informazioni cliniche individuali relative a tutti gli accessi di un cittadino a qualsiasi struttura sanitaria possono essere rese disponibili in modo sicuro in qualsiasi momento e in qualsiasi punto di accesso della rete.

Tuttavia, le informazioni devono essere scambiate tramite reti sicure e i dati personali del cittadino devono rispettare precisi vincoli di privacy secondo la normativa vigente; tali vincoli saranno di diverso grado, in funzione dei diversi scopi per cui i dati clinici vengono condivisi.

In Europa, nel 2007, il c.d. **Gruppo ex art. 29** adottò un importante documento , cui, due anni dopo, si sarebbero ispirate le linee guida del Garante, in esso viene fornita la definizione di Cartella Clinica Elettronica:

> *Ai fini del presente documento di lavoro una "cartella clinica elettronica" (dappresso CCE) è definita come: "Una documentazione medica completa o documentazione analoga sullo stato di salute fisico e mentale, passato e presente, di un individuo, in forma elettronica, e che consenta la pronta disponibilità di tali dati per cure mediche e altri fini strettamente collegati."*

Analogamente FSE e dossier sanitario contengono diverse informazioni inerenti allo stato di salute di un individuo relative a eventi clinici presenti e trascorsi (es.: referti, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica.

In quest'ambito i dati personali sono collegati tra loro con modalità informatiche di vario tipo che ne rendono, comunque, possibile un'agevole consultazione unitaria da parte dei diversi professionisti o organismi sanitari che prendono nel tempo in cura l'interessato.

Pertanto, traendo spunto dalla definizione di CCE, all'interno del Provvedimento a carattere generale del 16 luglio 2009, il dossier e fascicolo sanitario sono definiti nel modo seguente:

[1] *Si tratta del Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE), adottato il 15 febbraio 2007.*

Si parla di dossier sanitario:

> *"qualora tale strumento sia costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es., ospedale o clinica privata) al cui interno operino più professionisti. I dossier sanitari possono anche costituire, ad esempio, l'insieme di informazioni sanitarie detenute dai singoli titolari coinvolti in una iniziativa di Fse regionale.".*

Fig. 3 -

Mentre il fascicolo elettronico è definito come:

> *"il fascicolo formato con riferimento a dati sanitari originati da diversi titolari del trattamento operanti più frequentemente, ma non esclusivamente, in un medesimo ambito territoriale (es., azienda sanitaria, laboratorio clinico privato operanti nella medesima regione o area vasta)"*

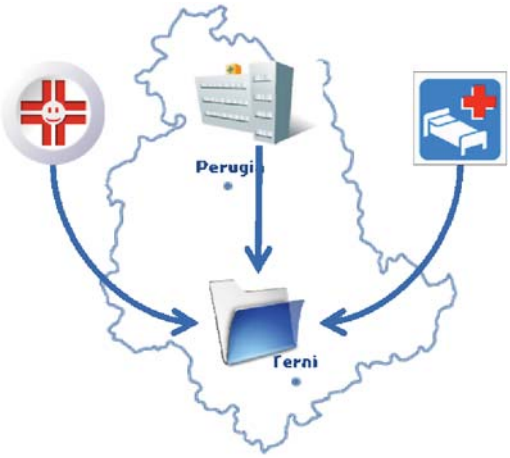


Fig. 4 -

Seppur ancora nel pieno dell'*iter* approvativo, è sicuramente d'interesse la definizione che, di FSE, viene data all'art. 15 del disegno di legge su «Sperimentazione clinica e altre disposizioni in materia sanitaria» presentato in Consiglio dei Ministri nel luglio 2010:

> *"Il fascicolo sanitario elettronico (Fse) è l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito".*

Principi applicabili al FSE

Occorre premettere che al Fascicolo sanitario elettronico si applicano tutti i principi indicati già nel codice privacy.

E' bene accennare a quei punti salienti in cui le Linee guida richiamano l'attenzione su quali informazioni trattare, per quale finalità e quali soggetti devono essere posti nelle condizioni di trattarle.

Il richiamo alle c.d. modalità di trattamento è costante nelle linee guida, ad esempio si fa riferimento al fatto che:

> *il Fse deve essere costituito preferendo, di regola, soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l'interessato..*

Facendo, in questo caso, riferimento alla necessità di non creare duplicazioni non necessarie d'informazioni sensibili.

Da non sottovalutare l'impatto di questa indicazione in termini di sicurezza dei dati, ovviando al problema di creare un centro ad hoc che coinvolgerebbe, necessariamente, un soggetto terzo (rispetto ai trattamenti svolti dalle singole strutture), e complicherebbe ulteriormente la catena di responsabilità e i possibili impatti in termini di sicurezza

Lo stesso rilievo deve essere riconosciuto all'affermazione di una misura che ricorre più volte (sia pure in termini parzialmente differenti) tanto nei provvedimenti dell'Autorità quanto nell'allegato B) del codice privacy, ovvero:

> *lla separazione delle informazioni sanitarie dai dati amministrativi*

Il Garante individua poi le finalità per cui i dati possono essere inseriti nel FSE, escludendo che gli stessi possano, ad esempio, essere utilizzati per finalità di programmazione della spesa sanitaria (estensione che, come si è accennato a proposito del disegno di legge "sanità" in lavorazione, si sta cercando di introdurre a livello di fonte primaria), e limitando, in tal modo, il trattamento alla finalità di prevenzione, diagnosi e cura dell'interessato.

Inoltre, in ossequio al principio di pertinenza non potranno essere richieste all'interessato che abbia conferito il proprio consenso, informazioni che non si rivelino necessarie al perseguimento della finalità individuata.

Altro punto che richiama l'attenzione di chi approfondisce le linee guida è, senz'altro, quello dei soggetti coinvolti nella creazione, gestione e aggiornamento del FSE.

In particolare i numerosi riferimenti alla figura del titolare devono essere letti nell'ottica dello strumento che si prende in considerazione, a seconda che si tratti di un mero dossier ovvero di un FSE.

Si prenda ad esempio, un progetto di dossier sanitario posto in essere dall'Ospedale Alfa. In esso saranno raccolte le informazioni provenienti dai diversi reparti e dai diversi specialisti dell'Ospedale medesimo, per consentire in occasione di eventi che coinvolgano la cura del paziente in quella struttura, di disporre di un compendio di informazioni che forniscano un quadro il più esauriente possibile dell'anamnesi e delle patologie afferenti al paziente stesso. In quest'ottica l'ospedale Alfa sarà individuato come titolare del trattamento.

Nel caso di un FSE, invece, in esso convergeranno informazioni sanitarie provenienti da diversi titolari coinvolti nell'iniziativa (si può trattare di titolari all'interno di una ASL, di una Regione o di una "area vasta").
Ciascun titolare manterrà le prerogative e gli obblighi che la normativa gli riconosce.

In particolare, nel rispetto dei principi di pertinenza, non eccedenza e indispensabilità del dato, occorrerà che i titolari strutturino il fascicolo in chiave "modulare" al fine di consentire una dilatazione ed una contrazione:

- dei soggetti che ad esso hanno accesso,
- delle informazioni disponibili,

dei livelli di consenso prestati. Il fatto di porre (virtualmente) nello stesso contenitore, fruibile anche direttamente dall'interessato, rappresenta il punto di convergenza con le linee guida sui referti on-line, al punto 4, recitano:

> *In alcune delle iniziative di refertazione on-line in essere, è offerto all'interessato anche un servizio aggiuntivo, solitamente gratuito, consistente nella possibilità di archiviare, presso la struttura sanitaria, tutti i referti effettuati nei laboratori della stessa. Il suddetto archivio è generalmente consultabile on-line dall'interessato, il quale può anche effettuare il download dei referti ivi raccolti. *…+*
> *Tali archivi, raccogliendo tutti i referti effettuati nel tempo dall'interessato ed essendo realizzati presso un organismo sanitario in qualità di unico titolare del trattamento (es., laboratorio di analisi, clinica privata), ricadono nella definizione di dossier sanitario, secondo quanto indicato nel richiamato Provvedimento del Garante del 16 luglio 2009, recante "Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario". Ciò stante, il titolare del trattamento che intenda offrire all'interessato la possibilità di raccogliere i referti in tali archivi deve tenere conto delle garanzie –anche di sicurezza- individuate nel citato provvedimento per i dossier sanitari.*

Sempre in merito alla messa a disposizione dei reperti, nelle linee guida viene ricordato che essa non deve far venire meno il rispetto del diritto sotteso al disposto di cui all'art. 84 del codice privacy.

In quest'ottica, l'Autorità, richiamando quanto già espresso in altre sedi, ha indicato come soluzione una modalità consistente nel garantire l'intermediazione:

> *accompagnando la messa a disposizione del reperto (inteso come il risultato dell'esame clinico o strumentale effettuato, come ad es. un'immagine radiografica, un'ecografica o un valore ematico) con un giudizio scritto e la disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato.*

Il consenso al trattamento di dati personali ed il consenso informato al trattamento sanitario: differenze ed assonanze.

Propedeutico all'introduzione del diritto di oscuramento di cui si parla diffusamente nel successivo paragrafo, risulta essere il consenso al trattamento che nelle Linee guida assume un ruolo centrale concettualmente espresso in una frase che può essere interpretata come conditio sine qua non di tutto il Provvedimento:

> *Il diritto alla costituzione o meno del FSE/dossier si deve, quindi, tradurre nella garanzia di decidere liberamente, sulla base del consenso, se acconsentire o meno alla costituzione di un documento che, come si è detto, raccoglie un'ampia storia sanitaria.*

Il consenso al trattamento, che in altri settori è sempre più spesso relegato ad un ruolo se non proprio marginale quanto meno di stanca routine, riemerge in tutta la sua forza di principio cardine: all'obbligo burocratico dell'informativa ex art. 13 si affianca come conseguenza (non sempre logica ed immediata) il diritto a scegliere dell'individuo cui deve essere garantito in modo assoluto sia il controllo delle proprie informazioni, sia se rispondere in modo positivo o negativo ad un altrui richiesta di "trattare" i suoi dati in modo parziale o totale.
Specificità ed autonomia sono i segni distintivi del consenso rinvenibile dalla lettura delle Linee guida:

> *Il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (cfr. art. 81 del Codice), deve essere autonomo e specifico*[2].

Ed ancora, più avanti, si può leggere:

> *L'inserimento delle informazioni relative ad eventi sanitari pregressi all'istituzione del Fse/dossier deve fondarsi sul consenso specifico ed informato dell'interessato, potendo quest'ultimo anche scegliere che le informazioni sanitarie pregresse che lo riguardano non siano inserite nel Fascicolo.*

Il paragrafo 8 delle Linee guida è interamente dedicato ai temi dell'informativa e del consenso.
Inizialmente viene ribadita la separatezza tra cure mediche e consenso al trattamento dei dati personali:

> *a garanzia del diritto alla costituzione o meno del Fse/dossier, l'interessato deve essere informato che il mancato consenso totale o parziale non incide sulla possibilità di accedere alle cure mediche richieste.*

[2] *Il primo comma dell'art. 81 ha rappresentato uno degli elementi di maggiore novità introdotti dal Codice Privacy in termini di semplificazione e snellimento cercando una prima e non facile della raccolta e gestione del consenso agli eccessi di burocratizzazione: Il consenso al trattamento dei dati idonei a rivelare lo stato di salute, può essere manifestato con un'unica dichiarazione, anche oralmente. In tal caso il consenso è documentato, anziché con atto scritto dell'interessato, con annotazione dell'esercente la professione sanitaria o dell'organismo sanitario pubblico, riferita al trattamento di dati effettuato da uno o più soggetti e all'informativa all'interessato, nei modi indicati negli articoli 78, 79 e 80.*

S'introduce una prima, importante e spesso non sempre chiara differenziazione tra il consenso informato da rilasciarsi in ambito sanitario ed il consenso al trattamento *strictu sensu*[3]. Tra le due formule di consenso, invero, esistono punti di contatto dei quali si dirà più esaustivamente *infra*.
Tornando all'analisi delle Linee guida si osserva che:

> *nel caso di FSE, l'informativa e la connessa manifestazione del consenso possono essere formulate distintamente per ciascuno dei titolari o, più opportunamente, in modo cumulativo.*

Se correttamente applicata tale disposizione è in linea con quanto indicato in altre situazioni analoghe e realizza un'opportuna semplificazione che, anche in base al concetto di bilanciamento d'interessi, vuole evitare ipertrofie informative ed eccessi di burocratizzazione tutti a discapito dell'effettiva e necessaria "informazione" da fornire al soggetto interessato. E ancora più avanti si può leggere:

> *L'interessato deve essere informato anche della circostanza che il Fascicolo/dossier potrebbe essere consultato, anche senza il suo consenso, ma nel rispetto dell'autorizzazione generale del Garante, qualora sia indispensabile per la salvaguardia della salute di un terzo o della collettività (art. 76 del Codice e Autorizzazione generale del Garante n. 2/2008 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale del 19 giugno 2008).*

Tale indicazione riveste particolare importanza anche alla luce del c. d principio di finalità che, in ragione delle finalità cui è destinato il trattamento, ammette che questo sia eseguito, in deroga al meccanismo del doppio livello di protezione (introdotto dalla Legge 675/96 e rappresentato dal consenso scritto + autorizzazione del Garante), in presenza anche di uno solo dei due presupposti (consenso al trattamento o autorizzazione del Garante).
Sempre dal punto di vista delle puntualizzazioni può essere letto il passaggio successivo che nulla aggiunge alle caratteristiche di completezza del binomio "informativa/consenso":

> *l'informativa deve anche mettere in luce la circostanza che il consenso alla consultazione del Fascicolo/dossier da parte di un determinato soggetto (ad es., del medico di medicina generale o del medico di reparto in cui è avvenuto il ricovero) può essere riferito anche al suo sostituto.*

Il paragrafo 8 delle Linee guida si conclude con una frase che si sofferma su due aspetti fondamentali che debbono essere contenuti nell'informativa che deve rendere note all'interessato le modalità attraverso le quali:

- *Rivolgersi al titolare per esercitare i diritti di cui agli artt. 7 e ss. del Codice,*
- Revocare il consenso all'implementazione del suo Fse/dossier o per esercitare la facoltà di oscurare alcuni eventi clinici.

[3] *Sulle differenze tra consensi si veda, tra gli altri, quanto espresso dal Comitato Nazionale di Bioetica e dal Comitato Nazionale per la Biosicurezza, le Biotecnologie e le Scienze della Vita sul tema della Raccolta di campioni biologici a fini di ricerca: vari aspetti per una corretta gestione dei dati personali e dei campioni collezionati in biobanche sono oggetto di normative sulla tutela dei dati personali, alle quali occorre fare riferimento. Per ottemperare a questa normativa è necessario inserire nei moduli di consenso informato una specifica sezione dedicata al "trattamento dei dati personali e sensibili" e chiedere un* ***consenso anche a questo specifico riguardo (che è cosa diversa dal chiedere il consenso a partecipare allo studio con o senza materiale biologico)****, corredando la nota informativa con i diritti riservati al soggetto previsti dall'art. 13 del d.lgs. 19612003.*

Esaurita la disamina sulle Linee guida e chiarite le differenze tra consenso al trattamento dei dati personali e consenso informato, appare opportuno soffermarsi sulle assonanze.
Tra questi ultimi spicca **il c.d. principio di autodeterminazione** cardine intorno al quale s'impernia il consenso informato al trattamento Sanitario.
Come affermato da alcuni commentatori, il diritto all'autodeterminazione deve essere inteso come diritto distinto e più ampio di quello del diritto alla salute e come tale tutelato a livello costituzionale sia dagli articoli 2 e 13 della Costituzione

> *In termini di libera e consapevole scelta del paziente che attiene alla sfera della sua libertà personale sia come più generico diritto alla salute, richiamato dall'art. 32, comma 2 della costituzione.*

Ed ancora sempre sul rapporto tra garanzie costituzionali e consenso informato gli autori così si esprimono:

> *Le affermazioni più inattese e più innovative, sono però quelle con cui la Corte conclude la sua ricostruzione dell'istituto del consenso informato, affermandone la «funzione di sintesi di due diritti fondamentali della persona: quello all'autodeterminazione e quello alla salute, in quanto, se è vero che ogni individuo ha il diritto di essere curato, egli ha, altresì, il diritto di ricevere le opportune informazioni in ordine alla natura e ai possibili sviluppi del percorso terapeutico cui può essere sottoposto, nonché delle eventuali terapie alternative; informazioni che devono essere le più esaurienti possibili, proprio al fine di garantire la libera e consapevole scelta da parte del paziente e, quindi, la sua stessa libertà personale, conformemente all'art. 32, secondo comma, della Costituzione».*

Detto principio, pur se non esplicitamente richiamato all'interno del Codice Privacy[4], viene citato nel *Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE). La parte terza intitolata Riflessioni su un quadro giuridico adatto per i sistemi di CCE,* esordisce con un'affermazione di portata generale:

> *Il Gruppo di lavoro Articolo 29 svilupperà in appresso gli aspetti dei sistemi di CCE per i quali delle **garanzie speciali** sembrano particolarmente necessarie per assicurare i diritti dei pazienti alla protezione dei dati. Considerato l'impatto dei sistemi di CCE e la particolare necessità di garantirne la trasparenza, sarebbe preferibile che tali garanzie venissero stabilite nell'ambito di uno speciale quadro giuridico completo (che attualmente manca sia a livello comunitario sia a livello nazionale N.d.R.).*

Tra tali garanzie spicca il Rispetto dell'autodeterminazione declinato nel documento di lavoro in una serie di punti sintetizzati nel seguito:

- **L'accettazione come garanzia** è diversa dal **consenso come base giuridica** che possa estrinsecarsi anche sotto la forma di un diritto al rifiuto (ad esempio, coma abbiamo visto, tramite l'esercizio del diritto ad oscurare alcune informazioni anche in tempi diversi).
- I dati sanitari andrebbero categorizzati al fine di utilizzarli, a seconda delle esigenze, con vari gradi di riservatezza (in linea, ad esempio, con quanto detto in termini di principio finalistico)
- Il trattamento di dati che possono essere particolarmente pregiudizievoli come dati psichiatrici, dati su un aborto, ecc. dovrebbero essere soggetti ad un consenso preventivo ed esplicito ed accessibili in modo separato (ad esempio con il ricorso alla busta sigillata).

[4] *In realtà, secondo quanto indicato nelle Linee Guida, detto principio sarebbe deducibile indirettamente dalla lettura del TITOLO V del Codice Privacy (Trattamento di Dati Personali in ambito sanitario): Il trattamento dei dati personali effettuato mediante il Fse o il dossier, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di autodeterminazione (artt. 75 e ss. del Codice).*

- Il paziente dovrebbe sempre avere la possibilità, se lo desidera, di impedire la comunicazione dei suoi dati medici, raccolti da un operatore sanitario durante la cura, ad altri operatori sanitari (diritto all'oscuramento).
- L'inserimento o meno di dati sanitari nel FSE dovrebbe essere considerata una libera scelta. Se inseriti, dovrebbero essere stabiliti precisi vincoli giuridici circa la possibilità di una loro completa cancellazione dai sistemi informativi (tale aspetto può essere disciplinato solo a livello giuridico per gli evidenti motivi di conservazione obbligatoria[5]).

A valle di questa disamina si sintetizzano, nel seguito, gli elementi base per raccogliere in maniera corretta il consenso:

- Il consenso può essere fornito solo a valle di una chiara, corretta e completa informativa. In questo senso non bastano i punti espressi nell'art. 13 ma devono essere esplicitate le ragioni della raccolta in base al contesto di riferimento del FSE che è, come visto molto ampio, secondo quel principio finalistico di cui si è detto supra.
- Il consenso deve essere prestato rigorosamente in forma scritta *"ad probationem"* a nulla valendo forme semplificate o libere (ad es. manifestazione in forma orale o annotazione della sua acquisizione da parte del personale medico secondo le indicazioni di cui all'art. 81)
- Il consenso deve essere libero, espresso e chiaro pena la sua invalidità, in ossequio al principio di autodeterminazione, fatte salve le ipotesi di differimento in situazioni di emergenza per la tutela della salute e dell'incolumità fisica o di minore età del paziente.
- Il consenso, qualora prestato, deve essere sempre revocabile, in ogni momento.

[5] *Sul punto così si esprimono le Linee guida: In caso di revoca (liberamente manifestabile) del consenso, il Fse/dossier non deve essere ulteriormente implementato. I documenti sanitari presenti devono restare disponibili per l'organismo che li ha redatti (es. informazioni relative a un ricovero utilizzabili dalla struttura di degenza) e per eventuali conservazioni per obbligo di legge, ma non devono essere più condivisi da parte degli altri organismi o professionisti che curino l'interessato (art. 22, comma 5, del Codice).*

L'Analisi del concetto di oscuramento

Il capitolo 3 *("Diritto alla costituzione di un Fascicolo sanitario elettronico e di un dossier sanitario")* apre la seconda parte delle Linee guida dedicata alle Garanzie per l'interessato, introducendo il c.d. diritto all'oscuramento.

Preliminarmente si osserva come tale diritto, pur se non direttamente disciplinato all'interno del Codice Privacy, può essere considerato, a tutti gli effetti, sinonimo, in termini evolutivi, del diritto all'anonimato rinvenibile nel Codice Privacy in più parti:

- Art. 3 *(Principio di necessità nel trattamento dei dati)* introduce il concetto di anonimato laddove afferma che, pena l'illiceità del trattamento, i dati dove non diversamente possibile, debbano essere utilizzati in forma anonima, o comunque anonimizzabili[6]. Il limite all'identificabilità dell'interessato deve quindi essere inteso sia con riferimento a casi in cui il dato si presenti come nominativo sia nei casi in cui l'identificazione possa avvenire indirettamente attraverso il collegamento tra più informazioni combinato tra loro (c. d. concetto di pseudoanimizzazione)
- Art. 4, comma 1 lett. n) il dato anonimo è definito come *"il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile".*
- Art. 7 comma 3 lettera b), in tema di diritti dell'interessato che stabilisce come l'interessato ha diritto di ottenere, tra l'altro, "la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati".
- Art. 22 comma 3 che afferma come i soggetti pubblici possano "trattare solo i dati sensibili e giudiziari indispensabili per svolgere attività istituzionali che non possono essere adempiute, caso per caso, mediante il trattamento di dati anonimi o di dati personali di natura diversa".

Sempre sul diritto/necessità di utilizzo di dati anonimi, così si esprime *il Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE):*

> *qualora fattibile e possibile, i dati dei sistemi di CCE dovrebbero essere usati per altri scopi (ad es. statistiche o valutazione della qualità) solo in forma anonima, o come minimo usando una pseudonimizzazione sicura.*

Lo stesso Garante, in due distinti provvedimenti, ha richiamato, fin dal 2007, i principi di anonimizzazione (e di pseudo anonimizzazione):

- In materia di sperimentazioni cliniche
- In materia di trattamento di dati genetici

Passando all'analisi del contenuto delle Linee guida, il concetto di oscuramento è riportato, inizialmente, in forma solo embrionale:

> *Ferma restando l'indubbia utilità di un Fse/dossier completo, deve essere garantita la possibilità di non far confluire in esso alcune informazioni sanitarie relative a singoli eventi clinici (ad es., con riferimento all'esito di una specifica visita specialistica o alla prescrizione di un farmaco).*

[6] *Il concetto di dato anonimo va correlato all'utilizzo di sistemi informatici.*

L'estensore delle Linee Guida introduce due elementi apparentemente in contrasto:

- Per essere effettivamente utile, l'FSE/dossier sanitario dovrebbe essere completo ed esaustivo. Il modello di sanità elettronica (o c.d. *e-health*), infatti, nasce con lo scopo dichiarato di raccogliere, sistematizzare e rendere fruibili in ogni momento e a più soggetti, anche contemporaneamente, informazioni altrimenti frammentate o di difficile reperibilità. Tale modello s'inserisce nella scia di altre iniziative tese a migliorare il rapporto tra cittadino e Pubblica Amministrazione utilizzando canali di comunicazione tecnologicamente evoluti (si pensi all' *e-government* in termini di PEC, Archiviazione sostitutiva, Protocollo informatico, processo telematico, ecc.).
- Pur nella sua indubbia "utilità sociale", il FSE/dossier sanitario deve presentare elevati livelli di garanzia per l'individuo tutelando in maniera rigorosa la sua possibilità di scegliere, liberamente ed in maniera consapevole, quali informazioni inserire tenuto conto della delicatezza delle stesse, che come più volte affermato in dottrina, rappresentano il "nocciolo duro" dei dati personali[7].

Oltre a quanto si è detto supra in tema di consenso, libero, espresso con piena coscienza e a valle di un'adeguata informativa, l'altro elemento di tutela è rappresentato da quel "diritto ad oscurare" tutte quelle informazioni relative alla vita sanitaria che,

> *analogamente a quanto avviene nel rapporto paziente-medico curante, nel quale il primo può addivenire a una determinazione consapevole di non informare il secondo di certi eventi,*

il Garante ha voluto porre a baluardo difensivo dalle altrui intrusioni alla sfera di intimità e privatezza di ciascun individuo.

Le linee guida forniscono una prima definizione di oscuramento che, nello sforzo di sintesi compiuto dall'estensore, non rende giustizia alla loro complessità:

> *L'oscuramento dell'evento clinico (revocabile nel tempo) deve peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").*

Da questa frase si possono evincere le seguenti conseguenze, in termini di gestione e sistematizzazione delle informazioni che confluiranno nel FSE:

- La possibilità di oscurare le informazioni va riferita ad ogni singolo evento clinico (ad. es. visite specialistiche, analisi/indagine diagnostiche, cure farmacologiche, interventi in day hospital, ricoveri ospedalieri) sia passato che in corso.

---

[7] Tra i primi ad utilizzare questa definizione è stato Giuseppe Santaniello (già membro del Garante per la protezione dei dati personali) che in suo scritto del 2004 così si esprimeva: Va ricordato come la nozione di "diritto alla riservatezza" sia molto ampia, sì da presentarsi come un diritto a consistenza concentrica, al cui centro si colloca la categoria dei dati sensibili, che costituiscono il nocciolo duro del diritto alla privacy. Tale figura geometrica comporta una variabilità della tutela offerta a seconda del contenuto dei dati; per cui un regime di assoluta riservatezza è configurato solo con riferimento ai dati sensibili, mentre è graduale negli altri casi in cui non sussistano dati di tale natura.

- Per ogni singolo evento clinico deve essere prevista la possibilità di rendere reversibile la propria espressione di volontà trasformando un'iniziale negazione in una successiva concessione a trattare certe informazioni. Tale previsione deve valere anche per il processo contrario.
- L'accesso al FSE deve essere concesso solo a soggetti autorizzati (e quindi identificati preventivamente) dal Titolare (ad es. medico di medicina generale, pediatra di libera scelta, farmacista, medico ospedaliero specialista, senza contare il personale paramedico o familiari e parenti che possono avere necessità di conoscere le informazioni contenute). Stabilito il chi accede al FSE, Il Titolare deve anche indicare a quali informazioni è possibile accedere da parte dei singoli soggetti.
- Per ciascun soggetto abilitato ad accedere al FSE si deve prevedere la possibilità di escluderlo dal conoscere se il paziente/interessato, che ha esercitato il diritto ad oscurare alcuni suoi dati sanitari, abbia o meno esercitato tale facoltà.
- La facoltà di negare tale conoscenza, *(c.d. oscuramento dell'oscuramento),* deve essere resa possibile non solo per un tempo determinato *(temporaneamente)* ma in modo tale da evitare ogni automatismo *(automaticamente)*.

Stanti le conseguenze in termini di responsabilità civile e penale[8] per il Titolare, che possono discendere da un'errata interpretazione ed applicazione di questo passaggio, nel successivo capoverso il Garante fornisce un *esempio di esercizio della facoltà di oscuramento*, illustrando, in via del tutto generica, una soluzione di tipo tecnico consistente:

in una *"busta elettronica sigillata" non visibile, apribile di volta in volta solo con la collaborazione dell'interessato, ovvero utilizzando codici casuali relativi a singoli eventi che non consentono di collegare tra loro alcune informazioni contrassegnate*[9].

Ancora nelle successive righe del capitolo, il Garante tenta di specificare meglio il concetto con una serie di precisazioni che, come in questo caso, appaiono, se non superflue, lapalissiane:

> *Resta ferma la possibilità per il titolare del trattamento di informare i soggetti abilitati ad accedere a tali strumenti (medici et altri) che tutti i fascicoli o i dossier cui hanno accesso possono non essere completi, in quanto l'interessato potrebbe aver esercitato il suddetto diritto di oscuramento.*

[8] *Appare utile osservare come tutta la documentazione medica che può confluire nel FSE, abbia natura, come riconosciuto da costante giurisprudenza della Cassazione, di atto pubblico (Atto pubblico di fede privilegiata, ossia atto redatto dal medico pubblico ufficiale – nell'esercizio di una potestà di certificazione ed attestazione conferita dalla legge ed in conformità ai singoli regolamenti interni) con tutte le conseguenze civili e penali che possono scaturire (art. 328 c.p. Omissione in atti d'ufficio: ritardo o mancata compilazione della cartella, artt. 481 e 482 c.p. falso ideologico e materiale, 326 c.p. violazione del segreto d'ufficio, art. 622 c.p. Violazione del segreto professionale).*

[9] *Sul concetto di busta sigillata è utile quanto indicato nell'Informativa rilasciata dalla Regione Lombardia nell'ambito del progetto CRS – SISS (Carta Regionale dei Servizi - Sistema Informativo Socio-Sanitario).*

Ma è il successivo passaggio che spicca per importanza e rappresenta un punto chiave nella lettura e interpretazione del concetto di oscuramento:

> *nulla osta, inoltre, che il titolare del trattamento possa prevedere che l'interessato eserciti tale facoltà in presenza del medico che ha eseguito la prestazione sanitaria, affinché quest'ultimo gli possa illustrare le conseguenze, da un punto di vista clinico, di tale scelta.*

Al diritto a vedere tutelata la propria riservatezza (secondo alcuni commentatori "in modo assolutistico") le linee guida prevedono l'interesse opposto dell'organismo sanitario ad ottenere informazioni complete, esaustive e veritiere della storia anamnestica del paziente/interessato, pena il rischio concreto della perdita al diritto alla salute ponendo particolare enfasi sul corretto e coerente rapporto tra medico e paziente che deve essere alla base di qualsiasi percorso di cura e prevenzione.

Le linee guida esauriscono la trattazione dell'oscuramento con altre due affermazioni che nulla aggiungono a quanto detto prima:

> *Il titolare del trattamento che intenda istituire il Fse/dossier anche con informazioni sanitarie relative a eventi clinici precedenti alla sua costituzione (es. referti relativi a prestazioni mediche pregresse) deve essere autorizzato preventivamente dall'interessato, lasciando libero quest'ultimo di esercitare la facoltà di "oscuramento".*
> *In ogni caso, sia con riferimento alle informazioni sanitarie pregresse che a quelle attuali, il titolare del trattamento deve assicurare all'interessato di poter esercitare il diritto di oscuramento sia prima dell'inserimento delle informazioni sanitarie che successivamente.*

Accesso ai dati contenuti nel fascicolo

Nel nostro quadro normativo tra i diritti dell'interessato trova fondamentale collocazione l'accesso ai dati personali, in assenza del quale vengono "pregiudicate" diverse facoltà che ad esso sono subordinate.

Occorre precisare che il diritto di accesso si riferisce ai dati personali dell'interessato e per azionare questo diritto, come regolato dall'art. 7, non si possono addurre motivazioni diverse da quelle di tutela dei propri dati personali.

Per esempio

> *Non è accoglibile la richiesta di ottenere dal datore di lavoro l'accesso alle note di qualifica concernenti altri lavoratori.*

Allo stesso modo:

> *Non può considerarsi valido esercizio del diritto di accesso (ex art. 7 del codice privacy) una richiesta inoltrata al titolare o al responsabile del trattamento volta a raccogliere elementi di prova a fini investigativi ai sensi dell'art. 38 delle disp.Att. al c.p.p.*

Occorre tenere ben presente l'omnicomprensività del diritto d'accesso in quanto ha profondi legami con l'eventuale "indisponibilità" del dato.

In effetti, riguardando la fattispecie normativa dettata dall'art. 7,

> *Il diritto di accesso assume i contorni di posizione servente rispetto al potere di incidere sul trattamento dei dati, il cui esercizio sostanzia il contenuto forte della tutela apprestata dal Codice.*

Naturalmente la sfera costituita dal diritto d'accesso è limitata da più parti.

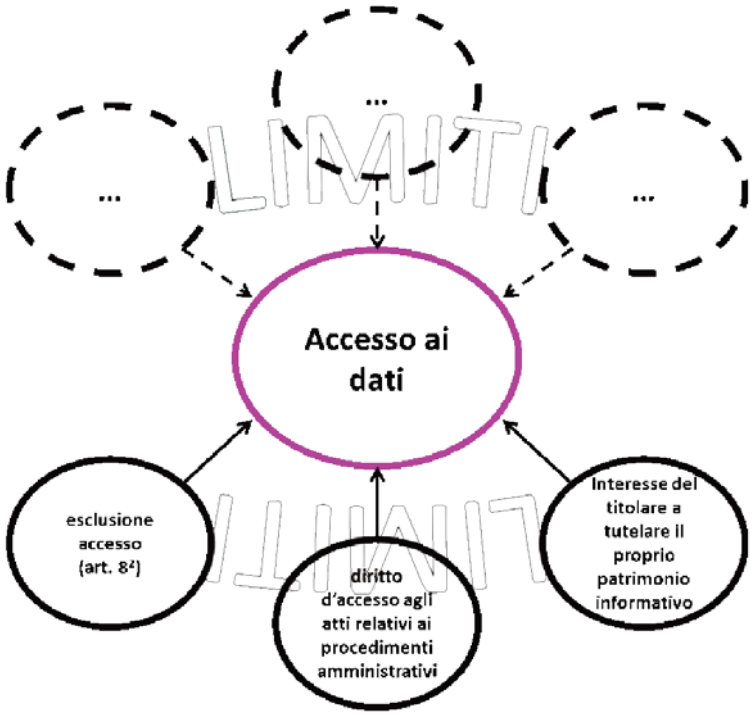


Fig. 5 -

- Il diritto d'accesso vede il primo limite, nell'art. 8, comma 2, i casi nei quali i diritti di cui all'articolo 7 non possono essere esercitati con richiesta al titolare o al responsabile o con ricorso ai sensi dell'articolo 145.
- Una seconda limitazione è individuabile nel fatto che, il contenuto informativo dell'accesso deve essere correlato all'interesse del titolare a non rendere disponibili le informazioni non riferibili direttamente all'interessato e che appartengano a terzi ovvero al "patrimonio" del titolare medesimo.

  Il potere attribuito al Garante per la protezione dei dati personali è finalizzato al perseguimento dell'interesse pubblico di conservare un equilibrio economico, contemperando l'interesse di coloro che hanno titolo ad esercitare il diritto di accesso con quello dei titolari del trattamento dei dati in modo da evitare, da un lato, cheun'eccessiva lievitazione dei contributi possa di fatto impedire l'esercizio del diritto e, dall'altro, che il diritto di accesso si traduca in un insopportabile peso economico

- Altro limite è quello che si contrappone al diritto di accesso ai dati personali, è dato dal diritto d'accesso agli atti relativi ai procedimenti amministrativi. L'art 59 del codice privacy rinvia alla legge 241 del 1990 (che ha subito importanti modifiche nel 2005) il compito di individuare presupposti, modalità e limiti per l'esercizio del diritto d'accesso a documenti amministrativi contenenti dati personali, conferendo alle attività finalizzate all'applicazione di tale disciplina il connotato di rilevante interesse pubblico.

Primariamente emerge quanto differenti nella natura stessa siano questi due diritti, atteso che l'uno persegue la propria finalità di controllo dei dati personali e l'altro persegue lo scopo di valutare attraverso il peculiare carattere della trasparenza, la correttezza del procedimento amministrativo ovvero difendere i propri "interessi giuridicamente rilevanti".

A questo proposito si pone in tutta la sua complessità la difficoltà di teorizzare una regola univoca che indichi, di volta in volta, il diritto prevalente.

Sul tema si sono articolati molti orientamenti tra loro anche contraddittori.

Con il tempo e soprattutto con l'introduzione del codice privacy da un lato e delle modifiche apportate alla legge 241 del 1990, dall'art. 16 della legge 15 del 2005, dall'altro, è invalso l'orientamento di tutelare la riservatezza attraverso una puntuale verifica, caso per caso, dell'effettiva necessità dell'accesso in chiave di tutela di un interesse giuridicamente rilevante per cui, ove tale condizione sussista in concreto, la riservatezza dei terzi non può costituire ostacolo all'esigenza di piena difesa dei propri diritti da parte dei cittadini e delle imprese che, a tal fine, necessitano di accedere alla documentazione amministrativa detenuta dall'ente.

Trattando, in questa sede, di dati "sanitari", il quadro normativo non sarebbe completo se non si riportasse, a proposito dell'accesso, quanto disposto dall'art. 60 (Dati idonei a rivelare lo stato di salute e la vita sessuale) del decreto legislativo 30 giugno 2003, n. 196:

Quando il trattamento concerne dati idonei a rivelare lo stato di salute o la vita sessuale, il trattamento è consentito se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso ai documenti amministrativi è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

I limiti che sono stati illustrati servono a capire quanto complesso possa essere per la struttura sanitaria, valutare:

- se il "presunto" interessato sia legittimato ad inoltrare richiesta d'accesso ovvero
- se il diritto del richiedente sia meritevole di tutela o di rango almeno pari a quello della protezione dei dati.

Tra i motivi che hanno spinto il Garante ad adottare le linee guida, trova spazio la necessità di fornire approcci "dirimenti" nel caso di ricorrenza di talune situazioni che in passato sono state oggetto di specifici pronunciamenti. Nell'occasione il Garante ha chiarito che, in alcuni casi l'ente che aveva ricevuto la richiesta di ostensione aveva addotto motivi non fondati per negare l'accesso medesimo.

Si pensi al provvedimento del 25 settembre 2008, in quell'occasione l'Autorità, accogliendo il ricorso dell'interessato, ha "bacchettato" gli Ospedali riuniti di Bergamo poiché avevano negato al richiedente l'accesso ai dati personali.

Il richiedente aveva esercitato il diritto d'accesso relativamente ai dati della sorella deceduta.

Nel frangente il Garante ha chiarito che si trattava del tipico caso in cui il ricorrente era legittimato ad accedere ai sensi dell'art. 9, comma 3, del Codice. Mentre non era fondata la contestazione degli Ospedali riuniti di Bergamo in cui si richiedeva di giustificare, in modo documentato, la sussistenza dei presupposti dalla norma indicati (il riferimento era all'art. 92 del codice), con particolare riferimento all'esistenza "di un diritto di rango pari a quello dell'interessato".

In quell'occasione, l'Autorità precisò che non si trattava di alcuno dei casi previsti dall'art. 92, comma 2. In questo articolo si fa riferimento a persone "diverse" dall'interessato, situazione nella quale è coerente procedere ad una valutazione secondo il criterio del "pari rango".

Altro provvedimento che aiuta a chiarire il comportamento che gli operatori sanitari dovranno tenere anche nel caso di richieste d'accesso al fascicolo sanitario elettronico, risale a circa un anno dopo, il 17 settembre 2009, questa volta ad esercitare i diritti dell'interessato non era un soggetto legato in linea collaterale alla persona deceduta, bensì il convivente.

Ancora una volta il Garante precisa come un legame, documentato, quale quello della convivenza sia tale da porre il convivente (in veste di richiedente prima e di ricorrente poi) nella posizione regolata dall'art. 9, comma 3, e non in quella prevista dall'art. 92 che avrebbe richiesto (al richiedente/ricorrente) di giustificare eventuali istanze rivolte a prender visione o ad ottenere il rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera, documentando la necessità:

- di far valere o difendere un diritto in sede giudiziaria ai sensi dell'articolo 26, comma 4, lettera c), di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

- di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

Se ne deduce che in caso di richiesta di accesso ai dati personali, la struttura si trovi dinnanzi ad un bivio dettato dal fatto di cogliere primariamente se il richiedente sia: l'interessato, un suo rappresentante (dotato di delega o procura), ovvero, in caso di persone decedute, un soggetto che abbia un interesse proprio, o agisca a tutela dell'interessato o per ragioni familiari meritevoli di protezione. Non essendo necessaria, in questo caso, la dimostrazione richiesta dall'art. 92 e il conseguente ricorso al criterio del "pari rango".

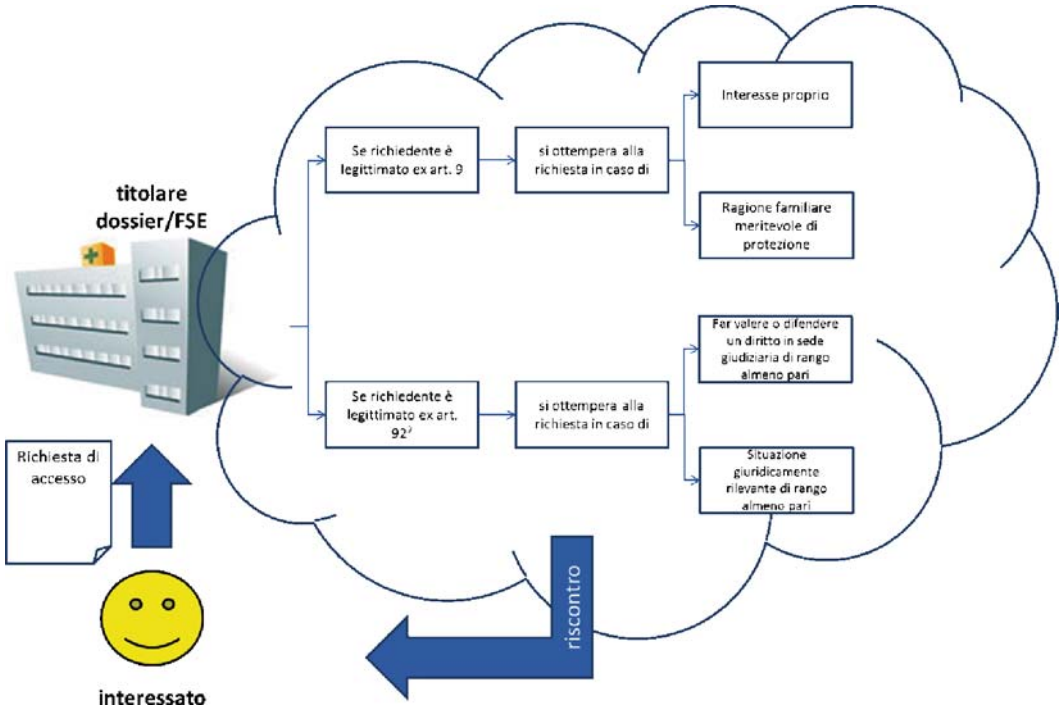


Fig. 6 -

Conseguenze e ricadute per il mancato accesso ai dati presenti nel FSE (RA) – Disponibilità dei dati contenuti nel fasciolo sanitario elettronico

Spesso ci si interroga sulla natura facoltativa o obbligatoria dell'adozione del dossier e del FSE, oppure intorno al fatto se l'adozione di queste soluzioni rappresenti un diritto del cittadino. In particolare due domande sono ricorrenti e ad esse, in questo paragrafo, cerchiamo di dare una risposta.

1. La costituzione del FSE è obbligatoria?
2. Cosa accade quando un cittadino che ha aderito ad un FSE vede tutti i vantaggi derivanti dalla condivisione delle informazioni, frustrati da problemi tecnici ovvero da temporanea indisponibilità del FSE?

Alla prima domanda è stata data una risposta già nelle linee guida del Garante, allorquando si afferma che

> *allo stato delle notizie al momento acquisite dall'Autorità, non consta l'esistenza di una norma che obblighi gli organismi sanitari a costituire un Fse o un dossier, la cui introduzione deve ritenersi, pertanto, facoltativa.*

Il secondo interrogativo ha una risposta tutt'altro che scontata, infatti la "facoltatività" dell'adozione di un sistema di FSE può indurre la struttura ad un approccio per così dire sperimentale, almeno nel periodo iniziale del "progetto".

Tuttavia a fronte della facoltatività dell'adozione di un FSE il consenso dell'interessato innesca un meccanismo a catena che porta, secondo chi scrive, ad un affidamento nell'efficienza del trattamento sotteso al FSE cui l'interessato ha accordato il consenso.

Lungi dal poter, in questa sede, approfondire i possibili impatti in tema di "responsabilità contrattuale" in caso di mancata disponibilità del FSE, sembra evidente che, almeno in astratto, l'indisponibilità delle informazioni contenute nel FSE possa comportare l'integrazione, da parte della struttura titolare del trattamento, della responsabilità ex art. 15 del codice privacy, sia per danni cagionati per effetto del trattamento sia per il mancato accesso ai propri dati personali da parte dell'interessato o da parte di un suo rappresentante.

Talvolta è stato contestato il fatto che il mancato accesso ai dati personali possa integrare il profilo di responsabilità di cui all'art. 15 del codice privacy, tuttavia questo limite sembra, allo stato, superato in quanto secondo autorevole dottrina i diritti di cui all'art. 7 sono strumento di tutela dei diritti della personalità enunciati all'art. 2 del codice privacy e questi ultimi

> *Sono presenti in maniera immanente e quindi costante. "Stare sullo sfondo" significa, in termini giuridici, che essi sono predefiniti dall'ordinamento e che questo appresta ad essi una tutela di carattere oggettivo, che solo in parte viene rimessa al potere del soggetto dei cui dati personali si tratta.*

In questi termini si sostanzia il legame tra i diritti dell'interessato (tra cui l'accesso ai dati personali) e l'art. 15 del codice privacy (danni cagionati per effetto del trattamento).

In tema di individuazione dei danni, atteso che accanto a quelli patrimoniali viene riconosciuto il diritto al risarcimento di quelli morali, il mancato accesso può implicare il fatto che il cittadino o chi sia stato autorizzato all'accesso, agisca ignorando alcune delle informazioni necessarie a costituire un libero convincimento, questo può avere ripercussioni in termini: di scelte mancate, di maggiori oneri so-

stenuti, di conseguenze esistenziali talvolta tragiche. Naturalmente se la perdita di un guadagno ed in genere i danni patrimoniali sono relativamente semplici da provare, discorso totalmente differente si presenta nel caso il "danno" subito abbia natura, per così dire, impalpabile. In questa seconda tipologia di danni (così come nell'ambito dei danni esistenziali) l'attribuzione dell'onere della prova e la sua inversione, giocano un ruolo determinante.

In sostanza l'interessato dovrà dimostrare il danno subito (fatto peraltro piuttosto agevole in ambito sanitario rispetto a settori dove il possibile danno è di difficile quantificazione) mentre la struttura dovrà dimostrare: l'adozione di idonee misure di sicurezza (anche in termini di business continuity) e l'irrilevanza della mancata disponibilità del dato, rispetto al pregiudizio subito dall'interessato.

All'atto pratico occorre sottolineare che esistono numerosi strumenti affinchè i soggetti che istituiscono il FSE si pongano al riparo dalle conseguenze testè paventate, e buona parte di questa "difesa" trova collocazione nelle aspettative che vengono date all'interessato al momento dell'adesione al FSE.

Ad esempio, l'informativa relativa al FSE proposto dalla Regione Lombardia, al punto 5 (finalità), indica che questo ha

> *La finalità di fornire ai medici operanti nel territorio lombardo uno strumento ulteriore e coadiuvante per la prevenzione, la diagnosi, la terapia e l'assistenza dei cittadini.*

Naturalmente oltre a fornire un'informativa corretta e aderente al trattamento operato, il proposito espresso nelle finalità dell'Informativa "lombarda" è anche motivato dal fatto che, allo stato attuale, il fascicolo è uno strumento necessariamente "ulteriore", in particolare per due ragioni:

- sia perchè la sua adozione è facoltativa;
- sia perchè - per il diritto all'oscuramento (all'oscuramento dell'oscuramento) e per la facoltatività dell'inserimento di informazioni pregresse - è uno strumento potenzialmente (direi, anche, probabilmente) incompleto.

La Misura di Sicurezza nell'ambito del "provvedimento": il ruolo delle autorità indipendenti e la gerarchia delle fonti

Un recente intervento del Gruppo di Lavoro ex art. 29 in ambito comunitario intitolato *"Parere sul principio di responsabilità"*[10], definisce una serie di azioni che consentano, a ciascun Titolare del trattamento,

> *di determinare le misure concrete da applicare in funzione dei rischi connessi al trattamento e dei tipi di dati trattati.*

Per quel che concerne la Sanità elettronica così, si esprime il documento:

> *la quantità sempre crescente di dati personali è accompagnata da un aumento del loro valore in termini sociali, politici ed economici. In alcuni settori, soprattutto in ambiente online, i dati personali sono diventati de facto la valuta di scambio per i contenuti online. Nel contempo, da un punto di vista sociale, vi è un crescente riconoscimento della protezione dei dati come valore sociale. In sintesi, via via che i dati personali diventano sempre più preziosi per i responsabili del trattamento in tutti i settori, anche i cittadini, i consumatori e la società in generale sono sempre più consapevoli della loro rilevanza. Questo fatto rafforza a sua volta la necessità di applicare misure rigorose per salvaguardarli.*

Più avanti sempre sul tema sanità on line si può leggere: i grandi responsabili del trattamento (In Italia i Titolari del trattamento, N.d.R.)

> *dovrebbero attuare misure rigorose per esempio se sono impegnati in operazioni rischiose di trattamento dei dati, come alcune operazioni nel quadro dei servizi sanitari online. Un ente locale od un'organizzazione la cui attività principale sia il trattamento dei dati (come nel caso delle strutture sanitarie N.d.R.) richiederebbero tutti misure specifiche, al fine di garantire una governance credibile ed efficace delle informazioni (attraverso, ad esempio, le note informative utilizzate, la descrizione delle misure di sicurezza di base, ecc.).*

Da questa premessa si intuisce l'importanza della misura di sicurezza che, sottratta dall'alveo del mero adempimento burocratico - "minimo" - cui è stata relegata da frettolose letture del Disciplinare Tecnico, ritrova centralità e rinnovata importanza nella forma giuridica del Provvedimento ex art. 154, emanato dal Garante per la Protezione dei dati personali.

Su quest'ultimo aspetto appare utile fare alcune considerazioni:

- Qual è il ruolo, i compiti e la funzione di garanzia delle Autorità indipendenti nel nostro ordinamento
- Quale valore giuridico attribuire al provvedimento nel contesto della gerarchia delle fonti

Riguardo al primo aspetto si osserva che l'Autorità Garante per la protezione dei dati personali rientra nel novero delle c.d. Autorità indipendenti e come tale:

- E' dotata di poteri autonomi che trascendono la semplice amministrazione (ad esempio, il potere di autoregolamentarsi e di emanare norme a valore giuridico);
- Non è subordinata gerarchicamente né politicamente ai Ministeri, quindi sono del tutto indipendenti rispetto a qualsiasi ingerenza ministeriale (gli unici corpi da sempre dotati di indipendenza dall'apparato di Governo sono solo quelli giurisdizionali);

[10] *Si veda il documento pubblicato alla URL:http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_it.pdf*

- Agisce in un settore specifico sul quale lo Stato ha delegato le competenze (cosi vale anche per altri settori quali il radiotelevisivo, mercato e della concorrenza, servizi pubblici essenziali, ecc.)
- E' caratterizzata, dal punto di vista del processo amministrativo, da un pro*cedimento accelerato previsto nella Legge n. 205/2000 "qualora si tratti di ricorsi avverso atti delle autorità amministrative indipendenti"*.
- Svolge un ruolo di c.d. "quarta funzione" che l'ordinamento giuridico italiano gli riconosce affiancando le tradizionali potestà legislativa, governativa e giurisdizionale.

Per quanto concerne il secondo aspetto, si osserva come negli ultimi anni la Privacy abbia subito un profondo mutamento: constatata l'impossibilità di un controllo capillare e di una verifica a "priori" sull'effettivo grado di applicazione dei principi generali richiesti dal Codice, il Garante si è affidato in maniera sempre più massiva al "Provvedimento" quale strumento privilegiato attraverso cui, a seconda dei casi e delle situazioni, vietare, autorizzare o prescrivere un certo comportamento.

In particolare i Provvedimenti possono avere:

- *Natura prescrittiva* (art.154, comma 1, lett. c), con i quali si invoca non solo un generico obbligo di rispetto della Legge (ad esempio, l'applicazione dei principi di cui agli artt. 3 e 11) ma, a seguito di verifiche ispettive o ricorsi, si fissano comportamenti, misure di sicurezza e adempimenti che i soggetti destinatari del provvedimento sono tenuti ad adottare per non incorrere in sanzioni di carattere civile/penale previste dal Codice.[11]
- *Natura inibitoria* (art. 154 comma 1, lett.d) con i quali, a seconda dei casi, sono indicati divieti del trattamento, blocco del trattamento, adozione in via residuale di tutti i provvedimenti previsti dalla disciplina in materia di trattamento. Questo tipo di provvedimenti sono adottati quando vi è un rischio di pregiudizio rilevante per uno o più interessati e si configuri la necessità di un urgente intervento[12].
- *Natura informativa o promozionale* (art. 154, comma 1, lett.h). attraverso i quali il garante cura la conoscenza della disciplina in materia di trattamento dei dati personali e delle relative finalità, nonché delle misure di sicurezza dei dati richiamando i Titolari del trattamento alla necessità diadottare idonee cautele volte a prevenire e ad accertare eventuali accessi non consentiti ai dati personali.[13].

[11] Hanno natura prescrittiva, tra gli altri, il Provvedimento sugli Amministratori di sistema, sulle intercettazioni telefoniche, sul Direct Marketing, ecc.

[12] Tra gli ultimi provvedimenti emessi in questo senso, si veda quello riguardante Google Street View per le comunicazioni captate su reti wi-fi.

[13] Rientrano in questa fattispecie oltre al Provvedimento in commento anche quello riguardante i Rifiuti di apparecchiature elettriche ed elettroniche (RAEE).

Appurata la natura dell'Autorità e il suo agire in posizione di neutralità e di imparzialità rispetto agli interessi pubblici e privati in gioco si può, in conclusione, affermare che:

- Gli interventi in uno specifico settore come quello della protezione dei dati personali sono oggetto di delega legislativa ad un soggetto giuridico dotato di competenze specifiche (il Garante privacy)
- Il Garante è messo in condizione di esprimere compiutamente le proprie posizioni anche per il tramite di apposita produzione normativa avente funzione regolamentare (che è rappresentata a tutti gli effetti dai Provvedimenti di cui all'art. 154) e di risoluzione dei contrasti (regolata dagli artt. 141 -151 del Codice)
- Con la forma del provvedimento il Garante esprime, secondo i casi, o una posizione che sfocia in oneri obbligatori per il destinatario o un modus operandi cui è consigliabile conformarsi sopratutto nel caso in cui siano previste misure di sicurezza di tipo specialistico, la cui mancata applicazione può sfociare in illeciti oltre che di natura penale (ex art. 169) anche di tipo civile (è il caso di cui all'art. 2050 c.c.).
- La portata dei provvedimenti può essere di carattere generale (come nel caso del provvedimento sugli amministratori di sistema) o specifico (i destinatari sono soggetti che operano in uno certo settore come nel caso del FSE/Dossier sanitario).
- La gerarchia delle fonti è rispettata in ragione della natura precipua dell'Autorità, del limitato settore in cui è chiamata ad intervenire e del rigoroso rispetto dei principi di imparzialità e di qualità democratica della loro azione (si veda a tal proposito il c.d. modello regolativo giustiziale che ha ricevuto una consacrazione, a livello di principio, da due Leggi la L. 62/2005 e la L. 262/2005).

I dati del Fascicolo Sanitario Elettronico

Con la progressiva affermazione di nuovi modelli assistenziali, come ad esempio la continuità di cura, e l'evoluzione delle tecnologie ICT che rendono oggi possibile la sanità elettronica, la gestione dei **dati clinici** è diventata una delle maggiori priorità.

In aggiunta ai tradizionali ambiti ospedalieri ed ambulatoriali (specialisti e medici di medicina generale), cui si rivolge la cartella clinica elettronica locale, denominata Electronic Medical Record (EMR) o Electronic Patient Record (EPR), si è sviluppato negli ultimi anni il concetto di **Electronic Health Record (EHR)** o, in italiano, **Fascicolo Sanitario Personale (FaSP)** nell'accezione del Ministero della Salute (mattone Patient File del NSIS) o Fascicolo Sanitario Elettronico (FSE) in quella del Tavolo di Sanità Elettronica guidato dal Dipartimento dell'Innovazione Tecnologica.

In teoria le due tipologie di cartelle differiscono per l'ambito cui si riferiscono, dal momento che la prima documenta un episodio di cura (ad esempio un ricovero, un day hospital o un accesso ambulatoriale), mentre la seconda raccoglie tutte le principali informazioni cliniche del paziente nel corso della sua vita.

Al momento il FSE è concepito come uno strumento di consultazione e non un'infrastruttura per l'interoperabilità tra le applicazioni. Un forte freno a questo possibile sviluppo è dato dai vincoli imposti dal rispetto dalla privacy e da molteplici aspetti di ordine legale. Più che un problema tecnologico, oggi superabile senza grandi problemi, l'interoperabilità in sanità richiede un notevole sforzo per superare i tradizionali modelli organizzativi e considerare l'informazione clinica con nuove logiche.

L'obiettivo di questo capitolo è una classificazione, che non ha la pretesa di essere esauriente, delle varie tipologie di dati che potrebbero essere incluse nel FSE. Ci sono informazioni che provengono da sistemi informativi e, quindi, probabilmente già memorizzati e strutturati nel database, oppure provenienti da reparti/processi non automatizzati e, quindi, raccolti in documenti "office" e conservati su file system locali o condivisi. Si devono, quindi, considerare i dati che provengono dalle macchine (tipicamente di diagnostica), con formati che possono essere eterogenei. Vi sono, infine, quei dati che il cittadino/paziente fornisce autonomamente e consapevolmente con l'intenzione di arricchire il proprio Fascicolo sanitario.

Indipendentemente dalla tipologia dei dati presenti all'interno della struttura sanitaria, siano questi dati strutturati o meno, è possibile proteggerli con adeguate tecnologie di cifratura e regolamentazione degli accessi, come pure tracciarne l'utilizzo nel tempo. Tali metodiche di protezione sono applicabili, con tecnologie diverse, a tutte le tipologie di dati che si trovano all'interno della struttura sanitaria e che possono, quindi, essere utilizzate nel FSE. Tali soluzioni sono 'impostabili' sia a livello applicativo che infrastrutturale, permettendo l'impiego del livello di protezione più adeguato.

4.1 Le tipologie dei dati

Le informazioni presenti nel FSE possono essere classificate in base a criteri funzionali. Un esempio è la catalogazione dei dati sulla base di documenti clinici ed eventi sanitari.

Esempi di Documenti Clinici ed Eventi Sanitari

- Anagrafiche (MMG, PDF, Strutture Sanitarie)
- Prescrizioni (Farmaceutiche, Specialistiche, Ricoveri)
- Prenotazioni
- Referti (Ambulatorio, Laboratori, Radiologia, Specialistici)
- Lettere Dimissioni
- Scheda di Accesso
- Scheda di dimissione Ospedaliera
- Verbali Pronto Soccorso-Day Hospital
- Certificati Medici
- Pronto Soccorso
- Patient Summary (Scheda Sanitaria Individuale)
- Scheda delle Vaccinazioni
- Scheda di Patologia
- Piano terapeutico
- Verbale di contatto telefonico
- Verbale di Follow-up

All'interno di queste macro categorie possiamo individuare le seguenti tipologie di dati:

- malattie infettive e diffusive
- vaccinazioni
- programmi di diagnosi precoce
- assistenza sanitaria di base
- assistenza specialistica ambulatoriale e riabilitativa
- assistenza domiciliare
- assistenza psichiatrica
- dipendenze
- assistenza ospedaliera
- emergenza sanitaria e 118
- assistenza residenziale e semi residenziale
- certificati di assistenza al parto e esiti gravidanza
- assistenza farmaceutica e farmacovigilanza
- attività fisica e sportiva
- assistenza integrativa
- assistenza termale
- rischi infortunistici e sanitari connessi con gli ambienti di vita e di lavoro

- infortuni stradali
- accertamenti di invalidità civile, disabilità, handicap
- riconoscimento del diritto all'esenzione
- dati sulla mortalità presso le aziende ASL

Un'ulteriore classificazione è quella derivante dall'applicazione della normativa vigente (D.Lgs. 196/03) che si base sulla tipologia di dati tipici nella gestione della Privacy:

- dati anonimi
- dati personali
- dati sensibili (comprendente i dati Sanitari)

4.2 I Formati dei dati

Un'aspetto rilevante nell'analisi del FSE è quello relativo al formato in cui sono presenti le informazioni. In tal senso possiamo individuare dati tipicamente destrutturati, dati mappati e dati ultimi ma non ultimi dati basati su formati proprietari.

- documenti testuali o di forma destrutturata (documenti "pdf", "txt", "jpeg" etc.)
- documenti strutturati, mappati su schemi XML, CDA, HL7, DICOM
- dati di formati proprietari

Nei prossimi paragrafi saranno descritti gli standard maggiormente diffusi per la descrizione dei dati in documenti strutturati.

4.2.1 HL7 (Health Level Seven) e CDA (Clinical Document Architecture)

Lo standard HL7 deriva il suo nome dal particolare livello dello standard OSI (Open Systems Interconnection) a cui è indirizzato: il livello **di applicazione** o **livello 7.** Nasce alla fine degli anni '80 con lo scopo di uniformare e semplificare lo scambio elettronico d'informazioni cliniche ed amministrative tra i diversi sistemi presenti in un'azienda sanitaria (HIS, RIS, LIS, ecc.). HL7 definisce il formato dei messaggi oggetto di scambio, le modalità di sincronizzazione degli scambi e le specifiche dei messaggi di errore. Diverse applicazioni offrono interfacce conformi al modello HL7, che permettono di ridurre i costi necessari per mettere in comunicazione sistemi diversi.

Lo standard risulta sufficientemente flessibile da permettere di personalizzarlo per le proprie necessità. In pratica, le soluzioni basate su HL7 sono soluzioni su misura, per le quali è necessaria una fase di studio che consiste nell'analisi del contesto in cui lo si vuole applicare. Inoltre, lo standard fornisce le specifiche dettagliate per le tipologie d'interfacce considerate a più alta priorità (es. per le procedure di ADT, ordini e dati clinici). L'intento è di fornire un quadro di riferimento comune, sufficientemente generico ma robusto da consentire l'estensione delle interfacce esistenti.

La CDA (Clinical Document Architecture) è uno standard basato su XML il cui obiettivo è quello di specificare la codifica, la struttura e la semantica dei documenti clinici. La CDA fa parte della versione 3 dello standard HL7 e come altre parti dello standard, è stato studiato e sviluppato utilizzandone il modello di riferimento (RIM) di HL7. La CDA specifica che il contenuto di un documento deve essere composto da:

- una parte testuale, obbligatoria, leggibile ed interpretabile dalle persone
- una parte strutturata, utilizzabile per l'elaborazione automatica

In particolare, la parte strutturata si basa su sistemi di codifica, quali SNOMED e LOINC, per l'espressione di concetti.

4.2.2 DICOM (Digital Imaging and COmmunications in Medicine)

Il formato DICOM è uno standard per la trasmissione tra apparecchiature diverse di dati digitali (immagini biomediche ed informazioni medico-sanitarie), mediante la definizione di un protocollo di comunicazione. Lo standard fa uso di tecnologie e protocolli di rete standard (Ethernet, TCP/IP). Analogamente a HL7, DICOM è un protocollo a livello di applicazione (secondo il modello ISO/OSI).

DICOM realizza un esplicito e dettagliato modello di descrizione di una serie di **oggetti** (paziente, immagine, etc.) che formano il dato radiologico, e di come essi sono tra loro collegati. Alla base dei protocolli definiti da DICOM esiste un modello funzionale del mondo reale, cioè un modello di come le diverse attività ospedaliere (in particolare quelle radiologiche) si svolgono nell'ambiente operativo.

Un'entità del mondo reale (paziente, ricovero, immagine, ecc.) viene modellata come un oggetto su cui è possibile definire un'insieme di attributi (es: l'oggetto paziente conterrà gli attributi dati anagrafici, data di ricovero, etc.). Definiti gli oggetti di interesse e tutte le loro caratteristiche, DICOM definisce per ogni oggetto quali operazioni possono essere eseguite. Tali operazioni sono chiamate DIMSE (Dicom Message Service). La combinazione di un oggetto ed i corrispondenti servizi prende il nome di SOP (Service Object Pair).

4.3 Autorizzazione e accesso ai dati

Anche se conservati all'interno delle strutture sanitarie, i dati di tipo medico restano di proprietà del paziente che ne conserva l'esclusiva discrezionalità sulla loro conservazione e accesso. Per questa ragione, è assolutamente necessario che l'infrastruttura tecnologica utilizzata metta a disposizione, oltre a funzionalità di cifratura, anche funzionalità che permettano la gestione dei permessi di accesso alle informazioni.

L'accesso e la consultazione dei dati devono poter essere gestite in due diverse direzioni:

- a quali informazioni è possibile accedere
- chi può accedere alle informazioni

Quindi, l'infrastruttura deve permettere la gestione delle autorizzazioni al livello delle macro categorie sopra citate. Ciò significa che il paziente deve essere messo nella condizione di poter esprimere livelli di autorizzazione differenti per ognuna delle macro categorie definite.

Inoltre, il paziente deve poter essere in grado di esprimere il livello di autorizzazione in funzione **di chi** accede ai dati. In questo caso è necessario distinguere fra:

caso 1. ruoli interni alla struttura sanitaria

caso 2. ruoli esterni alla struttura sanitaria

caso 3. nominale

Nel primo caso il livello di granularità individuato comprende, a titolo esemplificativo, i seguenti ruoli:

- applicativo sanitario: tutti gli applicativi sanitari possono accedere alle informazioni
- primario
- medico
- caposala
- infermiere

L'organizzazione dei ruoli non segue la gerarchia sanitaria, ossia il paziente può negare l'accesso al medico ma garantirlo all'infermiere.

Nel secondo caso, il paziente deve poter consentire o negare l'accesso alle proprie informazioni da parte di altre strutture sanitarie, laboratori o dal "medico di famiglia".

L'ultimo caso descrive la possibilità di poter indicare puntualmente chi può o non può avere accesso alle informazioni del FSE. Questa opportunità garantisce al paziente di poter garantire l'accesso ai propri dati in caso, ad esempio, di visite specialistiche.

A titolo esemplificativo, si immagini un paziente che si reca presso una struttura sanitaria per affrontare un intervento chirurgico. Il paziente, al momento del ricovero, fornisce le proprie **informazioni anagrafiche** e le informazioni relative al proprio stato di salute (es.: **prescrizioni farmaceutiche, allergie, vaccinazioni**).
Prima dell'intervento chirurgico, il paziente si sottoporrà ad una serie di accertamenti pre-operatori (**TAC, esami sangue, elettrocardiogramma, ecc.**). Tutte queste informazioni congiuntamente al **verbale di sala operatoria** e alle **prescrizioni post-intervento** andranno a formare la cartella clinica del paziente.
Le informazioni raccolte nella cartella clinica, categorizzate secondo la struttura proposta, andranno a formare l'EMR/EHR, ossia il record che descrive lo specifico evento clinico. A questo punto il paziente potrà stabilire **a quali** informazioni è possibile accedere **e chi** vi potrà accedere, arricchendo il proprio FSE.

Può quindi accadere che il paziente decida che le informazioni relative alle prescrizioni siano consultabili da tutti i ruoli presenti nella struttura sanitaria (caso 1), da nessuno al di fuori della struttura sanitaria (caso 2) ad esclusione del proprio medico curante (caso 3).

Analogamente, il paziente può decidere che ai referti (**TAC, esami sangue, elettrocardiogramma**) possano accedere solo i **primari** e i **medici** presenti all'interno della struttura sanitaria (caso 1) e uno **specialista** che non appartiene alla struttura sanitaria (caso 3).

4.4 Conclusioni

Per ogni sistema informativo basato su dati strutturati, come ad esempio ogni applicativo che utilizza un database, è possibile utilizzare una protezione "sistemistica" dei dati sensibili salvaguardando in tal modo gli investimenti effettuati nel tempo sui sistemi.
Infatti, questo tipo di protezione prevede che i dati residenti sui database siano cifrati, ma nel contempo siano accessibili in modo completamente trasparente all'applicativo che li utilizza.

È possibile trovare dei documenti non strutturati in ogni dispositivo di memorizzazione: da un filesystem condiviso all'interno della struttura sanitaria ai computer dei singoli medici, dalle memorie residenti nelle apparecchiature sanitarie ai dispositivi USB tascabili.

Esistono strumenti in grado di memorizzare su un unico sistema anche documenti non strutturati, e renderli fruibili con l'utilizzo del protocollo che si desidera: pur rimanendo memorizzati all'interno di un unico repository i dati possono essere fruiti via web (con un browser), utilizzando condivisioni protette di rete o altre connessioni sicure. La centralizzazione dei dati non strutturati permette anche di evitare la proliferazione di copie di documenti identici o molto simili, utilizzando anche tecniche di individuazione di similarità.

Inoltre, indipendentemente dal fatto che questi documenti siano o meno memorizzati all'interno di un unico repository, è possibile proteggerli mediante tecniche di cifratura e controllarne l'accesso anche al di fuori del perimetro della struttura sanitaria.

Tali documenti, una volta protetti, rimangono ad accesso esclusivo delle persone autorizzate a vederli e non è possibile estrarne il contenuto in alcun modo (né con copia-incolla, né rinominando i file, né tantomeno catturando l'immagine presente a video). Grazie ad una console centralizzata è possibile modificare i diritti di accesso a files già rilasciati

Mappatura Tecnologica

L'obiettivo primario di questo capitolo è leggere la normativa secondo la prospettiva non dei requisiti funzionali in senso applicativo quanto dei requisiti funzionali finalizzati alla tutela dei dati personali e della loro sicurezza.

Riprendendo gli aspetti individuati precedentemente, ai fini di una soluzione informatica, il FSE risulta essere un oggetto con le seguenti caratteristiche:

- è il risultato del lavoro di soggetti diversi, collocati in organizzazioni diverse (Titolari diversi) e con profili di responsabilità e, quindi di accesso ai dati, differenti;
- non è di proprietà di chi lo produce;
- non è di proprietà di chi lo mantiene;
- è centrato sull'interessato che è il proprietario delle informazioni ed è esterno a tutte le organizzazioni che le producono;
- presuppone la capacità di colloquio fra ambienti ed organizzazioni diverse.

rispetto al quale il proprietario può:

- decidere di non volerlo;
- dettare i criteri di accessibilità;
- decidere di oscurare parti delle informazioni sanitarie;
- decidere di non rendere visibile la scelta di oscurare parti delle informazioni sanitarie (il c.d oscuramento dell' l'oscuramento).

Prima ancora di entrare nel merito dei requisiti di sicurezza esplicitamente individuati dal Garante all'art.10, appare evidente come questi aspetti impongano una complessità di gestione assai rilevante dove la componente sicurezza è fondamentale dall'origine.

La sicurezza nella gestione delle informazioni non è, dunque, un requisito aggiuntivo ad altri requisiti funzionali, ma una caratteristica intrinseca di ciascun requisito funzionale, e questo è in linea con la proposta di un approccio architetturale.

Il secondo obiettivo di questo capitolo è porre in relazione tali requisiti e ciò che essi implicano nella realizzazione di una soluzione con tecnologie o classi di tecnologie in grado di soddisfarli.

Complessivamente si tratta, dunque, di individuare gli elementi di un'architettura di sicurezza che, grazie ai servizi che assicura, possa contribuire alla semplificazione delle soluzioni applicative, riducendone al contempo il costo di gestione.

Riferimenti e implicazioni delle linee guida.

Le Linee guida del Garante, per quanto riguarda i requisiti di sicurezza ed alcune garanzie dei diritti degli interessati al trattamento di dati personali, si collocano all'interno della tendenza generale alla costituzione di sistemi di gestione della sicurezza delle informazioni (ISMS) basati su standard di mercato.

Tale approccio comprende un perimetro più ampio del solo ambito tecnologico, interessando gli aspetti organizzativi ed i processi decisionali in modo trasversale.

Diversi sono gli standard industriali riconosciuti che affrontano questi temi. In particolare è utile citare ISO/IEC 27000 che raggruppa best practice e standard per la costituzione di un ISMS.

Nel più generale quadro della normativa sulla tutela dei dati personali, attuare le Linee guida comporta l'implementazione di misure organizzative e tecnologiche riconducibili ad alcune di quelle previste dallo standard ISO citato ed avvicina al raggiungimento di uno standard di sicurezza delle informazioni utile per garantire obiettivi più ampi di tutela dei soli dati personali e dei diritti alla privacy degli interessati.

Far riferimento ad un ISMS permette di inquadrare le tematiche di compliance al provvedimento del Garante nel contesto più ampio della sicurezza delle informazioni, contesto che riguarda il funzionamento complessivo del sistema sanitario e non esclusivamente la tutela del diritto alla privacy, ottenendo così dei benefici di tipo progettuale ed economico nelle fasi realizzative.

Analisi del testo: elementi di una architettura di sicurezza implicate dai requisiti delle linee guida.

Le Linee guida individuano, in un articolo specifico (art. 10), le misure di sicurezza che devono essere poste in essere a tutela dei dati personali. In ognuno degli altri articoli, però, gli specifici requisiti funzionali per il FSE presuppongono un livello di sicurezza che richiede di essere analizzato.

In ogni caso, le risposte possono essere di natura applicativa, cioè risolte da funzionalità specificamente disegnate in risposta al requisito normativo o realizzate tramite un'architettura di sicurezza che fornisca servizi alle applicazioni. Questo secondo approccio garantisce il riuso delle best practice, un livello di efficacia e di economicità di realizzazione e di gestione non ottenibili con un approccio applicativo.

Per queste ragioni, nel seguito, il testo è analizzato estraendo (parti in corsivo), articolo per articolo, i requisiti sensibili all'approccio architetturale anziché applicativo.

Ambito di applicazione delle Linee guida (art.2)

> *Il Fse dovrebbe essere costituito preferendo di regola soluzioni che non prevedano una duplicazione in una nuova banca dati delle informazioni sanitarie formate dai professionisti o organismi sanitari che hanno preso in cura l'interessato.*
>
> *In secondo luogo, provenendo i dati sanitari e i documenti riuniti nel Fse da più soggetti, dovrebbero essere adottate idonee cautele per ricostruire, anche in termini di responsabilità, chi ha raccolto e generato i dati e li ha resi disponibili nell'ambito del Fse.*
>
> *Qualora attraverso il Fse o il dossier si intendano perseguire anche talune finalità amministrative strettamente connesse all'erogazione della prestazione sanitaria richiesta dall'interessato (es. prenotazione e pagamento di una prestazione), tali strumenti dovrebbero essere strutturati in modo tale che i dati amministrativi siano separati dalle informazioni sanitarie(2), prevedendo profili diversi di abilitazione degli aventi accesso agli stessi in funzione della differente tipologia di operazioni ad essi consentite.*

Dai requisiti sopra riportati, si evincono alcune caratteristiche infrastrutturali:

- i dati risiedono, nella responsabilità del Titolare, quando sono stati generati e vengono acceduti da altri Titolari/Titolati via rete.

  - **Punti chiave / tecnologie: sicurezza della rete, disponibilità dell'infrastruttura, encryption dei dati**

- l'accesso ai dati deve essere garantito a soggetti esterni all'organizzazione del Titolare, con finalità legittime ed a cui l'interessato ha dato il proprio consenso. L'identificazione e l'autorizzazione di chi richiede l'accesso devono, quindi, riguardare organizzazioni diverse.
  - **Punti chiave / tecnologie: gestione dell'identità elettronica e dei profili d'accesso; capacità di federare le identità e i profili di ambienti diversi.**

Non tutti i requisiti, ovviamente, trovano soluzione a livello infrastrutturale: alcuni di essi, come ad esempio la capacità di risalire al Titolare che ha raccolto il consenso relativo al dato, ricadono nelle caratteristiche funzionali della soluzione e, pertanto, esulano dagli obiettivi del documento. Sono, però, aspetti da non sottovalutare in quanto la tracciabilità degli accessi è un elemento di sicurezza essenziale per risalire a chi ha compiuto azioni fraudolente .

Diritto alla costituzione di un Fascicolo sanitario elettronico o di un dossier sanitario (art. 3)

In base alle disposizioni contenute nel Codice dell'amministrazione digitale, deve essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali e, in particolare, delle disposizioni del Codice dell'amministrazione digitale (d.lg. 7 marzo 2005, n. 82).

Il tema della disponibilità delle informazioni sanitarie è rilevante, in particolare, se collegato alla opzione per cui le informazioni risiedono nel perimetro organizzativo del Titolare che le ha raccolte e dunque, non sono duplicate (art. 2). Avendo l'interessato espresso il consenso alla costituzione del FSE, l'indisponibilità dell'informazione può condurre alla negazione sostanziale del diritto di cura e dalla tutela della salute. Si tratta, con tutta evidenza, di un profilo di responsabilità assai rilevante, che va oltre il tema privacy in senso stretto.

Di conseguenza, per quanto attiene all'infrastruttura, la disponibilità dell'informazione presuppone la disponibilità di tutte le componenti che connettono la domanda di informazione al luogo in cui essa è memorizzata.

  - **Punti chiave / tecnologie: ne consegue come l'infrastruttura erogante i servizi relativi l'FSE dovrà essere basata su concetti quali la Scalabilità, il BackUp/Recovery, l'alta affidabilità del sistema, le funzionalità di Disaster Recovery.**

Il trattamento dei dati personali effettuato mediante il Fse o il dossier, perseguendo le menzionate finalità di prevenzione, diagnosi, cura e riabilitazione, deve uniformarsi al principio di autodeterminazione (artt. 75 e ss. Del Codice). All'interessato dovrebbe essere consentito di scegliere, in piena libertà, se far costituire o meno un se/dossier con le informazioni sanitarie che lo riguardano, garantendogli anche la possibilità che i dati sanitari restino disponibili solo al professionista o organismo sanitario che li ha redatti, senza la loro necessaria inclusione in tali strumenti.

Il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura (cfr. art. 81 del Codice), deve essere autonomo e specifico. Tuttavia, dovrebbero essere previsti momenti distinti in cui l'interessato possa esprimere la propria volontà, attraverso un consenso di carattere generale per la costituzione del Fse e di consensi specifici ai fini della sua consultazione o meno da parte dei singoli titolari del trattamento (es. medico di medicina generale, pediatra di libera scelta, farmacista, medico ospedaliero)."

Ferma restando l'indubbia utilità di un Fse/dossier completo, dovrebbe essere garantita la possibilità di non far confluire in esso alcune informazioni sanitarie relative a singoli eventi clinici (ad es., con riferimento a una specifica visita specialistica o alla prescrizione di un farmaco).

L'"oscuramento" dell'evento clinico (revocabile nel tempo) dovrebbe peraltro avvenire con modalità tali da garantire che, almeno in prima battuta, tutti (o alcuni) soggetti abilitati all'accesso non possano venire automaticamente (anche temporaneamente) a conoscenza del fatto che l'interessato ha effettuato tale scelta ("oscuramento dell'oscuramento").

- **Punti chiave / tecnologie: questi requisiti impongono una gestione dei diritti di accesso e funzionalità molto sofisticate e condivise fra più titolari, coinvolgendo non solo gli operatori sanitari ma anche i cittadini (cioè milioni di interessati). E' possibile soddisfarli realizzando soluzioni che riguardano sia l'architettura di sicurezza sia il livello applicativo.**

L'obbligo di garantire questi requisiti a livello nazionale suggerisce l'adozione di modelli e standards condivisi.

Individuazione dei soggetti che possono trattare i dati

"Nell'individuare gli incaricati il titolare o il responsabile dovrebbero indicare con chiarezza l'ambito delle operazioni consentite (operando, in particolare, le opportune distinzioni tra il personale con compiti amministrativi e quello con funzioni sanitarie), avendo cura di specificare se gli stessi abbiano solo la possibilità di consultare il Fascicolo/dossier o anche di integrarlo o modificarlo (cfr. punto 5 del presente provvedimento)."

Il tema del controllo degli accessi, della gestione delle identità e dei ruoli, considerando l'alto tasso di mobilità e di personale temporaneo e/o dei soggetti che il cittadino ha abilitato in termini di accesso all'FSE, appare come una precondizione per garantire la gestione corretta dei dossier e, quindi, del FSE. Si tratta di un compito che deve essere delegato all'infrastruttura perché altrimenti dovrebbe essere declinato in modo coerente all'interno di tutte le piattaforme applicative che concorrono all'erogazione di servizi sanitari e amministrativi.

- **Punti chiave / tecnologie: la gestione applicativa dei ruoli e dei profili di accesso ad essi collegati è tipicamente una tematica applicativa a cui l'infrastruttura è funzionale. E' altresì vero che oggi può essere affrontata attraverso l'adozione di tecnologie infrastrutturali che governano a pieno titolo tutti gli aspetti legati alla gestione del ciclo di vita del dipendente e dei soggetti terzi che hanno diritti di accesso all'FSE.**

La gestione dei ruoli e delle identità e, di conseguenza, degli accessi deve essere affrontata a livello di ogni singola entità che concorre al FSE, dunque a livello di dossier. In caso contrario, non potrebbero essere garantiti i requisiti descritti nei punti precedenti e successivi, relativamente ai diritti dell'interessato.

Accesso ai dati personali contenuti nel Fascicolo sanitario elettronico e nel dossier sanitario (Art. 5)

Dovrebbero essere pertanto preferite soluzioni che consentano un'organizzazione modulare di tali strumenti in modo da limitare l'accesso dei diversi soggetti abilitati alle sole informazioni (e, quindi, al modulo di dati) indispensabili, in questo senso le tecnologie abilitano ad un livello di granularità che arriva al singolo dato elementare.

L'abilitazione all'accesso deve essere consentita all'interessato nel rispetto delle cautele previste dall'art. 84 del Codice, secondo cui gli esercenti le professioni sanitarie e gli organismi sanitari possono comunicare all'interessato informazioni inerenti al suo stato di salute (es. referti, esiti di consulti medici) per il tramite di un medico -individuato dallo stesso interessato o dal titolare- o di un esercente le professioni sanitarie, che nello svolgimento dei propri compiti intrattiene rapporti diretti con il paziente(3). Tale garanzia dovrebbe essere osservata anche quando l'accesso al Fascicolo avviene mediante l'utilizzo di una smart card

In ogni caso, l'accesso al Fse/dossier dovrebbe essere circoscritto al periodo di tempo indispensabile per espletare le operazioni di cura per le quali è abilitato il soggetto che accede.

Questo articolo affronta un tema – quello dell'accesso degli interessati – che comporta un cambio nell'ordine di grandezza del problema, sia per gli aspetti quantitativi che qualitativi: dalla gestione di centinaia/migliaia di utenti professionali conosciuti e formati alla gestione di milioni di utenti indistinti.

È da notare che il diritto di accesso degli interessati è limitato ai dati che li riguardano o rispetto ai quali si è instaurato un diritto specifico. Diventa centrale il tema dell'autenticazione, cioè il tema dell'identificazione certa del paziente.

- **Temi critici: Strong authentication e Intrusion Detection Systems.**

Diritti dell'interessato sui propri dati personali (art. 7 del Codice)

"Come già precisato, all'interessato devono essere garantite facili modalità di consultazione del proprio Fse/dossier (Cfr. punto 4), nonché, ove previsto, di ottenerne copia, anche ai fini della messa disposizione a terzi (es. medico operante in un'altra regione o in un altro Stato)."

La possibilità di consultare il proprio FSE on line riporta al tema già trattato dell'identificazione certa dell'interessato.

- **Tema critico: Strong authentication.**

Se, invece, la consultazione può avvenire solo mediante una procedura gestita da personale interno, il tema si sposta sul piano organizzativo.

Limiti alla diffusione e al trasferimento all'estero dei dati

"Anche il trasferimento all'estero dei dati sanitari documentati nel Fse/dossier per finalità di prevenzione, diagnosi e cura dell'interessato può avvenire esclusivamente con il suo consenso, salvo il caso in cui sia necessario per la salvaguardia della vita o della incolumità di un terzo (art. 43 del Codice)".

Questo requisito può diventare rilevante sia in caso di outsourcing dei servizi IT sia nel caso in cui il paziente sia inserito in un programma di ricerca che preveda collaborazioni con soggetti terzi residenti all'estero.

Le implicazioni, più che tecnologiche, sono di natura organizzativa e contrattuale da un lato e di acquisizione del consenso dall'altro.

Misure di sicurezza

"Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati dovrebbero essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).

Dovrebbero essere, inoltre, assicurati:

- *idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);*

- *procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;*
- *individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;*
- *tracciabilità degli accessi e delle operazioni effettuate;*
- *sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie."*

L'insieme dei requisiti elencati corrisponde a quello emerso dall'analisi puntuale dei singoli articoli e configura un'architettura completa di data security, identity management e data access security, sottostante al livello applicativo e con quest'ultimo integrata.

Affrontare il soddisfacimento di questi requisiti al livello applicativo comporta una duplicazione di informazioni e di attività di gestione di queste informazioni tale da pregiudicare sia l'efficacia della tutela dei diritti sia l'efficienza e la sostenibilità economica della soluzione.

I requisiti di sicurezza specificatamente indicati devono essere garantiti a livello dell'organizzazione di ciascun singolo titolare (ASL, Ospedale, laboratorio, etc.) e, quindi, a livello del sistema sanitario in cui sono inclusi, rispetto al quale viene attivato il FSE.

Ai requisiti specificatamente previsti dalle Linee guida vanno aggiunti quelli definiti da altri provvedimenti del Garante di applicazione generale come il Provvedimento sugli Amministratori di sistema.

Scenari d'uso – Utenti del sistema FSE

Gli scenari d'uso presentati in questo paragrafo vedono coinvolti i seguenti principali attori:

- operatore sanitario – è il medico dell'azienda sanitaria, oppure il medico di base, lo specialista, l'infermiere, il farmacista, etc.;
- operatore di accettazione – è il personale amministrativo, incaricato del trattamento dei dati di anagrafica e fatturazione;
- paziente – è l'interessato, ossia il proprietario dei dati personali, oppure chi esercita la patria potestà;
- Admin – è l'amministratore del sistema FSE.

La tabella di seguito riassume l'insieme degli scenari, specificando per ciascuno di essi obiettivi ed attori coinvolti.

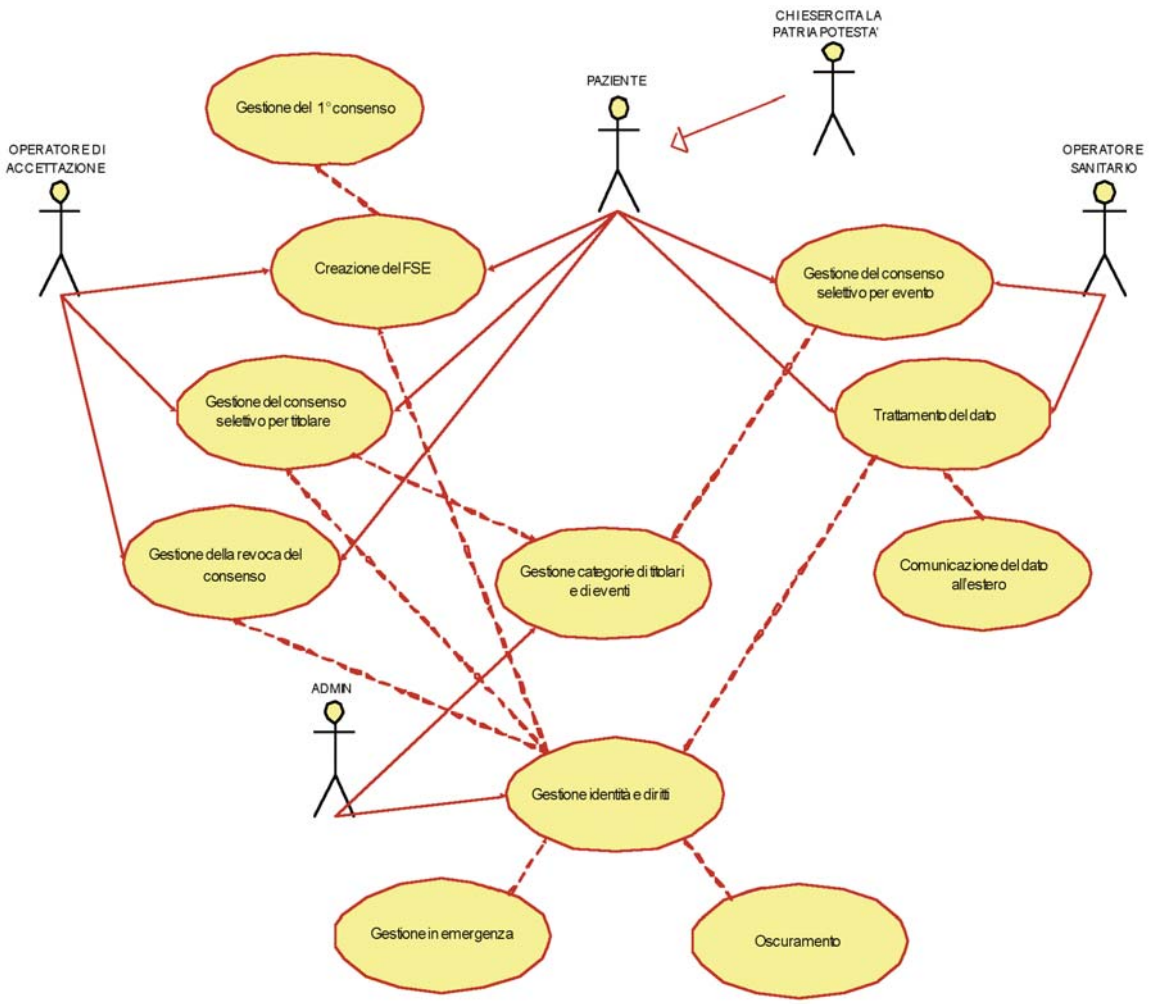


Fig. 6 - Scenari d'uso del sistema FSE, vista utente

Tabella 1 - Scenari d'uso del sistema FSE

Use Case ID	Use Case Name	Objective	Actors	Include/Estende
UC01	Creazione del FSE	Il paziente richiede la creazione di un FSE per il trattamento dei propri dati personali e viene informato dall'OPERATORE DI ACCETTAZIONE circa le modalità di trattamento.	PAZIENTE, OPERATORE DI ACCETTAZIONE	Include UC02
UC02	Gestione del 1° consenso	Il paziente esprime il proprio consenso informato alla creazione e mantenimento di un FSE.	PAZIENTE, OPERATORE DI ACCETTAZIONE	
UC03	Gestione del consenso selettivo per titolare	Il paziente acconsente al trattamento dei propri dati personali da parte di operatori sanitari individuati.	PAZIENTE, OPERATORE DI ACCETTAZIONE	Include UC06
UC04	Gestione della revoca del consenso	Il paziente revoca il suo consenso al mantenimento di un FSE che lo riguarda.	PAZIENTE, OPERATORE DI ACCETTAZIONE	
UC05	Gestione identità e diritti	Creazione, modifica e disattivazione degli account sul sistema.	ADMIN	Include UC01, UC03, UC04
UC06	Gestione categorie di titolari e di eventi	Creazione, modifica, eliminazione delle categorie di titolari e delle categorie di eventi.	ADMIN	
UC07	Oscuramento	Oscuramento dell'evento clinico per il quale non sono stati riconosciuti diritti all'utente del sistema.	ADMIN	Estende UC05
UC08	Gestione in emergenza	In casi di urgenza, specificatamente autorizzati, vengono concessi diritti ad operatori sanitari per i quali non è stato espresso il consenso da parte dell'interessato o di chi ne esercita la patria potestà.	ADMIN	Estende UC05
UC09	Gestione del consenso selettivo per evento	Il paziente acconsente all'inserimento nel FSE di eventi clinici.	PAZIENTE, OPERATORE SANITARIO	Include UC06
UC10	Trattamento del dato	L'utente svolge operazioni sui dati secondo il profilo di accesso ed i diritti assegnati.	PAZIENTE, OPERATORE SANITARIO	Include UC05
UC11	Comunicazione del dato all'estero	Comunicazione del dato all'estero L'utente è abilitato a comunicare dati e file contenuti nel FSE.	OPERATORE SANITARIO	Estende UC10

6.1 Dettaglio

In questo paragrafo vengono forniti dettagli per ciascuno scenario d'uso definito nella tabella predente.

Tabella 2 - Creazione del FSE

UC ID	**UC01 Creazione del FSE**
Descrizione	Viene creato il FSE di un nuovo assistito.
Precondizioni	L'interessato dà il consenso alla creazione del FSE.
Attore principale	PAZIENTE, OPERATORE DI ACCETTAZIONE
Attore secondario	–
Scenario	1. L'OPERATORE DI ACCETTAZIONE registra/recupera l'anagrafica dell'assistito (dal sistema regionale). 2. L'OPERATORE DI ACCETTAZIONE fornisce all'interessato l'informativa sul trattamento dei dati personali. 3. A partire dai dati di anagrafica viene aperto un FSE del paziente.
Postcondizioni	

Tabella 3 - Gestione del 1° consenso

UC ID	**UC02 Gestione del 1° consenso**
Descrizione	L'interessato esprime il consenso informato.
Precondizioni	
Attore principale	PAZIENTE, OPERATORE DI ACCETTAZIONE
Attore secondario	–
Scenario	1. Viene reso il consenso informato dell'interessato alla creazione e mantenimento di un FSE che lo riguardi o relativo ad un soggetto nei riguardi del quale eserciti la patria potestà. 2. A partire dai dati di anagrafica viene registrato l'utente nel sistema IAM (se il sistema viene configurato per consentire l'accesso ai dati anche all'interessato).
Postcondizioni	L'assistito resta in attesa di ricevere le credenziali di accesso al sistema.

Tabella 4 - Gestione del consenso selettivo per titolare

UC ID	**UC03 Gestione del consenso selettivo per titolare**
Descrizione	L'interessato esprime il consenso (revoca il consenso) al trattamento dei propri dati sulla base delle categorie di titolari presenti nel sistema (configurabili) e delle categorie di eventi (configurabili).
Precondizioni	-
Attore principale	PAZIENTE, OPERATORE DI ACCETTAZIONE,
Attore secondario	
Scenario	1. L'OPERATORE DI ACCETTAZIONE informa l'interessato e chiede il consenso al trattamento secondo associazioni di default tra categorie di eventi e titolari. 2. L'OPERATORE DI ACCETTAZIONE informa l'interessato sull'oscuramento di default degli eventi per gli utenti non aventi i diritti. 3. L'OPERATORE DI ACCETTAZIONE chiede all'interessato il consenso alla modifica dell'impostazione di default dell'oscuramento, secondo associazioni tra categorie di eventi e titolari. 4. I consensi espressi sono registrati e trasmessi al sistema IAM.
Postcondizioni	

Tabella 5 - Gestione della revoca del consenso

UC ID	**UC04 Gestione della revoca del consenso**
Descrizione	L'assistito revoca il consenso al trattamento dei propri dati personali attraverso il mantenimento di un FSE.
Precondizioni	Esiste un FSE relativo all'interessato.
Attore principale	PAZIENTE, OPERATORE DI ACCETTAZIONE
Attore secondario	–
Scenario	5. L'OPERATORE DI ACCETTAZIONE riceve e registra la richiesta di revoca del consenso da parte dell'interessato. 6. Lo stato di revoca viene trasmesso al sistema IAM. 7. Il sistema IAM provvede a bloccare le operazioni di inserimento e modifica. 8. Il sistema IAM provvede a bloccare le operazioni in lettura da parte di soggetti differenti dal titolare del trattamento.
Postcondizioni	–

Tabella 6 - Gestione identità e diritti

UC ID	**UC05 Gestione identità e diritti**
Descrizione	ADMIN determina gli account ed i permessi da assegnare e/o da ritirare, in base ai consensi espressi o revocati dall'interessato
Precondizioni	–
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN provvede alla creazione degli account sul sistema IAM. 2. ADMIN provvede all'attribuzione dei ruoli e permessi opportuni sul sistema IAM. 3. ADMIN provvede al ritiro dei permessi e degli account sul sistema IAM
Postcondizioni	–

Tabella 7 - Gestione categorie di titolari e di eventi

UC ID	**UC06 Gestione categorie di titolari e di eventi**
Descrizione	ADMIN determina associazioni di default tra categorie di titolari e categorie di eventi
Precondizioni	–
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN provvede alla creazione, modifica e ritiro della lista di titolari sul sistema IAM. 2. ADMIN provvede alla creazione, modifica e ritiro della lista di eventi sul sistema IAM. 3. ADMIN provvede alla creazione, modifica e ritiro delle associazioni tra titolari ed eventi sul sistema IAM
Postcondizioni	–

Tabella 8 - Oscuramento

UC ID	UC07 Oscuramento
Descrizione	Di default, per ciascun utente sono oscurati gli eventi per i quali non gli sono attribuiti diritti.
Precondizioni	Sono definiti identità e diritti.
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN provvede a definire di default l'oscuramento sul sistema IAM. 2. ADMIN provvede a modificare l'impostazione di default in base al consenso espresso dall'interessato (UC03).
Postcondizioni	–

Tabella 9 - Gestione in emergenza

UC ID	UC08 Gestione in emergenza
Descrizione	Sono attribuite credenziali e diritti per l'acceso al FSE, anche in assenza del consenso dell'interessato o di chi ne esercita la patria potestà, per i casi di urgenza autorizzati e registrati.
Precondizioni	Autorizzazione specifica
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN riceve una richiesta di provisioning autorizzata, in assenza del consenso espresso dell'interessato o di chi ne esercita la patria potestà. 2. ADMIN attribuisce sul sistema IAM diritti sul FSE ad un OPERATORE SANITARIO univocamente individuato, per un tempo definito. 3. ADMIN revoca sul sistema IAM i diritti all'OPERATORE SANITARIO.
Postcondizioni	–

Tabella 10 - Gestione del consenso selettivo per evento

UC ID	UC09 Gestione del consenso selettivo per evento
Descrizione	L'interessato esprime il consenso al trattamento di specifici eventi clinici.
Precondizioni	
Attore principale	PAZIENTE, OPERATORE SANITARIO
Attore secondario	
Scenario	1. L'OPERATORE SANITARIO informa l'interessato e chiede il consenso all'inserimento nel FSE di specifici nuovi eventi sanitari. 2. Il PAZIENTE esprime il suo consenso (non consenso) all'inserimento e/o all'oscuramento di specifici nuovi eventi sanitari. 3. I consensi espressi sono registrati e trasmessi al sistema IAM.
Postcondizioni	–

Tabella 11 - Trattamento del dato

UC ID	**UC10 Trattamento del dato**
Descrizione	L'utente del sistema effettua le operazioni di trattamento che gli sono consentite dal profilo e dai diritti assegnati.
Precondizioni	Esiste l'utente nel sistema.
Attore principale	PAZIENTE, OPERATORE SANITARIO
Attore secondario	
Scenario	1. L'utente del sistema accede ai dati ed effettua le operazioni che gli sono consentite dal profilo e diritti assegnati. 2. Ogni operazione effettuata dall'utente è registrata e mantenuta dal sistema di audit log.
Postcondizioni	–

Tabella 12 - Comunicazione del dato all'estero

UC ID	**UC11 Comunicazione del dato all'estero**
Descrizione	L'utente del sistema effettua le operazioni di trasmissione dei dati ad altro titolare situato all'estero
Precondizioni	Esiste l'utente nel sistema.
Attore principale	OPERATORE SANITARIO
Attore secondario	
Scenario	1. L'utente del sistema accede ai dati ed effettua le operazioni che gli sono consentite dal profilo e diritti assegnati. 2. Ogni operazione effettuata dall'utente è registrata e mantenuta dal sistema di audit log.
Postcondizioni	–

Scenari d'uso del sistema IAM

Gli scenari d'uso presentati in questo paragrafo vedono coinvolti i seguenti principali attori:

- Titolare – ha la responsabilità in merito alla protezione ed al trattamento dei dati personali ed alla creazione, modifica e disattivazione degli utenti del sistema FSE.
- Utente – è l'utente del sistema, abilitato alle operazioni di trattamento definite dal ruolo che gli viene attribuito. Sono generalizzazioni dell'Utente il Paziente e l'Operatore sanitario.
- Admin – è l'amministratore del sistema.

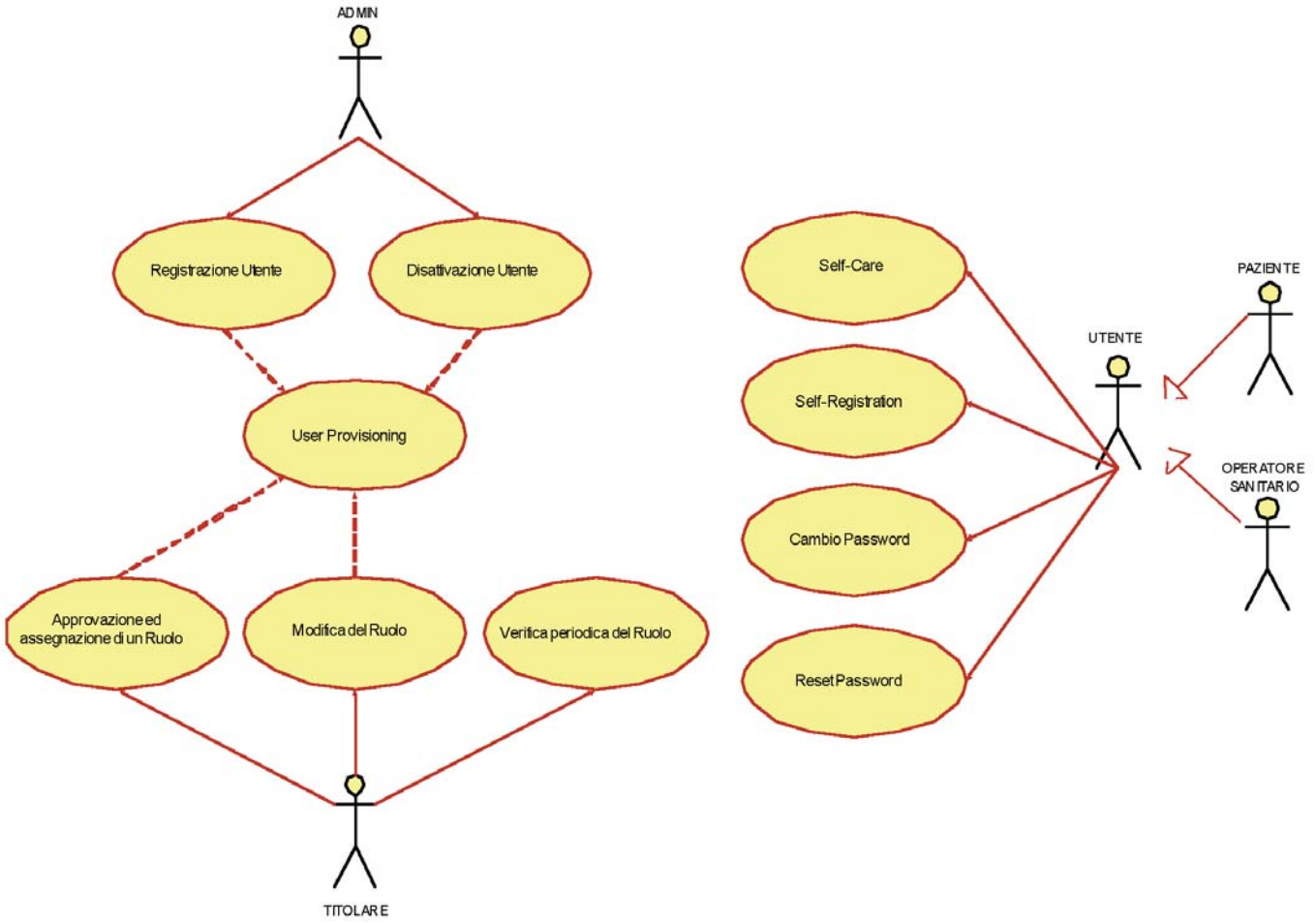


Fig. 7 - Scenari d'uso del sistema IAM – Vista utente

Tabella 13 – Scenari d'uso del sistema IAM

Use Case ID	Use Case Name	Objective	Actors	Include/Estende
UC12	Registrazione Utente	Un nuovo utente (paziente o operatore sanitario) viene registrato nel sistema.	ADMIN	Include UC21
UC13	Disattivazione Utente	L'utenza di un paziente o operatore sanitario viene disattivata.	ADMIN	Include UC21
UC14	Self–Care	Un paziente visualizza ed aggiorna i propri dati presenti nel sistema.	UTENTE	
UC15	Self–Registration	Un operatore sanitario effettua richiesta di accesso al sistema.	UTENTE	
UC16	Reset Password	L'utente effettua un reset della password.	UTENTE	
UC17	Cambio Password	L'utente cambia la propria password.	UTENTE	
UC18	Approvazione e assegnazione del Ruolo	Il Titolare approva l'assegnazione del nuovo ruolo ad un utente ed autorizza l'accesso ai sistemi di sua competenza (in base al consenso espresso dall'interessato).	TITOLARE	Include UC21
UC19	Modifica del Ruolo	Il Titolare approva la modifica del ruolo di un utente (in base al consenso espresso dall'interessato).	TITOLARE	Include UC21
UC20	Verifica periodica del Ruolo	Il Titolare verifica periodicamente i ruoli ed i permessi assegnati ad un utente.	TITOLARE	
UC21	User Provisioning	Creazione, modifica e rimozione degli account sui sistemi		

6.2 Dettaglio

In questo paragrafo vengono forniti dettagli per ciascuno scenario d'uso definito nella tabella predente.

Tabella 14 – Registrazione Utente

UC ID	UC12 Registrazione Utente
Descrizione	Un nuovo utente viene aggiunto al sistema FSE.
Precondizioni	Il nuovo utente non esiste nel sistema.
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN inserisce il nuovo utente nel sistema 2. L'anagrafica del nuovo utente viene trasmessa al sistema IAM secondo pianificazione 3. Il nuovo utente viene memorizzato nel sistema IAM 4. Vengono effettuate le opportune attività di provisioning (UC21)
Postcondizioni	–

Tabella 15 – Disattivazione Utente

UC ID	UC13 Disattivazione Utente
Descrizione	L'utente non deve avere più accesso al sistema, vengono disabilitate le sue credenziali.
Precondizioni	L' utente esiste nel sistema.
Attore principale	ADMIN
Attore secondario	–
Scenario	1. ADMIN modifica lo stato dell'utente nel sistema 2. Lo stato dell'utente viene trasmesso al sistema IAM secondo pianificazione 3. Vengono effettuate le opportune attività di deprovisioning (UC21)
Postcondizioni	–

Tabella 16 - Self-Care

UC ID	UC14 Self–Care
Descrizione	L'utente accede al sistema IAM per aggiornare autonomamente i propri dati.
Precondizioni	L'utente è già presente nel sistema.
Attore principale	UTENTE
Attore secondario	–
Scenario	1. L'utente accede al sistema 2. L'utente aggiorna i dati 3. Il sistema provvede ad aggiornare i dati su tutti i sistemi target per i quali l'utente dispone di un account
Postcondizioni	–

Tabella 17 - Self–Registration

UC ID	**UC15 Self–Registration**
Descrizione	L'utente accede al sistema IAM per richiedere la creazione di un account per l'accesso al sistema FSE.
Precondizioni	L'utente è già presente nel sistema.
Attore principale	UTENTE
Attore secondario	–
Scenario	1. L'utente accede al sistema 2. L'utente effettua la richiesta di account per il sistema desiderato 3. Il sistema provvede a notificare la richiesta di creazione account al Titolare per l'approvazione (che avviene sulla base del consenso espresso dall'interessato).
Postcondizioni	–

Tabella 18 – Reset Password

UC ID	**UC16 Reset Password**
Descrizione	L'utente accede al sistema IAM per richiedere il reset della password di un account presso un sistema target.
Precondizioni	L'utente conosce la domanda di sicurezza.
Attore principale	UTENTE
Attore secondario	–
Scenario	1. L'utente accede al sistema 2. L'utente richiede il reset della password 3. L'utente risponde alla domanda di sicurezza 4. Il sistema provvede a generare una password secondo le policy di sicurezza 5. Il sistema provvede al reset della password 6. Il sistema impone il cambio della password al primo accesso 7. Il sistema notifica la password all'utente
Postcondizioni	–

Tabella 19 – Cambio Password

UC ID	**UC17 Cambio Password**
Descrizione	L'utente effettua il cambio password
Precondizioni	–
Attore principale	UTENTE
Attore secondario	–
Scenario	1. L'utente accede al sistema 2. L'utente richiede il cambio della password 3. L'utente immette la password precedente 4. L'utente immette la nuova password 5. Il sistema verifica che la password inserita rispetti le policy di sicurezza 6. Il sistema provvede a cambiare la password sul sistema target
Postcondizioni	–

Tabella 20 – Approvazione ed attribuzione del Ruolo

UC ID	UC18 Approvazione ed attribuzione del Ruolo
Descrizione	Il Titolare approva l'assegnazione di un ruolo ad un utente sul sistema che gestisce (in base al consenso espresso dall'interessato).
Precondizioni	
Attore principale	Titolare
Attore secondario	
Scenario	1. Il sistema provvede a notificare al Titolare la richiesta di attribuzione di un Ruolo ad un utente ed il relativo consenso espresso dall'interessato 2. Il Titolare approva la richiesta di assegnazione 3. Il sistema provvede a ritirare gli account non più necessari per il ruolo assegnato (UC21) 4. Il sistema provvede a creare i nuovi account (UC21)
Postcondizioni	–

Tabella 21 – Modifica del Ruolo

UC ID	UC19 Modifica del Ruolo
Descrizione	Il Titolare approva la modifica del ruolo di un utente sul sistema che gestisce (in base al consenso espresso dall'interessato).
Precondizioni	–
Attore principale	Titolare
Attore secondario	
Scenario	1. Il sistema provvede a notificare al Titolare la richiesta di cambio ruolo ed il relativo consenso dell'interessato 2. Il Titolare approva la modifica del ruolo 3. Il sistema provvede a ritirare gli account non più necessari per il nuovo ruolo (UC21) 4. Il sistema provvede a creare i nuovi account (UC21)
Postcondizioni	–

Tabella 22 – Revisione periodica dei Ruoli assegnatl

UC ID	UC20 Revisione periodica dei Ruoli assegnati
Descrizione	Il Titolare rivede periodicamente le attribuzioni dei ruoli agli utenti.
Precondizioni	Il sistema, a seguito di policy, compone periodicamente la lista degli utenti da rivedere
Attore principale	Titolare
Attore secondario	
Scenario	1. Il Titolare accede al sistema 2. Il sistema propone l'elenco degli utenti da rivedere 3. Il Titolare seleziona un utente 4. Il Titolare ricertifica l'utente oppure gli attribuisce un nuovo ruolo (UC19)
Postcondizioni	–

Tabella 23 - User Provisioning

UC ID	**UC21 User Provisioning**
Descrizione	Attività di provisioning degli account sui sistemi target. Scenario incluso in: UC12, UC13, UC18, UC19
Precondizioni	–
Attore principale	–
Attore secondario	–
Scenario	1. Il sistema, in base ai ruoli assegnati all'utente, determina gli account ed i permessi da assegnare e/o da ritirare 2. Il sistema provvede alla creazione degli account sui sistemi target 3. Il sistema provvede all'attribuzione dei ruoli e permessi opportuni 4. Il sistema provvede a ritirare i permessi e gli account
Postcondizioni	–

Lo stato dell'arte delle minacce informatiche

L'evoluzione tecnologica e la crescente propagazione dei servizi digitali hanno reso i sistemi informatici sempre più complessi, sia dal punto di vista architetturale che gestionale. Un effetto indesiderato di tale diffusione è stato il contemporaneo incremento delle vulnerabilità e delle minacce, queste ultime sempre più spesso concretizzate mediante attacchi compiuti con strumenti informatici facilmente reperibili su Internet. Nel seguito saranno riportati alcuni aspetti dello scenario della sicurezza informatica nel 2009, con particolare attenzione alle minacce ed alle metodologie di attacco. Le fonti di riferimento utilizzate sono i report, disponibili pubblicamente di alcuni degli attori di rilievo nel panorama delle security (enti governativi, *vendor*, organizzazioni attive nel modo dell'IT security). In particolare si è fatto riferimento alla documentazione di US-CERT, CERT Coordination Centre, Symantec, Sophos, RSA, TrendMicro. Per quanto riguarda lo scenario italiano le informazioni sono state prevalentemente estratte dallo studio pubblicato nel 2009 dall'OAI (Osservatorio Attacchi Informatici).

7.1 Trend significativi nel panorama degli attacchi informatici

Negli ultimi anni sono stati documentati incrementi non solo negli attacchi ai siti web, ma anche nell'utilizzo di nuovi exploit e di toolkit per la creazione di malware. Nel seguito sono richiamati alcuni esempi significativi di vettori di attacchi (attacco ai client, malware, botnet) che potrebbero anche essere utilizzati contro l'infrastruttura o i componenti di supporto del FSE.

Attacchi verso componenti applicative dei Client

A partire dal 2009 sono stati rilevati un numero crescente di exploit nei confronti dei client che utilizzano contenuti estesi. Questa circostanza è dovuta anche al fatto che si tratta di applicazioni molto diffuse al mondo, che le rendono un bersaglio appetibile per la criminalità cibernetica.

Malware

Un altro elemento significativo nello spettro delle minacce è l'evoluzione dei software "Troiani". Questi oggetti sono ormai notevolmente sofisticati, utilizzando tecniche avanzate di rootkit per nascondersi sui sistemi aggrediti, eludere o disabilitare i sistemi antivirus e sempre più spesso, agganciarsi alle reti di botnet. Ad esempio i malware appartenenti alla famiglia Silentbanker (apparsi nel 2008) possono monitorare, in modo invisibile agli utenti, le transazioni finanziarie, dirottando i dati degli utenti verso siti internet di raccolta. L'uso coordinato dei client infettati ha prodotto la nascita delle Botnet.

Botnet

Le Botnet sono diventate delle vere infrastrutture informatiche a supporto di attività illegali, dallo spionaggio elettronico alla gestione di attacchi DOS distribuiti. La possibilità di gestire da remoto migliaia di sistemi compromessi permette alla criminalità informatica di colpire anche infrastrutture informatiche ben strutturate e protette (si citano per esempio gli attacchi alle reti governative del Vietnam e di grandi service provider (Google) nel 2010).

Nel seguito sono riportati alcuni dati inerenti la diffusione delle principali attività illecite mappate per area geografica. *(Fonte: Symantec Intelligence Report 2009).*

Overall Rank 2009	2008	Country	Percentage 2009	2008	2009 Activity Rank Malicious Code	Spam Zombies	Phishing Hosts	Bots	Attack Origin
1	1	United States	19%	23%	1	6	1	1	1
2	2	China	8%	9%	3	8	6	2	2
3	5	Brazil	6%	4%	5	1	12	3	6
4	3	Germany	5%	6%	21	7	2	5	3
5	11	India	4%	3%	2	3	21	20	18
6	4	United Kingdom	3%	5%	4	19	7	14	4
7	12	Russia	3%	2%	12	2	5	19	10
8	10	Poland	3%	3%	23	4	8	8	17
9	7	Italy	3%	3%	16	9	18	6	8
10	6	Spain	3%	4%	14	11	11	7	9

Il caso italiano

Esistono pochi studi relativi alla situazione degli attacchi ai sistemi informativi nel panorama nazionale. Uno dei più significativi è stato pubblicato in un report dell'**Osservatorio sugli Attacchi Informatici in Italia** (rif. *http://www.malabo-advisoring.it*). Sulla base di una survey effettuata negli ultimi due anni su un campione rappresentativo di CIO/CSO/CISO, l'Osservatorio ha elaborato una credibile descrizione dello stato degli attacchi informatici nel nostro paese.

Nel seguito si riportano alcuni dei risultati più significativi; per le informazioni complete si veda il report della Fonte.

1) Diffusione attacchi per tipologia

TIPOLOGIA	%
Utilizzo di Malware (sia su client che su server)	84%
Attacchi di Phishing e Social Engineering	58%
Furto di apparati informatici	50%
Attacchi alle reti e al DNS	42%
Accesso e uso non autorizzato ai sistemi informatici	34%

2) Tecniche e strumenti di sicurezza adottati

STRUMENTI E METODOLOGIE di PROTEZIONE	%
Antivirus/Antispyware	95%
Firewall e DMZ	85%
Identificazione con userid/password	84%
VPN	79%
Sistemi di autorizzazione	77%

Gli attacchi ai sistemi informatici sanitari

Un recente rapporto pubblicato dalla Javelin Strategy & Research **(fonte: RSA Fraud Report 2010)** ha evidenziato come le frodi derivanti dall'esposizione di documenti medici ed informazioni personali sulla salute, siano diventate un business in piena espansione per i criminali informatici.
Nel rapporto si evidenzia, ad esempio, come le frodi derivanti da accesso illecito ai dati sanitari siano aumentate dal 3% nel 2008 al 7% nel 2009. Un aspetto interessante da sottolineare è che l'obiettivo della criminalità informatica nel settore sanitario non è solo il furto dei dati personali per commettere furti di identità. Lo studio ha dimostrato come i criminali siano stati in grado di sfruttare le informazioni trafugate dalle cartelle cliniche per commettere atti illegali di varia natura, oltre al furto di identità.

Infatti, con l'accesso ad informazioni relative ad esempio alle carte di credito, un truffatore può effettuare specifici tipi di frode, ma con l'abilitazione indebita ai set di informazioni più completi, come quelli presenti nei FSE, i tipi di truffa che possono essere commessi sono assai più differenziati. Questo è uno dei motivi per cui le organizzazioni sanitarie stanno diventando un target privilegiato fra i criminali informatici.

Ad esempio uno dei modi in cui viene perpetrata una frode sanitaria è presentando false documentazioni agli assicuratori e alle agenzie pubbliche che forniscono servizi sanitari. Accedendo indebitamente ai dati contenuti all'interno di cartelle cliniche elettroniche, un criminale informatico può avvalersi di tali informazioni per fatturare servizi che non sono mai stati resi.

I cittadini possono quindi essere danneggiati in molti modi a causa della divulgazione o violazione della propria cartella clinica o fascicolo sanitario. In primo luogo, a causa della completezza dei dati disponibili nella documentazione clinica, i cybercriminali possono commettere furti di identità tradizionali, come l'apertura di conti correnti a nome di una persona. Inoltre gli interessati potrebbero essere coinvolti in indagini penali per abuso di prestazioni mediche (es. acquisti di farmaci) effettuate a loro insaputa, oppure essere ricattati con la minaccia di vedere diffusi dati sensibili riguardanti la propria salute o situazione familiare.

Nei prossimi paragrafi vengono presentati alcuni scenari di attacco ad una ipotetica infrastruttura di gestione di un FSE. Gli scenari ipotizzati, descritti utilizzando una consolidata metodologia di analisi dei rischi, fanno riferimento ad azioni deliberate volte a trafugare, alterare o rendere indisponibili i dati sanitari contenuti nel FSE.

Descrizione qualitativa di alcune tipologie di attacco/minacce sui sistemi FSE

Per l'identificazione e la produzione di scenari di attacco si è scelto di partire dall'elenco di minacce riconosciute dalla metodologia di analisi del rischio MAGERIT e ci si è focalizzati sul sottoinsieme di quelle relative agli **attacchi intenzionali.**

Si sono volutamente tralasciati i seguenti gruppi di minacce:

- eventi di origine industriale;
- errori e avarie non intenzionali;
- eventi naturali.

Partendo dalle minacce di tipo **attacchi intenzionali**, si identificano tre possibili modalità di attacco sui dati FSE, identificabili come segue:

1. accesso illecito ai dati[1];
2. modifica / eliminazione / corruzione dei dati[2];
3. Denial of service[3].

Per ognuna delle modalità di attacco elencate, specifiche componenti del FSE sono coinvolte o potenzialmente vulnerabili e più precisamente:

Modalità di attacco	Componenti FSE coinvolte o vulnerabili
Accesso illecito ai dati	Archivi periferici (contenenti i dossier sanitari) Sistema centrale di autorizzazione / indicizzazione Sistema di accesso dell'utente proprietario dei dati Sistema di accesso dei soggetti titolati alla consultazione Sistema "di emergenza" per lo sblocco dell'accesso a tutti i dati
Modifica / eliminazione dei dati	Archivi periferici (contenenti i dossier sanitari) Forzatura del sistema di oscuramento dati fornito all'utente
Denial of service	Archivi periferici (contenenti i dossier sanitari) Sistema centrale di autorizzazione / indicizzazione Sistema di accesso dei soggetti titolati alla consultazione

Per ognuna delle tipologie di attacco individuate vengono ora descritti alcuni scenari di attacco ritenuti più probabili o significativi. Si tenga presente che alcune delle minacce rappresentate nel seguito possono venir abbattute o meno in conseguenza dell'utilizzo di diversi tipi di approcci tecnologici nella realizzazione del FSE (es. utilizzo per l'autenticazione di carte con microchip piuttosto che magnetiche, etc.).

[1] (Minacce MAGERIT coinvolte: "Attacchi intenzionali" numero 6, 7, 9, 11, 12, 16, 19, 25).
[2] (Minacce MAGERIT coinvolte: "Attacchi intenzionali" numero 7, 11, 15, 16, 17, 18, 26).
[3] (Minacce MAGERIT coinvolte: "Attacchi intenzionali" numero 7, 24).

Struttura dei successivi paragrafi

Paragrafo	Descrizione
Impatto	Indica quali delle dimensioni Disponibilità, Integrità e Riservatezza possono venire compromesse dalla minaccia, in relazione anche alla tipologia di attacco in analisi (Accesso illecito ai dati, Modifica/eliminazione/corruzione dei dati, Denial of service).
Causa	Descrive l'azione scatenante (o iniziale) di attuazione della minaccia.
Modalità	Propone uno o più esempi di come la minaccia possa venir attuata.
Conseguenza	Descrive le conseguenze dell'attuazione della minaccia e fornisce un esempio circa quali dati possano venir compromessi ed in che modo.

Accesso illecito ai dati

Furto / clonazione / guessing delle credenziali utente

Impatto

- sulla disponibilità dei dati: nessuno;
- sull'integrità: nessuno;
- sulla riservatezza: alto.

Causa

Appropriazione da parte di uno o più terzi delle credenziali di accesso appartenenti al proprietario dei dati (il paziente).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono molteplici:

- furto della tessera e guessing/ritrovamento del codice di accesso;
- copia delle credenziali durante l'utilizzo in dispositivi automatici (es. "totem" come quelli utilizzati per il pagamento del ticket);
- copia delle credenziali durante l'utilizzo presso un soggetto ad abilitato a consultare (es. farmacia).

Conseguenza

Tramite le credenziali utente è possibile accedere a tutti i dati appartenenti al paziente stesso, sebbene senza la possibilità di modificarli.
Nel presente scenario i dati medici del paziente vengono prelevati e quindi resi pubblici oppure utilizzati, insieme a quelli di altri pazienti, per studi o ricerche.

Utilizzo illecito delle credenziali speciali per accesso d'emergenza (Pronto Soccorso)

Impatto

- sulla disponibilità dei dati: nessuno;
- sull'integrità: basso;
- sulla riservatezza: alto.

Causa

Appropriazione da parte di uno o più terzi delle credenziali di accesso appartenenti a un ente abilitato ad utilizzare l'accesso d'emergenza ai dati, accesso che ignora le limitazioni di visualizzazione eventualmente imposte dal paziente (es. Pronto Soccorso).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono anche in questo caso molteplici:

- furto delle credenziali fisiche dal luogo ove esse sono custodite;
- consegna/duplicazione delle credenziali da parte di risorse autorizzate al loro utilizzo;
- copia delle credenziali durante il loro utilizzo tramite sistemi informatici manomessi in precedenza.

Conseguenza

Tramite le credenziali di emergenza è possibile accedere a tutti i dati appartenenti a qualsiasi paziente registrato nel FSE.
In base agli aspetti tecnici di realizzazione del FSE stesso, potrebbe essere altresì possibile l'inserimento di nuove informazioni nel dossier conservato localmente presso l'ente coinvolto.
Nel presente scenario i dati medici del paziente vengono prelevati e quindi resi pubblici oppure utilizzati, insieme a quelli di altri pazienti, per studi o ricerche. L'eventuale possibilità di inserimenti di dati nel dossier locale non è, in questo caso, considerata minaccia grave in quanto facilmente riportabili alle condizioni precedenti.

Furto delle credenziali di accesso / forzatura dell'accesso amministrativo a db periferico (Dossier)

Impatto:

- sulla disponibilità dei dati: medio;
- sull'integrità: alto;
- sulla riservatezza: alto.

Causa

Appropriazione da parte di uno o più terzi delle credenziali di accesso amministrativo legate ad un archivio periferico (cioè il database presso i quali si conservano i dossier sanitari afferenti ad una specifica struttura).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono anche in questo caso molteplici:

- furto delle credenziali qualora conservate in forma tangibile;
- consegna/duplicazione delle credenziali da parte di risorse autorizzate al loro utilizzo;
- guessing di credenziali protette con password deboli.

Conseguenza

Tramite le credenziali amministrative è possibile effettuare qualsiasi operazione **sul database locale dei dossier.**
A livello di consultazione è possibile quindi trafugare tutti i dossier conservati localmente e diffonderli a soggetti interessati (sebbene l'accesso all'intero fascicolo, descritto in precedenza, fornirebbe dati di gran lunga più completi e numerosi).

Forzatura dell'accesso al sistema centrale di autorizzazione / indicizzazione

Impatto:

- sulla disponibilità dei dati: alto;
- sull'integrità: alto;
- sulla riservatezza: alto.

Causa

Forzatura dell'accesso o appropriazione da parte di uno o più terzi delle credenziali di accesso amministrativo legate al sistema centrale di autorizzazione/indicizzazione (cioè il database presso il quale si conservano tutti i "puntatori" ai dati conservati sui dossier e dove si conservano le credenziali di tutti gli utilizzatori).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono anche in questo caso molteplici:

- furto delle credenziali qualora conservate in forma tangibile;
- consegna/duplicazione delle credenziali da parte di risorse autorizzate al loro utilizzo;
- guessing di credenziali protette con password deboli.

La forzatura dell'accesso, invece, può avvenire in conseguenza di vulnerabilità del software, mancati aggiornamenti di sicurezza, configurazione non sufficientemente robusta dei sistemi che ospitano il sistema centrale, etc.

Conseguenza

Ottenuto l'accesso al sistema centrale è possibile accedere ai dati conservati presso uno qualsiasi dei sistemi periferici, in virtù del fatto che è il sistema, centrale a gestire le autorizzazioni e i livelli di privilegio.
Si noti che in base alle caratteristiche ed agli aspetti progettuali e tecnologici dell'intero sistema, diversi livelli di accesso ai dati periferici possono essere ottenuti, dalla cognizione della "mappa dei collegamenti" riferiti ad ogni individuo ma senza specifico accesso ai dati fino all'accesso completo a tutte le informazioni contenute negli FSE di ognuno sfruttando le autorizzazioni custodite nel sistema centrale.

Modifica / eliminazione / corruzione dei dati

Furto delle credenziali di accesso / forzatura dell'accesso amministrativo a db periferico (Dossier)

Impatto:

- sulla disponibilità dei dati: medio;
- sull'integrità: alto;
- sulla riservatezza: alto.

Causa

Appropriazione da parte di uno o più terzi delle credenziali di accesso amministrativo legate ad un archivio periferico (cioè il database presso i quali si conservano i dossier sanitari afferenti ad una specifica struttura).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono anche in questo caso molteplici:

- furto delle credenziali qualora conservate in forma tangibile;
- consegna/duplicazione delle credenziali da parte di risorse autorizzate al loro utilizzo;
- guessing di credenziali protette con password deboli.

Conseguenza

Tramite le credenziali amministrative è possibile effettuare qualsiasi operazione **sul database locale dei dossier.**
Nello scenario descritto si ipotizza la cancellazione o la manomissione di tutti i dossier presenti localmente e/o la manomissione dei parametri operativi del database in modo da renderlo inutilizzabile per il maggior tempo possibile.
Nell'ipotesi che i backup dei dati e delle configurazioni non siano effettuati, oppure nel caso in cui essi siano in qualche modo accessibili da chi ha le credenziali amministrative e quindi manomissibili a loro volta, il danno di disponibilità ed integrità risulterebbe ancora maggiore.
Si noti comunque che il danno descritto dal presente scenario sarebbe limitato unicamente alla porzione di dossier conservati nella struttura locale.

Forzatura dell'accesso al sistema centrale di autorizzazione / indicizzazione

Impatto:

- sulla disponibilità dei dati: alto;
- sull'integrità: alto;
- sulla riservatezza: alto.

Causa

Appropriazione da parte di uno o più terzi delle credenziali di accesso amministrativo legate al sistema centrale di autorizzazione/indicizzazione (cioè il database presso il quale si conservano tutti i "puntatori" ai dati conservati sui dossier e dove si conservano le credenziali di tutti gli utilizzatori).

Modalità

Le modalità tramite le quali può avvenire l'appropriazione delle credenziali sono anche in questo caso molteplici:

- furto delle credenziali qualora conservate in forma tangibile;
- consegna/duplicazione delle credenziali da parte di risorse autorizzate al loro utilizzo;
- guessing di credenziali protette con password deboli.

Conseguenza

Tramite le credenziali amministrative è possibile effettuare qualsiasi operazione **sui sistemi centrali precedentemente descritti.**
In questo scenario si ipotizza la cancellazione o la manomissione dei sistemi al fine di rendere indisponibili i sistemi di autenticazione a tutta l'infrastruttura FSE e/o rendere indisponibili i "puntatori" ai dati periferici rendendo di fatto inutilizzabile l'intera infrastruttura.
Anche in questo caso la presenza o meno di backup e la loro facile manomissione possono cambiare notevolmente l'impatto a medio/lungo termine di quanto descritto nello scenario di attacco.

Denial of service

Attacco DoS sul sistema centrale di autorizzazione/indicizzazione

Impatto:

- sulla disponibilità dei dati: alto;
- sull'integrità: nessuno;
- sulla riservatezza: nessuno.

Causa

Attacco tecnologico diretto alle componenti centrali del sistema di autorizzazione / indicizzazione (contenente i "puntatori" ai dati) al fine impedirne la comunicazione con le restanti componenti periferiche.

Modalità

L'attacco può avvenire sfruttando, ad esempio, vulnerabilità tecnologiche specifiche dell'infrastruttura centrale non precedentemente rilevate e corrette o colpendo l'infrastruttura di comunicazione dei dati oppure colpendo le infrastrutture di supporto del sistema centrale.

Conseguenza

L'indisponibilità del sistema centrale rende di fatto inoperativa l'intero FSE, rendendo infatti impossibili le attività di:

- autenticazione degli utenti, di qualsiasi tipologia;
- consultazione di qualsiasi dossier periferico;
- modifica dei privilegi di accesso ai dati o delle caratteristiche di oscuramento.

Attacco DoS su un sistema periferico

Impatto:

- sulla disponibilità dei dati: medio;
- sull'integrità: basso;
- sulla riservatezza: basso.

Causa

Attacco tecnologico diretto ad una o più componenti periferiche (dossier) del FSE, al fine di impedirne la comunicazione con il sistema centrale di autenticazione e indicizzazione.

Modalità

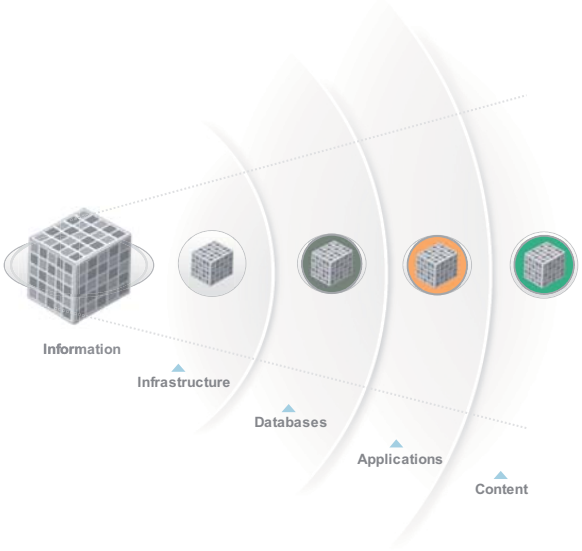
L'attacco può avvenire sfruttando, ad esempio, vulnerabilità tecnologiche specifiche dell'infrastruttura periferica non precedentemente rilevate e corrette dai suoi gestori, oppure colpendo l'infrastruttura di comunicazione dei dati oppure colpendo le infrastrutture di supporto ai sistemi.

Conseguenza

L'indisponibilità di un dossier priva potenzialmente il sistema FSE di una porzione di dati, pur non minandone in alcun modo il funzionamento.
Le conseguenza di un attacco di questo tipo insistono unicamente sui dati conservati nel dossier periferico, rendendone impossibile l'interazione con le componenti esterne del sistema, interazioni che tipicamente si identificano con la consultazione dei dati.
Il FSE di un paziente che abbia tutti o una parte dei propri dati conservati nello specifico dossier periferico ospitato nella struttura sottoposta ad attacco è reso indisponibile sino al termine dell'attacco stesso.

Componenti Tecnologiche

Oracle Security Inside Out



Database Security
- Encryption and Masking
- Privileged User Controls
- Multi-Factor Authorization
- Activity Monitoring and Audit
- Secure Configuration

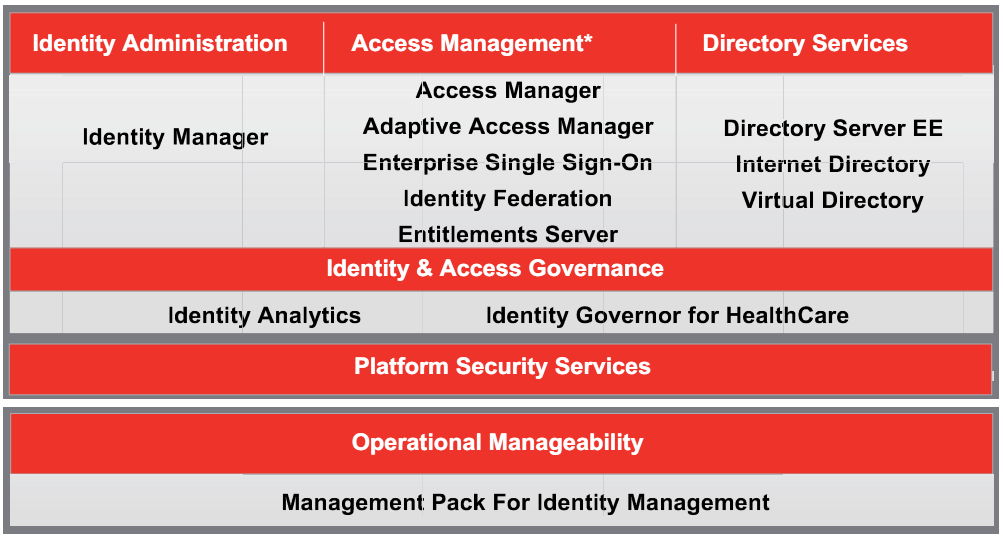
Identity Management
- User Provisioning
- Role Management
- Entitlements Management
- Risk-Based Access Control
- Virtual Directories

Information Rights Management
- Document-level access control
- All copies, regardless of location (even beyond the firewall)
- Auditing and revocation

INFORMATION RIGHT MANAGEMENT

Oracle Information Rights Management	Soluzione per la gestione della sicurezza dei documenti digitali.	Oracle Information Rights Management 11g è una nuova forma di tecnologia per la sicurezza delle informazioni che protegge e traccia le informazioni digitali sensibili ovunque siano utilizzate o conservate. Oracle Information Rights Management utilizza la crittografia per estendere la protezione delle informazioni al di là del repository - per ogni copia delle informazioni più sensibili di un'organizzazione, ovunque sia conservata e utilizzata: sul desktop dell'utente finale, via laptop o dispositivi mobili, in altri repository, all'interno o all'esterno del firewall aziendale. *http://www.oracle.com/us/products/middleware/identity-management/information-rights-mgmt/index.html*

Oracle's Identity Management Portfolio



***Access Management includes Oracle OpenSSO STS and Oracle OpenSSO Fedlet**

IDENTITY MANAGEMENT		
Oracle Identity Manager	Amministrazione delle identità digitali	Oracle Identity Manager 11g è la soluzione di nuova generazione per la gestione dei ruoli e degli utenti che automatizza il processo di creazione, aggiornamento e cancellazione sia degli account utente che dei diritti di accesso a livello di attributo su tutte le risorse aziendali. Con Oracle Identity Manager 11g, le organizzazioni sperimentano performance superiori, scalabilità senza paragoni e un'estrema facilità d'uso. *http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-manager/index.html*
Oracle Access Manager	Controllo degli accessi alle applicazioni WEB (Web SSO)	Oracle Access Manager permette agli utenti delle applicazioni o dei sistemi IT di autenticarsi una sola volta e di avere accesso a una vasta gamma di risorse IT. Oracle Access Manager un sistema di controllo dell'accesso condiviso da tutte le applicazioni web based. Il risultato è una soluzione di single sign-on (SSO) centralizzata e automatizzata per la gestione dei diritti di accesso alle informazioni attraverso l'intera infrastruttura IT. *http://www.oracle.com/us/products/middleware/identity-management/oracle-access-manager/index.html*
Oracle Adaptive Access Manager	Autenticazione forte e prevenzione delle frodi per proteggere le applicazioni Web	Oracle Adaptive Access Manager 11g fornisce alle imprese ed ai loro clienti ullivello superiore di protezione attraverso meccanismi di autenticazione forte multi-factor facile da implementare grazie all'impiego di token virtuali e una prevenzione delle frodi proattiva ed in tempo reale. *http://www.oracle.com/us/products/middleware/identity-management/oracle-ada-access-mgr/index.html*

Oracle Enterprise Single Sign-On	Controllo degli accessi alle applicazioni Terminal based, Client server e web (ESSO)	Oracle Enterprise Single Sign-On Suite offre agli utenti un servizio unificato di sign-on e di autenticazione per tutte le loro risorse aziendali, incluse applicazioni desktop, client-server, proprietarie o basate su mainframe. Anche se gli utenti viaggiano o condividono posti di lavoro, possono beneficiare della flessibilità di un unico log-on, che elimina la necessità di molteplici nomi utente e password e consente di applicare password e policy di autenticazione forte. *http://www.oracle.com/us/products/middleware/identity-management/oracle-enterprise-sso/index.html*
Oracle Identity Federation	Access Federation	Oracle Identity Federation 11g fornisce un server di federazione multi-protocollo autoconsistente e flessibile che può essere rapidamente implementato con i sistemi di gestione delle identità e degli accessi esistenti. Grazie all'utilizzo dei principali protocolli standard, garantisce l'interoperabilità consentendo di condividere in modo sicuro le identità tra fornitori, clienti e partner commerciali senza l'aumento dei costi necessari per la gestione,manutenzione e amministrazione di identità e credenziali aggiuntive. *http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-federation/index.html*
Oracle Entitlement Server	Motore di gestione delle autorizzazioni per applicazioni enterprise	Oracle Entitlements Server esternalizza e centralizza i criteri di autorizzazione a grana fine per le applicazioni aziendali e servizi web. Questo risultato è ottenuto attraverso criteri di autorizzazione completi, riutilizzabili e pienamente verificabili ed un semplice modello di amministrazione facile da utilizzare. *http://www.oracle.com/us/products/middleware/identity-management/oracle-entitlements-server/index.html*
Oracle Web Services Manager	Tool per la definizione e l'implementazione della sicurezza nei Web Services	Oracle Web Services Manager è un'applicazione J2EE progettata per definire e implementare la sicurezza dei servizi Web in ambienti eterogenei, offre gli strumenti per la gestione dei servizi Web sulla base di livelli di servizio e consente all'utente di monitorare l'attività runtime attraverso grafici di facile consultazione. *http://www.oracle.com/us/products/middleware/identity-management/oracle-web-services-mgr/index.html*
Oracle Directory Services Plus	Un package che comprende tre soluzioni di Directory Services	Oracle Directory Services Plus è l'unica soluzione integrata che fornisce un insieme completo di soluzioni di directory ad alte prestazioni per le aziende. Oracle Directory Services Plus è un pacchetto unico che comprende: * Oracle Directory Server Enterprise Edition - Il leader del mercato dei directory server che fornisce servizi LDAP ad alte prestazioni, ideale per ambienti eterogenei. * Oracle Internet Directory – Directory conforme a LDAP costruito sul Database Oracle ad alte prestazioni e profondamente integrato con le applicazioni ed il middleware Oracle, ideale per gli ambienti Oracle. * Oracle Virtual Directory - Aggrega virtualmente le informazioni di identità da più fonti e presenta una visione unificata in tempo reale, eliminando la necessità di sincronizzare o spostare i dati di identità. *http://www.oracle.com/us/products/middleware/identity-management/oracle-directory-services/index.html*

Oracle Identity Analytics	Governance delle identità digitali	La transizione della gestione delle identità da un problema dell'IT a un abilitatore del core business è supportata dall'analisi delle identità. Oracle Identity Analytics 11g offre questa intelligenza con una ricca analisi delle identità, cruscotti e funzionalità avanzate di conformità, che controllano, analizzano, revisionano e regolano l'accesso degli utenti per mitigare il rischio, costruire la trasparenza e soddisfare requisiti di conformità. L'integrazione di Oracle Identity Analytics 11g con Oracle Identity Manager 11g garantisce l'attivazione di azioni correttive automatiche, compresi i controlli preventivi e rilevatori di segregazione delle responsabilità. *http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-analytics/index.html*
Oracle Governor for HealthCare	Gestione globale della sicurezza per dati e applicazioni nel Mercato Sanità	Oracle Security Governor è una soluzione unica e completa di gestione della sicurezza che aiuta le organizzazioni sanitarie con un controllo proattivo e una rilevazione a posteriori delle violazioni di sicurezza e della privacy. La rilevazione a posteriori consente la tempestiva segnalazione di sospette violazioni che potrebbero avere avuto luogo nel passato. Con il controllo proattivo, tali violazioni possono anche essere evitate in tempo reale. Oracle Security Governor offre una completa visibilità dell'accesso ai dati e alle applicazioni e delle attività sospette attraverso il monitoraggio proattivo dei rischi, analisi e reporting, tenendo conto di errori umani, errori di processo, accessi non autorizzati dall'interno, attività sospette e possibili furti di identità. Questa capacità di monitoraggio del rischio aiuta le organizzazioni a rispondere agli odierni stringenti requisiti di conformità in ambito sanitario. http://www.oracle.com/us/products/middleware/identity-management/security-governor-healthcare-168615.html
Oracle Management Pack for Identity Management	Ambiente per la gestione delle soluzioni Oracle di Identity Management	Oracle Management Pack for Identity Management gestisce in modo proattivo prestazioni, disponibilità e livelli di servizio per i servizi di identità, fornendo una soluzione di gestione enterprise completa e integrata per la suite di prodotti Oracle Identity Management. http://www.oracle.com/us/products/middleware/identity-management/oracle-mgmt-pack-for-im/index.html

Database Defense-in-Depth

Encryption and Masking
- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control
- Oracle Database Vault
- Enterprise User Security
- Oracle Label Security

Auditing and Monitoring
- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Blocking and Logging
- Oracle Database Firewall

DATABASE SECURITY		
Oracle Advanced Security	Crittografia dei dati nel database e dei dati in transito sulla rete	Oracle Advanced Security aiuta le organizzazioni a rispettare gli obblighi relativi a privacy e normative quali Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), nonché numerose leggi di notifica delle violazioni di sicurezza. Con Oracle Advanced Security, i clienti possono trasparentemente crittografare tutti i dati delle applicazioni o specifiche colonne con dati sensibili, quali numeri di carta di credito, numeri di sicurezza sociale, o informazioni personali. Crittografando i dati presenti nel database, oppure ogni volta che lasciano il database per spostarsi in rete o per un backup, Oracle Advanced Security fornisce la soluzione più conveniente per la protezione completa dei dati. http://www.oracle.com/us/products/database/options/advanced-security/index.html
Oracle Secure Backup	Backup sicuro	Oracle Secure Backup con Oracle Database 11g offre elevate prestazioni per il backup su rete per Oracle Database e file systems per piattaforme Linux, UNIX e Windows con il supporto per oltre 200 differenti dispositivi a nastro dei fornitori leader. Il modulo Oracle Secure Backup Cloud integra le strategie di backup esistenti e può funzionare indipendentemente dall'offerta Oracle Secure Backup tape management. http://www.oracle.com/us/products/database/secure-backup/index.html

Oracle Data Masking	Mascheramento dei dati sensibili per ambienti di test e sviluppo	Oracle Data Masking Pack per Enterprise Manager aiuta le aziende a rispettare i requisiti di privacy e protezione dei dati come la Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), nonché numerose leggi che limitano l'uso dei dati relativi ai clienti. Con Oracle Data Masking, informazioni sensibili come numeri di carta di credito o di sicurezza sociale possono essere sostituiti con valori realistici, consentendo che i dati di produzione siano utilizzati senza rischi per lo sviluppo, il test, o la condivisione con partner esterni per altri scopi non di produzione. Oracle Data Masking utilizza una libreria di modelli e di regole per trasformare i dati in modo coerente al fine di mantenere l'integrità referenziale per le applicazioni. http://www.oracle.com/us/products/database/data-masking-161222.html
Oracle Database Vault	Protezione dei dati dagli accessi di utenze privilegiate	Oracle Database Vault consente alle organizzazioni di indirizzare i requisiti delle regolamentazioni e di aumentare la sicurezza delle applicazioni esistenti. Con Oracle Database Vault, le organizzazioni possono proteggere proattivamente i dati delle applicazioni, memorizzati nel database Oracle, dall'accesso di utenti privilegiati del database. I dati delle applicazioni possono essere ulteriormente protetti utilizzando le politiche multi fattore di Oracle Database Vault che controllano l'accesso sulla base di fattori predefiniti quali l'ora del giorno, l'indirizzo IP, il nome dell'applicazione e il metodo di autenticazione, prevenendo accessi ad-hoc non autorizzati e by-pass delle applicazioni. http://www.oracle.com/us/products/database/options/database-vault/index.html
Enterprise User Security	Gestione centralizzata delle utenze	Enterprise User Security, una funzionalità di Oracle Database Enterprise Edition, sfruttando Oracle Directory Services e in un directory LDAP. Enterprise User Security riduce i costi di amministrazione, aumenta la sicurezza e migliora la conformità attraverso una gestione centralizzata delle utenze del database un provisioning e de-provisioning centralizzato degli utenti del database, una gestione centralizzata della password e un self-service per la password reset euna gestione centralizzata delle autorizzazioni utilizzando ruoli di database globali. Oracle Virtual Directory (OVD), un servizio di virtualizzazione del directory (non un repository) incluso in Oracle Directory Services, consente alle aziende di implementare Enterprise User Security sfruttando l'infrastruttura di directory esistente, in modo da ridurre ulteriormente il costo totale. http://www.oracle.com/technetwork/database/security/index-099042.html

Oracle Label Security	Classificazione multi livello dei dati	Oracle Label Security è uno strumento potente e facile da usare per la classificazione dei dati e per favorire l'accesso ai dati in base alla loro classificazione. Progettato per soddisfare le esigenze del settore pubblico per la sicurezza multi-livello e di controllo di accesso obbligatorio, Oracle Label Security fornisce un ambiente flessibile che organizzazioni, sia pubbliche che private, possono utilizzare per gestire l'accesso ai dati sulla base del "need to know" al fine di proteggere la riservatezza dei dati e di ottenere la conformità normativa. http://www.oracle.com/us/products/database/options/label-security/index.html
Oracle Audit Vault	Raccolta, consolidamento e analisi di dati di Audit	Oracle Audit Vault riduce i costi per la conformità e il rischio di minacce interne grazie all'automazione della raccolta e del consolidamento dei dati di audit. Audit Vault fornisce un warehouse sicuro e altamente scalabile, permettendo rapportistica semplificata, analisi e rilevamento delle minacce sui dati di audit. Inoltre, le impostazioni di controllo del database sono gestiti a livello centrale e monitorati direttamente da Audit Vault, riducendo i costi della sicurezza. Con Oracle Audit Vault, le organizzazioni hanno gli strumenti per applicare le policy sulla privacy, la protezione contro le minacce interne, e indirizzare i requisiti normativi quali la Sarbanes-Oxley e la PCI-DSS. http://www.oracle.com/us/products/database/audit-vault-066522.html
Oracle Database Configuration Management	Tool per la Gestione dei Database	Oracle Configuration Management Pack for Database Oracle supporta i database Oracle ed i sottostanti server e sistemi operativi, permette un esaustivo controllo delle configurazioni IT attraverso un'ampia e profonda copertura di elementi di configurazione accoppiata a potenti capacità di automazione, leader del settore. Oracle Configuration Management Pack for Database Oracle è parte di Oracle Enterprise Manager 11g, una soluzione di gestione IT che mette insieme soluzioni specifiche per la gestione dello stack Oracle e soluzioni complete per la gestione di ambienti IT eterogenei tra cui i sistemi operativi non-Oracle, host, database, middleware, sicurezza, rete e tecnologie di storage, il tutto all'interno di una singola console di gestione. http://www.oracle.com/oms/enterprisemanager11g/index.html http://www.oracle.com/us/products/enterprise-manager/database-management/index.html

Oracle Total Recall	Archiviazione di dati storici	Oracle Total Recall è un'opzione di Oracle Database 11g Enterprise Edition che consente alle aziende di storicizzare i loro dati in database sicuri e a prova di manomissione, mantenendoli accessibili alle applicazioni esistenti. Oracle Total Recall offre una soluzione sicura, efficiente, facile da usare e trasparente alle applicazioni per l'archiviazione a lungo termine e la revisione dei dati storici. La gestione dei dati storici non sarà più essere un compito oneroso. http://www.oracle.com/us/products/database/options/total-recall/index.html
Oracle Database Firewall	Monitoraggio su rete delle attività verso il database	Oracle Database Firewall è la prima linea di difesa sia per database Oracle che non Oracle. Controlla l'attività del database in rete per prevenire in tempo reale l'accesso non autorizzato, le "SQL injections", le escalation di privilegio o di ruolo e altri attacchi esterni o interni. Basato su un'innovativa tecnologia che può ricondurre milioni di istruzioni SQL ad un piccolo numero di caratteristiche SQL, Oracle Database Firewall offre un'accuratezza senza pari, scalabilità e prestazioni. Il rafforzamento dei modelli di sicurezza positivi ("white list") e negativi ("black list") fornisce una protezione dalle minacce senza perdita di tempo e costosi falsi positivi. Oracle Database Firewall permette inoltre alle aziende di affrontare SOX, PCI-DSS, HIPAA/HITECH, ed altre disposizioni normative, senza modifiche alle applicazioni esistenti o ai database, e dimostrare la conformità attraverso molteplici report predefiniti e personalizzabili. http://www.oracle.com/us/products/database/database-firewall-160528.html

Norme e standard internazionali

9.1 Introduzione

La ISO 27799:2008 è uno standard di sicurezza informatica sviluppato dalla *International Organization for Standardization* (ISO). Il suo titolo è *Health informatics -- Information security management in health using ISO/IEC 27002.* Lo scopo di tale standard è fornire una guida per le organizzazioni sanitarie e a detentori di informazioni sanitarie personali su come proteggere le informazioni tramite la realizzazione di ISO/IEC 27002 con un taglio dedicato alla particolare natura del settore sanitario.

L'ISO 27799:2008 si applica alle informazioni sulla salute in tutti i loro aspetti:

- formato delle informazioni (scritto, registrazioni sonore, disegni, video e immagini mediche);
- supporto di memorizzazione utilizzato (carta, nastri, dispositivi elettronici di memorizzazione);
- mezzo di trasmissione utilizzato (lettera postale, fax, posta elettronica, reti di computer aziendale).

Con l'implementazione di questo standard internazionale, le strutture ed i e gestori delle informazioni sanitarie saranno in grado di garantire un livello minimo di requisiti di sicurezza adeguato alle circostanze della loro organizzazione al fine di assicurare la riservatezza, l'integrità e la disponibilità dei dati trattati.

Guardando oltre oceano, più in particolare negli Stati Uniti, dove la denuncia del furto informatico è obbligatoria e dove esistono da anni puntuali statistiche sulla sottrazione di dati informatici che dettagliano il mercato coinvolto, la tipologia di dato sottratto e le tecniche attuate ci troviamo in presenza di un quadro normativo articolato e completo, basato su:

- Health Insurance Portability and Accountability Act (HIPAA) Privacy Rules che disciplina l'uso e la divulgazione di determinate informazioni personali e sanitarie in possesso "degli enti interessati"
- Il sottotitolo D del Health Information Technology for Economic and Clinical Health Act (HITECH Act), affronta i problemi di privacy e sicurezza connessi con la trasmissione elettronica di informazioni sanitarie.
  Questo sottotitolo estende la Privacy and Security Provisions della HIPAA ai soci in affari degli enti considerati e introduce nuove norme per la segnalazione delle violazioni e i relativi risvolti di giustizia civile e penale

L'Unione Europea sta valutando un emendamento al Data Protection Directive (95/46/EC), recepito con diverse leggi nelle varie nazioni, per introdurre l'obbligatorietà della segnalazione per le violazioni dei dati elettronici.

Questa azione dovrebbe creare due effetti: dare consapevolezza del reale rischio corso dai dati sanitari individuali e aumentare la pressione su chi ha la responsabilità di proteggere tali dati.

9.2 Implicazioni della ISO 27002 nel settore Healthcare

Di seguito sono riportati i controlli della normativa ISO 27799 suddivisi in paragrafi, ognuno dei quali corrisponde ai gruppi di controlli stabiliti dall normativa stessa e derivanti dalla ISO 27002.

9.2.1. Information security Policy

Un documento di Politica relativo alla gestione della sicurezza delle informazioni è l'elemento cardine di qualsiasi ISMS (Information Security Management System) e si posiziona tipicamente all'apice del framework documentale relativo al Sistema di Gestione stesso. Nella particolare contesto di un ambiente di prestazione di servizi sanitari, il documento di Politica sulla sicurezza delle informazioni si arricchisce di ulteriori contenuti di spiccata inerenza all'ambiente sanitario stesso, tra i quali si annoverano i requisiti legali, contrattuali ed etici relativi alla protezione delle informazioni stesse.

Il delicato ambito nel quale la norma andrà ad inserirsi richiede un attento studio sugli argomenti che essa andrà a definire e che potranno spaziare dalle responsabilità etiche dello staff medico, alle modalità di accesso alle informazioni mediche, alla gestione dei protocolli di sicurezza rispetto alle priorità sanitarie, fino ai protocolli da applicare in caso di condivisione di alcune informazioni al di fuori della struttura in oggetto.

La revisione della Politica deve avvenire almeno annualmente, in accordo con quanto previsto dalla originaria norma ISO27001 e dovrà valutare in particolar modo gli aspetti legati al contesto sanitario.

9.2.2. Organizzazione della sicurezza delle informazioni

L'organizzazione della sicurezza delle informazioni rispecchia quanto già previsto per gli ISMS generici, tenendo tuttavia in considerazione le peculiari caratteristiche dei dati trattati che richiedono alcuni accorgimenti specifici, volti a:

- facilitare l'accesso ai dati da parte dei relativi proprietari, pur mantenendone alti livelli di riservatezza (anche attraverso Accordi di Riservatezza più stringenti di quelli normalmente richiesti da un ISMS);
- agevolare lo scambio di informazioni (nei limiti previsti) all'interno dell'organizzazione;
- garantire l'immediata accessibilità delle informazioni quando richieste;
- gestire in modo sicuro l'eventuale scambio di informazioni con terze parti incaricate di specifici servizi, tramite vincoli contrattuali, limitazione degli accessi, definizione di soglie di livello di servizio, reportistica periodica e accordi di auditing.

9.2.3. Gestione degli asset

Nel contesto in oggetto la tipologia di asset che maggiormente richiede attenzione è quella di tipo informativo. Al di là delle attività tipiche di gestione degli asset (assegnazione della responsabilità, della custodia, documentazione dei ruoli), particolare cautela deve essere spesa in questo caso nella loro classificazione.

La dimensione della riservatezza dell'informazione, in particolare, oltre a rispondere a specifici requisiti cogenti, può richiedere l'applicazione di ulteriori criteri restrittivi basati su ulteriori caratteristiche quali:

- la percezione soggettiva della confidenzialità in caso di informazioni inerenti la salute (in conseguenza della quale un'ulteriore restrizione nell'accesso a determinate informazioni può essere consigliata);
- il contesto all'interno del quale l'informazione è trattata (dettagli anagrafici trattati da un ospedale pubblico possono avere una criticità inferiore ad elenchi anagrafici trattati da una clinica specializzata in malattie specifiche);
- l'età dell'informazione stessa (con il passare degli anni informazioni ai tempi ritenute critiche possono aver visto diminuito il loro livello di riservatezza, al contrario di altre che possono averlo visto accresciuto).

9.2.4. Sicurezza legata alle risorse umane

In contesti delicati come quello dell'healthcare, attività quali le verifiche e lo screening precedente all'assunzione di una risorsa rivestono un ruolo di importanza non indifferente e non possono venir ignorati, tanto da rendere necessario, in alcune realtà di effettuare nuove verifiche sulla stessa risorsa qualora trascorra un lasso di tempo troppo lungo tra lo screening e l'effettiva entrata in ruolo.

Simili considerazioni sono legate alla cessazione dei rapporti di lavoro: di nuovo, la criticità delle informazioni trattate richiede che il rischio legato alle minacce di accesso non autorizzato sia ridotto al minimo possibile; ne consegue come, più che in altri contesti, la pronta ed immediata rimozione o blocco dei privilegi di accesso debba essere effettuata sulle risorse uscenti. Particolare attenzione, in questo caso, deve essere dedicata anche alle risorse temporanee, quali ad esempio studenti universitari, o al personale interno che a seguito di periodica rotazione dei ruoli ha necessità di accedere a informazioni diverse.

In ultima istanza, può essere utile gestire l'assegnazione degli incarichi talvolta anche su base geografica e più precisamente legata alla residenza delle risorse: spesso accade, infatti, che non si voglia dare accesso alle proprie informazioni riservate a vicini di casa, colleghi o parenti che lavorano in ambito sanitario; all'opposto può capitare che personale interno reputi a sua volta sconveniente lavorare o accedere ad informazioni appartenenti a tali parenti, vicini di casa o colleghi.

9.2.5. Sicurezza fisica ed ambientale

La definizione fisica dell'ambiente è tra gli elementi che maggiormente caratterizzano l'ambiente di erogazione di servizi sanitari:

- per la forte concentrazione di informazioni sensibili;
- per la presenza di strumenti ed apparati critici per l'incolumità dei pazienti;
- per la compresenza di addetti a diverso livello di clearance (personale medico e paramedico, inservienti) e pubblico (pazienti e relativi accompagnatori);
- per la particolare vulnerabilità dei pazienti a diverse minacce.

Queste considerazioni rendono particolarmente necessarie attente riflessioni nell'adottare i controlli relativi alla definizione delle aree di interdizione e dei controlli di accesso alle stesse, eventualmente rivedendo la disposizione degli strumenti e delle aree di attesa.

Le particolarità delle aree sensibili obbliga anche a promuovere la consapevolezza del personale impartendo istruzioni per operare con particolare discrezione e riservatezza in aree come corsie e accettazioni e ambulatori.

9.2.6. Gestione delle operazioni e delle comunicazioni

Per quanto riguarda gli aspetti di gestione delle operazione e delle comunicazioni le peculiarità dell'ambiente sanitario che vengono indirizzate dalla norma sono legate alla sensibilità del dato e comportano la necessità di particolare enfasi su alcuni aspetti:

- segregazione di compiti e responsabilità, per garantire la riservatezza e l'integrità dell'informazione;
- separazione degli ambienti di sviluppo e di esercizio, che in ambiente sanitario deve essere considerata indispensabile al fine di garantire la continuità delle attività di esercizio ed evitare accessi e modifiche inintezionali ai dati di produzione;
- criteri di accettazione e trasferimento in esercizio, che devono essere formalizzati ed adeguati ai rischi specifici dell'intervento evolutivo previsto, in considerazione delle gravi conseguenze che un'erronea elaborazione dei dati potrebbe provocare;
- misure per prevenire la disseminazione accidentale del dato, quali cifratura della messaggistica contenente dati sanitari personali, distruzione sicura dei supporti, protezione di dispositivi portatili o rimovibili.

Inoltre occorre sottolineare l'attenzione che lo standard pone alla ispezionabilità del sistema che può essere spesso chiamato ad essere di supporto ad inchieste giudiziare ed amministrative, rendendo quindi necessaria la raccolta e la conservazione sicura di log raccolti da sorgenti affidabili e sincronizzate.

9.2.7. Controllo degli accessi

Quando si considera il controllo accessi in ambito sanitario si devono prendere in carico gli aspetti operativi particolari quali:

- il numero di utenti che devono avere accesso al dato;
- la varietà dei profili degli utenti;
- le condizioni di particolare urgenza in cui spesso si svolgono gli accessi;
- la possibilità che il paziente non sia in grado di cooperare esprimendo il consenso.

Tra gli utenti deve essere considerato anche il paziente, che pur con un ruolo estremamente specializzato e limitato nelle modifiche, deve poter accedere ai suoi dati personali.

Lo standard ISO raccomanda la gestione dei privilegi di accesso tramite un modello RBAC che associ ai ruoli le funzionalità consentite ed agli utenti i pazienti in carico, modulando il rigore con l'agilità necessaria per fronteggiare le emergenze cliniche che possono presentarsi in un Pronto Soccorso.

L'autenticazione deve offrire garanzie di sicurezza all'altezza della sensibilità del dato e deve tenere in considerazione le condizioni operative di un reparto, le quali possono rendere estremamente inefficace l'autenticazione via password.

Per contemperare queste due esigenze lo standard suggerisce l'adozione della strong authentication.

9.2.8. Acquisizione, sviluppo e mantenimento dei sistemi informativi

In questo paragrafo vengono affrontati alcuni degli aspetti della normativa di maggior interesse in rapporto al Fascicolo Sanitario Elettronico.

Nell'erogazione dei servizi di assistenza un paziente può, per scelta o necessità di avvalersi delle cure di diversi enti o, nell'ambito di un medesimo ente attraversare diversi reparti, dando luogo a più registrazioni.

Un sistema deve essere in grado di fornire un'identificazione univoca del paziente e di riconciliare registrazioni multiple riferibili al medesimo utente nell'ambito di vari atti e di vari processi diagnostici e terapeutici.

Questo è uno dei pochi requisiti specificatamente introdotti dallo standard ISO 27999, ed è particolarmente complesso se si considerano le condizioni operative di un pronto soccorso, nelle quali può risultare piuttosto difficile garantire un livello adeguato di identificazione di un paziente.

Parallelamente all'identificazione certa del dato sanitario, è necessario garantire che la conservazione dei dettagli che rendono possibile tale identificazione sia limitata al tempo strettamente necessario. Questa precauzione è finalizzata a limitare la possibilità di compromettere dati sanitari sensibili ed è comune tanto alla legislazione quanto allo standard ISO.

Altro aspetto fondamentale è la validazione del dato di output. L'utilizzo del dato in un contesto clinico è critico per l'incolumità di un paziente e deve permetter all'utente (medico od operatore sanitario) di verificare con certezza che le informazioni fornite si riferiscano al paziente in trattamento e siano complete.

Il processo di sviluppo deve garantire che per test e collaudi non siano mai utilizzati dati sanitari personali reali, ricorrendo a test data set appositamente composti o a sistemi per il mascheramento e la trasformazione dei dati.

9.2.9. Gestione degli incidenti legati alla sicurezza delle informazioni

Un sistema informativo sanitario può essere coinvolto in incidenti che sono originati e conclusi nell'ambito del sistema informatico o in incidenti in cui il sistema informativo può avere registrato dati rilevanti per la ricostruzione degli eventi.

La particolarità nella gestione degli incidenti di sicurezza in ambito sanitario sta nell'attenzione che deve essere posta nel considerare gli effetti che l'incidente può avere sulla sfera personale del paziente sia in termini di privacy che di effetti negativi sul processo terapeutico.

Nei casi in cui si dovesse ravvisare una di queste condizioni lo standard raccomanda di informare il paziente degli incidenti che lo hanno riguardato.

Devono essere, inoltre, predisposti strumenti e processi:

- per analizzare alla luce dell'evento l'efficacia dei controlli predisposti e delle valutazioni del rischio ad essi sottesi;
- per raccogliere e custodire le prove necessari a successive inchieste giudiziarie ed amministrative relative ad abusi del sistema o a negligenze professionali.

9.2.10. Aspetti della gestione della continuità operativa legati alla sicurezza delle informazioni

La continuità operativa di un sistema informativo sanitario deve fronteggiare emergenze strettamente legate al funzionamento del sistema informativo insieme ad emergenze sanitarie.

Come tutti i sistemi *Safety Critical*, un sistema informativo sanitario deve rispondere a requisiti di continuità operativi particolarmente stringenti che richiedono predisposizioni tecniche ed organizzative molto accurate.

La pianificazione della continuità operativa deve armonizzarsi con i piani che fronteggiano emergenze sanitarie, perseguendo finalità spesso contrastanti quali:

- aumento del livello di supporto richiesto sui servizi prioritari;
- temporanea indisponibilità del personale tecnico disponibile;
- irregolarità nelle forniture;
- compromissione delle infrastrutture.

La complessità di tale piano richiede una particolare attenzione alle verifiche programmatiche che coinvolgano gli operatori sia per quanto concerne gli aspetti logici sia per quelli fisici.

9.2.11. Conformità

La legislazione vigente in Italia è ancora più rigorosa delle raccomandazioni dello standard ISO per quanto riguarda revisione periodica del piani e gestione del consenso.

Mappatura ISO 27001 - CobiT

Requisito Fascicolo Sanitario Elettronico e Dossier Sanitario (Linee guida in tema di Fascicolo sanitario elettronico (Fse) e di dossier sanitario - 16 luglio 2009 - *(G.U. n. 178 del 3 agosto 2009)* - Parte II: Le garanzie per l'interessato – Punto 10: misure di sicurezza)	**Controlli Cobit**	**Controlli ISO 27001 – Annex A**	**Esempio di Soluzione Tecnologica**
Nell'utilizzo di sistemi di memorizzazione o archiviazione dei dati devono essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (ad esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).	**DS 11.2** Storage and Retention Arrangements - Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements.	• 9.1.1 Physical security perimeter • 9.1.2 Physical entry control • 9.2.1 Equipment siting and protection • 10.5.1 Information backup • 10.7.1 Management of removable media • 15.1.3 Protection of organisational records	Advanced Security Option Information Right Management Soluzioni Oracle di Content Management
Idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (ad es., in relazione alla possibilità di consultazione, modifica e integrazione dei dati);	**DS 5.3** Identity Management - Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in	• 5.1.1 Information security policy document • 5.1.2 Review of the information security policy • 6.1.2 Information security co-ordination • 6.1.5 Confidentiality agreements • 8.2.2 Information security awareness, education and training • 11.1.1 Access control policy • 11.6.1 Information access restriction	Oracle Identity Manager Oracle Access Manage Oracle Advanced Access Manager Oracle Entitlement Server

	line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights.	• 11.7.1 Mobile computing and communications • 11.7.2 Teleworking	
Procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;	**DS 5.4** User Account Management - Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges.	• 6.1.5 Confidentiality agreements • 6.2.1 Identification of risks related to external parties • 6.2.2 Addressing security when dealing with customers • 8.1.1 Roles and responsibilities • 8.3.1 Termination responsibilities • 8.3.3 Removal of access rights • 10.1.3 Segregation of duties • 11.1.1 Access control policy • 11.2.1 User registration • 11.2.2 Privilege management • 11.2.4 Review of user access rights • 11.3.1 Password use • 11.5.1 Secure logon procedures • 11.5.3 Password management system • 11.6.1 Information access restriction	Oracle Identity Manager Oracle Identity Analitics.

Individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali	**DS 11.6** Security Requirements for Data Management - Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements.	• 10.5.1 Information backup • 10.7.3 Information handling procedures • 10.8.3 Physical media in transit • 10.8.4 Electronic messaging • 12.3.1 Policy on the use of crypto controls • 12.3.2 Key management • 12.4.2 Protection of system test data • 12.4.3 Access control to program source code • 15.1.4 Data protection and privacy of personal information	Advanced Security Option
Tracciabilità degli accessi e delle operazioni effettuate; Sistemi di audit log per il controllo degli accessi al database e per il rilevamento di eventuali anomalie	**DS 5.5** Security Testing, Surveillance and Monitoring - Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed.	• 6.1.8 Independent review of information security • 10.10.2 Monitoring system use • 10.10.3 Protection of log information • 10.10.4 Administrator and operator logs • 12.6.1 Control of technical vulnerabilities • 13.1.2 Reporting security weaknesses • 15.2.2 Technical compliance checking • 15.3.1 Information systems audit controls	Audit Vault DataBase Firewall
Nel caso di Fse, devono essere, poi, garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.	**DS 5.11** Exchange of Sensitive Data - Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin	• 6.2.1 Identification of risks related to external parties • 10.6.1 Network controls • 10.6.2 Security of network services • 11.4.1 Policy on use of network services • 11.4.2 User authentication for external connections • 11.4.3 Equipment identification in networks	Advanced Security Option

		• 11.4.4 Remote diagnostic and configuration port protection • 11.4.5 Segregation in networks • 11.4.6 Network connection control • 11.4.7 Network routing control • 11.6.2 Sensitive system isolation • 12.3.1 Policy on the use of crypto controls • 12.3.2 Key management	

GLOSSARIO

AdS - Amministratore di Sistema
ANSI - American National Standards Institute
CAD - Codice dell'Amministrazione Digitale
CCE - Cartella Clinica Elettronica
CDA - Clinical Document Architecture (standard ANSI - HL7)
CEN - European Committee for Standardization
CEN TC251 - Comitato Tecnico del CEN sulla Sanità Elettronica
CIE - Carta d'identità Elettronica
CNS - Carta Nazionale Servizi
CPR - Computer-based Patient Record (EPR)
CRS - Carta Regionale dei Servizi
CRS - Care Record Service
CUP - Centro Unificato di prenotazione
DDI - Dip. Digitalizzazione e Innovazione tecnologica (ex- DIT)
DICOM - Standard per la trasmissione di immagini in sanità
DMP - Dossier Medicale Personnel (FSE francese)
EHR - Electronic Health Record
EHRcom - standard EN 13606 del CEN
epSOS - European patient Smart Open Services
EuroRec European Institute for Health Records
HL7 - Health Level 7, organizzazione per la produzione di standard per la sanità elettronica
IBSe - Infrastruttura di Base per la Sanità Elettronica
InFSE - progetto sulla Infrastruttura tecnologica del FSE
IPSE - progetto sulla interoperabilità del Patient Summary e dell'e-Prescription
LEA - Livelli Essenziali di Assistenza
LOINC - Logical Observation Identifiers Names and Codes
MMG - Medico di Medicina Generale
PACS - Picture Archiving and Communication Systems
PHR - Personal Health Record
PDF - Pediatra di Famiglia
RIM - Reference Information Model di HL7
RIS - Radiology Information System
RSA - Residenze sanitarie assistenziali

SDO	- Schede di dimissione Ospedaliera
SOA	- Service-Oriented Architecture
SPC	- Sistema Pubblica di Connettività
SSN	- Servizio Sanitario Nazionale
SSR	- Servizio Sanitario Regionale
TS-CNS	- tessere sanitarie e carta nazionale Servizi
TSE	- Tavolo di Sanità Elettronica
CCR	- Continuity of Care Record
CEN	- Commissione Europea di Normalizzazione
CDA	- Clinical Document Architecture
CNIPA	- Centro Nazionale per l'Informatica nella Pubblica Amministrazione
CRM	- Consultazione Referti Medici
DEA	- Dipartimento di Emergenza e Accettazione
DICOM	- Digital Imaging and Communications in Medicine
ebXML	- Electronic Business using eXtensible Markup Language
EHR	- Electronic Health Record
EPR	- Electronic Patient Record
HL7	- Health Level Seven
HL7-RIM	- HL7 Reference Information Model
IHE	- Integrating the Healthcare Enterprise
ISO	- International Standard Organization
LOINC	- Logical Observations Identifiers, Names and Codes
MIME	- Multipart Internet Mail Extension
MMG	- Medico di Medicina Generale
OID ISO	- Object Identifier
PLS	- Pediatra di Libera Scelta
SOAP	- Simple Object Access Protocol
SWF	- Scheduled Workflow (profilo IHE)
URI	- Uniform Resource Identifier
XDS	- Cross-Enterprise Document Sharing (profilo IHE)
XML	- Extensible Markup Language

AUTORI

AIEA è l'Associazione Italiana Information Systems Auditors.

Costituita in Milano nel 1979, l'AIEA riunisce e certifica coloro che in Italia svolgono professionalmente attività di Auditing e Controllo di sistemi ITC sia individualmente, sia come associati, partner o dipendenti di società.

Gli obiettivi dell'AIEA:

- ampliare la conoscenza e l'esperienza dei suoi aderenti nel campo dell'Information Systems Auditing, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- provvedere ad una adeguata informazione e comunicazione reciproca ai fini dell'aggiornamento nel campo delle tecniche di auditing nell'Information Technology and Communication;
- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo di affidabilità dell'organizzazione e di sicurezza dei sistemi;
- facilitare i rapporti di scambio con analoghe associazioni estere;
- promuovere a livello nazionale la partecipazione degli Information Systems Auditor, alla certificazione C.I.S.A. (Certified Information Systems Auditor).

AIEA è membro dell'ISACA, International System Audit and Control Association, l'organismo che riunisce le associazioni professionali nazionali, che hanno lo scopo di rappresentare e certificare la figura professionale degli aderenti in quanto conforme alle caratteristiche richieste dai propri statuti. Ad ISACA attualmente aderiscono circa 20.000 auditors e consulenti informatici in più di 100 Paesi, di cui circa 3.000 in Europa.

Sito web: www.aiea.it

Autori

Giulio Spreafico - Amministratore della Spreafico di Spreafico Giulio e C. S.a.S e socio di AIEA, capitolo di Milano di ISACA.

Il **Clusit**, nato nel 2000 presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano, è la più importante ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese: Ricerca, Industria, Commercio e Distribuzione, Banche e Assicurazioni, Pubblica Amministrazione, Sanità, Consulenza e Audit, Servizi, Telecomunicazioni, Informatica.

Le attività ed i progetti in corso:

- formazione specialistica: Seminari CLUSIT;
- certificazioni professionali: corsi ed esami CISSP e BCI;
- ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria;
- le Conference specialistiche: Security Summit (Milano, Roma e Verona);
- ROSI: un metodo per valutare il ritorno dell'investimento in sicurezza informatica;

- Progetti Clusit per piccole e microimprese;
- Canale Clusit su YouTube: la sicurezza ICT in video pillole;
- Progetto Scuole: la Formazione sul territorio.

Sito web: www.clusit.it

Autori

Massimiliano Manzetti - Membro Comitato Direttivo Clusit.

Deloitte.

Forte di un network di società presenti in 140 Paesi, e di circa 169.000 professionisti, Deloitte porta i propri clienti al successo grazie al suo know how e ad una profonda conoscenza dei singoli mercati in cui è presente. In Italia, Deloitte è una tra le più grandi realtà di servizi professionali alle imprese. Presente dal 1923 conta, oggi, 2.800 professionisti, che assistono i clienti nel raggiungimento di livelli d'eccellenza grazie alla fiducia nell'alta qualità del servizio, all'offerta multidisciplinare e alla presenza capillare sul territorio nazionale. L'offerta, che copre tutti i settori merceologici (Aviation & Transport Services, Consumer Business, Energy & Resources, Financial Services Industry, Manufacturing, Public Sector Real Estate,Technology, Media & Telecommunications), è erogata dalle seguenti aree:

- audit;
- consulting;
- Enterprise Risk Services;
- Financial Advisory Services;
- legal;
- tax;
- XBS.

Deloitte ERS Enterprise Risk Services è la società del network Deloitte specializzata nei servizi in materia di Corporate Governance, Sistemi di Controllo Interno, Gestione dei rischi aziendali (Risk management) di Regulatory compliance, di Sicurezza e di Privacy.

Sito web: www.deloitte.com/view/it_IT/it/servizi/ERS/index.htm

Autori

Tommaso Stranieri - Partner in Deloitte Enterprise Risk Services
CISA e membro AIEA

Dario Vaccaro - Supervisor in Deloitte ERS, certificato LA ISO 27001

Il Gruppo Terasystem fornisce servizi di Consulenza e System Integration nell'ambito del consolidamento, virtualizzazione, sicurezza e gestione delle infrastrutture IT complesse, coprendo l'intera gamma di servizi tecnologici, dallo sviluppo di una strategia IT alle soluzioni per ottimizzare l'infrastruttura e le applicazioni. Proponiamo una Consulenza innovativa in grado di ridurre i costi, i rischi e di migliorare i livelli di servizio garantendo risultati misurabili, approcci concreti e tempi certi per l'analisi dell'ambiente, delle applicazioni e dell'infrastruttura IT. La nostra indipendenza, che ci svincola da logiche di produzione, e la nostra esperienza pluridecennale ci consentono di individuare sempre la soluzione migliore, tagliata sull'unicità di ogni nostro cliente. Forniamo la nostra consulenza attraverso una struttura di processo che combina la metodologia esclusiva di GlassHouse, avanzati strumenti software e l'elevata competenza dei nostri consulenti, acquisita nella realizzazione di progetti per clienti di rilevanza nazionale. Il corretto mix di teoria e pratica per affrontare con serenità le sfide che ogni giorno i clienti ci richiedono.

Sito web: www.gruppoterasystem.it

Autori

Paolo Capozucca - Business Development & Alliance Manager

Giacomo Aimasso - CISA, CISM – CTO B.U. Security & Data Protection

Andrea Zapparoli Manzoni - Principal Security Consultant

Giancarlo Colla - CTO Divisione Consulting

Kelyan opera da oltre trent'anni nell'Information technology: nata dall'accordo tra Kelyan SMC e A&C Holding, primarie aziende del settore IT, propone servizi che vanno dalle applicazioni gestionali Erp, alla gestione documentale, all'Enterprise Content Management, alla sicurezza informatica, sino alle infrastrutture.

Kelyan intende porsi come leader in Italia nel settore IT attraverso l'integrazione di attività di consulenza ERP, di sicurezza IT e di gestione dei processi documentali.

Con sedi in Emilia Romagna, Piemonte, Lombardia, Veneto e Lazio, Kelyan si rivolge al mercato della media impresa manifatturiera; la BU Micro Consulting si rivolge in particolare alla PMI di Piemonte e Liguria.

L'offerta sul mercato si articola anche sul canale indiretto, attraverso Net Team, la business unit che collabora con il canale di vendita Telecom Italia.

Oggi la società ha oltre 200 dipendenti e ha realizzato un fatturato di 32 milioni di euro nel 2009, con un parco di 3000 clienti attivi.

Sito web: www.kelyan.it

Autori

Enrico Ronchetti - Database Administrator & Architect.

KPMG è un network globale di società di servizi professionali, attivo in 146 paesi del mondo con circa 144 mila persone: in Italia, il network KPMG è rappresentato da diverse entità giuridiche attive nel business advisory, nella revisione e organizzazione contabile, e nei servizi fiscali e legali.

I servizi di IT Advisory di KPMG contano circa 500 professionisti in Italia presenti in 6 uffici e si focalizzano sullo sviluppo, sulla gestione dei sistemi informativi e sul presidio dei relativi rischi. La business unit "Security and IT Risk & Compliance", focalizzata negli ambiti della sicurezza dei sistemi informativi, compliance, sicurezza e monitoraggio delle performance, ha l'obiettivo di garantire ai propri clienti un servizio di eccellenza nella valutazione e nello sviluppo di strategie e soluzioni a supporto del business che riducono i rischi associati alla pianificazione, all'introduzione e alla scelta di tecnologie. Effettua valutazioni indipendenti sulle strategie, sui progetti e sulla sicurezza, fornendo valore e soluzioni per l'impresa nell'ambito della security, della privacy e dell'integrità dei dati; ottimizzando la gestione dei rischi e delle risorse IT con un pieno controllo dei livelli di servizio e dei costi.

Sito web: www.kpmg.com/IT

Autori

Pierluigi Lonero - Senior Manager. Esperto IT Advisory, Information Risk Management e Security.

Laura Quaroni - IRM Manager, Information Risk Management, IT Advisory

Mediaservice

@ Mediaservice.net è una Security Advisory Company che opera sul mercato della Sicurezza Informatica da più di 10 anni, fornisce Servizi di Sicurezza e Professional Consulting aventi come core business la Sicurezza delle Informazioni.

Per soddisfare le esigenze dei propri Clienti si avvale di risorse con esperienza pluriennale nel campo della sicurezza informatica, provenienti da esperienze aziendali di eccellenza, i quali svolgono servizi di consulenza a 360° spaziando dal campo della sicurezza proattiva, mediante valutazioni tecnologiche ed organizzative, a quello della sicurezza di processo volta a migliorare la gestione della sicurezza seguendo le leggi e gli standard di riferimento.

In termini di settori merceologici @ Mediaservice.net copre un campo d' azione vasto ed eterogeneo, fornendo servizi di sicurezza a Clienti operanti nel campo aerospaziale e dei trasporti in genere, fino alle pubbliche amministrazioni, ai settori delle telecomunicazioni della sanità e finanza.

Sito web: www.mediaservice.net

Autori

Alberto Perrone - Security Advisor, abilitazione di Lead Auditor ISO/IEC 27001:2005 e certificazione OSSTMM Professional Security Tester.

Presente in oltre 145 paesi nel mondo con oltre 106.000 dipendenti e un fatturato GAAP nell'anno fiscale 2010 pari a 26,8 miliardi di dollari, Oracle Corporation propone la più ampia, completa, aperta e integrata offerta di sistemi software e hardware e vanta oggi oltre 370.000 clienti – fra cui 100 delle imprese della classifica Fortune 100 e oltre 250.000 medie aziende. Oracle ha sempre messo la sicurezza al centro dei propri prodotti e, anche a seguito di alcune acquisizioni in quest'area (Oblix, OctetString, Thor Technologies, Bridgestream, Bharosa, Secerno, Sun), oggi fa sì che le organizzazioni possano contare su infrastrutture IT protette sia dalle minacce esterne che da quelle interne. Ciò è possibile grazie a prodotti, tecnologie e processi che consentono di indirizzare tutte le esigenze in termini di sicurezza, privacy e rispetto delle normative. In Italia, Oracle è impegnata a far crescere il livello di competenza del sistema attraverso la Oracle Community for Security. Nata nel 2007, si tratta della comunità dei Partner di Oracle dedicata alle tematiche che ruotano intorno alla sicurezza informatica. Oggi conta circa 30 membri.

Sito web: www.oracle.it

Autori

Angelo Bosis – Technology Sales Consultant Senior Manager

Valter Cravero - Sales Development Manager per l' Healthcare.

Alessandro Vallega - Business Development Manager Oracle Security e coordinatore Community for Security - Membro Comitato Direttivo Clusit.

Present SPA, con 700 professionisti nel 2009, uffici a Milano, Roma, Napoli, Torino, Padova e sedi a Londra, Stoccarda e Parigi, offre servizi di Consulenza, System Integration e Managed Services nelle Aree Applicative dell'ICT Security, e-Commerce, CRM, ECM, DWH/ Business Intelligence, ERP, VAS, Enterprise Application Integration, ICT Infrastructure.

Opera principalmente nei settori di mercato della Pubblica Amministrazione Centrale e Locale, Industria e Finanza, nel territorio nazionale e presso i Paesi dell'Unione Europea.

Realizza soluzioni chiavi in mano e/o progetti custom, integrazione di prodotti proprietari o package leader di mercato, eroga servizi applicativi, sistemistici ed in outsourcing.

Attraverso il Data Center collocato nella propria sede di Torino, eroga in outsourcing servizi specialistici orientati alla gestione della sicurezza e della continuità operativa delle infrastrutture ICT per oltre 120 importanti aziende italiane.

Autori

Alessia Ciampalini - Privacy Compliance Consultant, Certificazioni. CISA, ISO/IEC 27001 Lead Auditor

Francesco Severi - Security Practice Manager. Certificazioni: CISSP, ISO/IEC 27001 Lead Auditor, ITIL, PMP

Salvatore Lombardi - Business Development Manager. Certificazioni: ISO/IEC 27001 Lead Auditor, PMP

Protiviti è un Gruppo multinazionale di consulenza direzionale, leader nell'analisi e progettazione di modelli di Governance, Organizzazione e Controllo. Nata nel 2002 in California, Protiviti è un network caratterizzato da una presenza internazionale di rilievo con oltre 60 uffici presenti nelle principali città degli Stati Uniti, Canada, Sud America, Europa, Asia e Australia e oltre 2.500 persone.

In Italia, Protiviti opera nelle sedi di Milano, Torino e Roma e conta oltre 130 professionisti. La filiale italiana è in continua crescita, a conferma del sempre maggiore interesse del mercato delle aziende evolute nei confronti dei servizi di Governance. Obiettivo di Protiviti è la diffusione di una cultura aziendale finalizzata ad allineare i processi, i sistemi informativi e l'organizzazione alle migliori prassi internazionali. La base Clienti include oltre il 25% delle imprese del Fortune 1000. I valori che ci caratterizzano sono racchiusi nel brand "Protiviti", ideato per richiamare i principi chiave che ispirano la nostra consulenza: professionalism, proactiviti, indipendence, integriti, objectiviti.

Protiviti fa parte del Gruppo Robert Half International (RHI), quotato al NYSE e appartenente all'indice S&P 500, leader nel segmento Head Hunting.

Sito web: www.protiviti.it

Autori

Enrico Ferretti - Associate Director. CISA, CGEIT, LA ISO27001, PCI-DSS QSA, Membro AIPSA. Membro AIEA

Antonello Gargano - Senior Consultant. Membro AIEA

Daniele Pasini - Security Consultant

Reply S.p.A., una delle principali società italiane nel settore dell'E-business, è nata sull'idea che l'avvento della rete e delle nuove e sempre maggiori possibilità di comunicazione avrebbero radicalmente trasformato la società, i comportamenti e le aziende. Reply opera offrendo consulenza e servizi orientati alle aziende che vogliano progettare ed implementare soluzioni e nuove strategie di E-business o siano interessate a realizzare applicazioni in grado di sfruttare tutte le potenzialità e opportunità offerte della rete.

Le attività di Reply si concentrano nelle aree dell'e-business consulting (consulenza strategica, organizzativa e di processo), dell'e-business communication (comunicazione multimediale e servizi di web-marketing) e dell'e-business implementation (progettazione e implementazione di sistemi internet, portali, siti e applicazioni mission critical in architettura multicanale).

Reply S.p.A. è quotata al Nuovo Mercato di Borsa Italiana dal 6 dicembre 2000.

All'interno del Gruppo Reply SpA, Spike Reply è la società specializzata sulle tematiche relative all'area della Sicurezza e della tutela dei Dati Personali. La missione di Spike Reply è di permettere ai propri clienti di effettuare il loro business in condizioni di Sicurezza, supportandoli nello sviluppo delle idonee strategie e nella implementazione delle appropriate soluzioni per una gestione efficace della Sicurezza delle Informazioni.

Sito web: www.reply.eu/it

Autori

Roberto Leone - Senior Security Consultant

Sinfo One S.p.A. nasce nel 1984 e si rivolge alle aziende italiane fornendo soluzioni ERP estese, consulenza direzionale, organizzativa, di processo e tecnologica e servizi di system integration. L'offerta ERP è basata sulla piattaforma proprietaria Si Fides e sulla piattaforma Oracle JD Edwards Enterprise One, che Sinfo One completa con il proprio verticale per il Food & Beverage. Sinfo One opera su tutto il territorio nazionale attraverso un team di oltre 100 professionisti con esperienze nei diversi settori di mercato e profonde competenze sui relativi processi specifici.

Grazie alla profonda conoscenza della piattaforma Oracle JDEdwards ed alle competenze ed esperienze dei propri team di professionisti è in grado di offrire soluzioni verticalizzate e integrate a Enterprise Content Management, Enterprise Performance Management e Business Intelligence e Data Security.

Sito web: www.sinfo-one.it

Autori

Claudio Pasi - Business Development & Delivery Manager Tecnologia sulle aree Enterprise Content Management, Database & Data.

Dal 1999, lo **Studio Legale Abeti** fornisce un nuovo tipo di consulenza, non solo legale ma anche direzionale, rappresentando nei confronti dei clienti il link tra le esigenze del top management e quelle delle funzioni ICT.

Gli ambiti di riferimento in cui esercita la propria attività sono: la protezione delle informazioni, la responsabilità amministrativa delle società, la gestione dei flussi informativi (dall'ottimizzazione dei processi, alle procedure di archiviazione), la prevenzione dei crimini informatici e la tutela del diritto d'autore.

Il cliente può contare sulle professionalità dello Studio al fine di ottenere: pareri, redazione di contratti, valutazioni di impatto, stesura linee guida, policy e procedure, nonché attività di formazione nelle materie in cui sono specializzate le risorse dello Studio. Da alcuni anni partecipa, prestando la propria consulenza legale specializzata, ai lavori della Community for Security di Oracle.

Sito web: www.abeti.eu

Autori

Avv. Riccardo Abeti - Presidente della Commissione "New Technology, Personal Data and Communication Law" e membro del Comitato esecutivo dell'Unione Avvocati Europei.

Tech Gap Italia è un system integrator specializzato in progetti ICT destinati ai settori healthcare e manufacturing. La conoscenza approfondita di temi come la virtualizzazione e il consolidamento dei server, la data security (gestione identità, enterprise single sign on, strong authentication) e i progetti web 2.0 fanno di Tech Gap Italia il partner tecnologico ideale. Tech Gap Italia ha sviluppato per il mercato healthcare soluzioni end-to-end che vanno dal disegno infrastrutturale allo sviluppo di soluzioni mobile (iPhone), con particolare interesse ai concetti tipici dell'Empowerment del Cittadino/Paziente.

Sito web: http://techgap.it/

Autori

Paolo Mereghetti - Project Manager

Mirco Sozzi - Direttore Tecnico

ZEROPIU lavora al fianco delle aziende clienti, realizzando e gestendo sistemi, infrastrutture IT e applicazioni grazie ad un'efficace combinazione tra competenza organizzativa, esperienza tecnica,unita alla conoscenza di tecnologie avanzate.

L'attività spazia dalla consulenza tematica e organizzativa, alla realizzazione di progetti IT; dallo sviluppo di soluzioni ad hoc all'assistenza tecnica,passando per l'erogazione di servizi di help desk e formazione.

Le aree di competenza sono:

- attuazione della normativa Privacy e implementazione di sistemi di gestione IT e di ISMS (standard ITIL e ISO 27001);
- sicurezza logica (Role management e IAM);
- realizzazione di infrastrutture tecnologiche;
- sviluppo di soluzioni e applicazioni integrabili in ambito di portali Intranet/Extranet.

ZEROPIU inoltre mette a disposizione dei clienti una gamma di servizi IT:

- gestione/manutenzione dell'infrastruttura software;
- upgrade ed evoluzione delle applicazioni;
- supporto operativo, Help desk/Call Center (tecnico).

Sito web: www.zeropiu.it

Autori

Sergio Fumagalli - Vice Presidente. Certificazioni: ISO 9001, Membro Clusit.