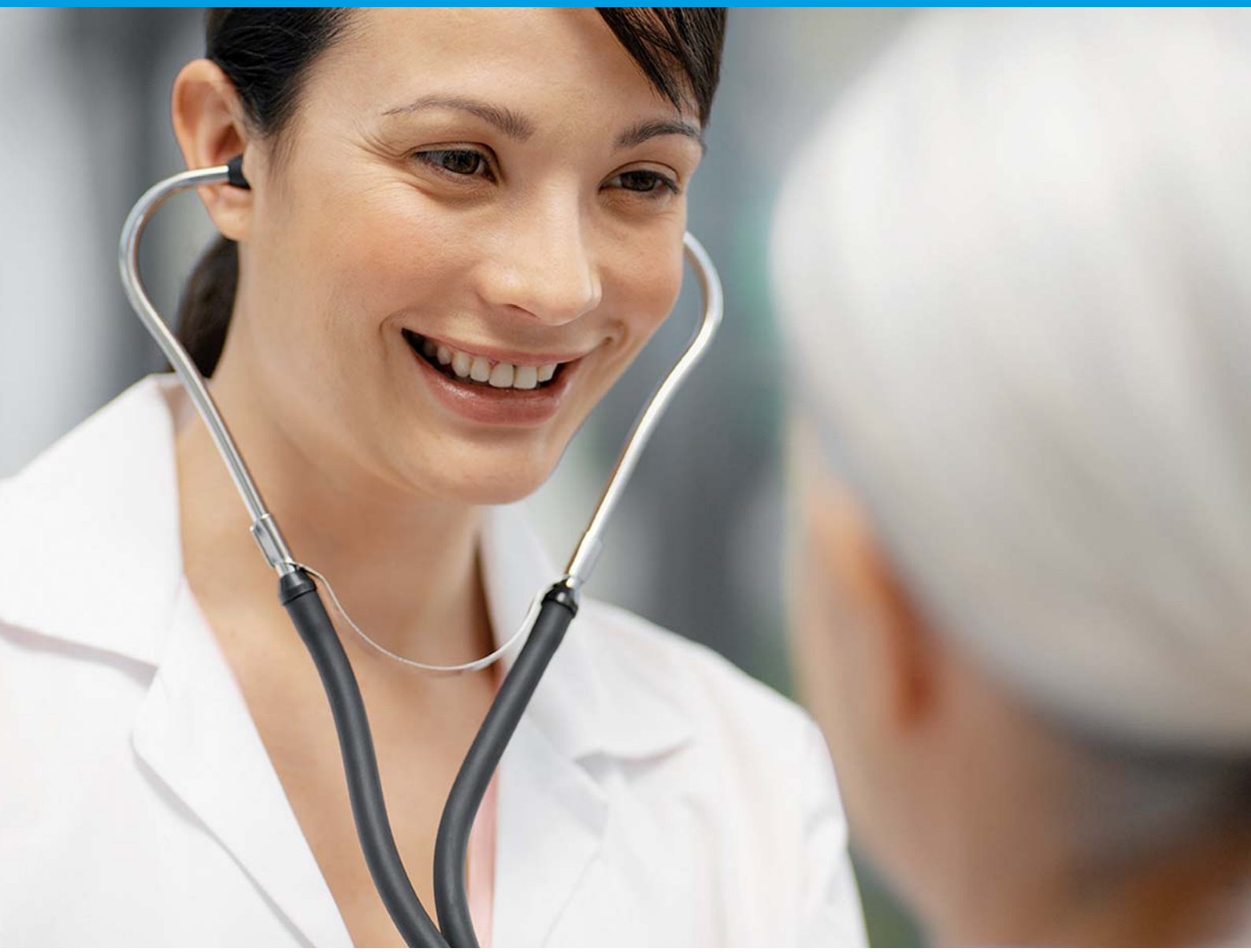


Fascicolo Sanitario Elettronico:

il ruolo della tecnologia nella tutela della privacy e della sicurezza

Management summary.

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, specializzata 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.

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 ed gli attori dell'offerta di applicazioni e servizi professionali che contribuiscono alla soluzione degli aspetti applicativi e gestionali.

Il documento è articolato in 8 macro sezioni, ognuna delle quali affronta in modo sintetico, ma allo stesso tempo esaustivo, gli aspetti che caratterizzano il tema della sicurezza applicato al Fascicolo Elettronico Sanitario.

La sezione "Chi scrive e quali obiettivi si pone" delinea, nell'ambito del documentorelativo al FSE, gli obiettivi che il gruppo di lavoro sulla sicurezza si è posto e persegue.

La sezione "Riferimenti Normativi" prende in esame gli aspetti legati alla normativa che disciplina il Fascicolo elettronico negli aspetti di privacy e sicurezza.

"Implicazioni tecnologiche dei requisiti normativi e delle linee guida" tratta le implicazioni informatiche derivate dagli aspetti Normativi.

La sezione "Analisi del testo: elementi di una architettura di sicurezza implicate dai requisiti delle linee guida" analizza i requisiti funzionali evincendone le caratteristiche infrastrutturali.

"L'architettura per una soluzione sostenibile" è la sezione in cui vengono fornite le indicazioni per disegnare ed implementare l'FSE nel rispetto delle indicazioni del Garante e coerentemente con le esigenze informatiche ad esso correlate.

"Minacce di sicurezza" è la sezione in cui si evidenziano le minacce informatiche ed i rischi connessi all'adozione dell'FSE.

Da ultimo, "Best practices internazionali" riassume le indicazioni che le entità internazionali forniscono nella gestione della sicurezza delle informazioni (ISMS) basate su standard di mercato.

Nelle pagine seguenti si trova una sintesi del lavoro svolto, mentre si rimanda al minisito di supporto (ospitato all'indirizzo http://fse.clusit.it) la possibilità di fare un download completo delle considerazioni ed analisi svolte dal gruppo di lavoro.

Chi scrive e quali obiettivi si pone

La Community for Security è un'organizzazione che tratta il tema della sicurezza dell'informazione e che raccoglie le più importanti aziende di informatica italiane ed internazionali dell'ecosistema dei partner Oracle. Essa vede tra i suoi partecipanti anche le primarie 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 Fascicolo Sanitario Elettronico, 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, Sudio Legale Abeti, Tech Gap e Zeropiu.

Il gruppo di lavoro 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.

Il gruppo di lavoro non si è, inoltre, posto l'obiettivo di affrontare gli aspetti funzionali ed applicativi, ma ha deciso di focalizzarsi sulle proprie competenze di base che riguardano la sicurezza.

L'obiettivo è di contribuire al dibattito in corso, proponendo un'architettura tecnologica di sicurezza supportata da considerazioni legali ed organizzative, in grado di dare una risposta di qualità, efficace ed efficiente ai requisiti posti dalle linee guida.

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.

I requisisti posti dal Garante e la tutela dei diritti costituzionali del paziente costituiscono sul piano tecnologico, una sfida molto ambiziosa che richiede di sfruttare le tecnologie più innovative per garantire il soddisfacimento dei requisiti e la sostenibilità economica.

Le soluzioni devono consentire, tra l'altro:

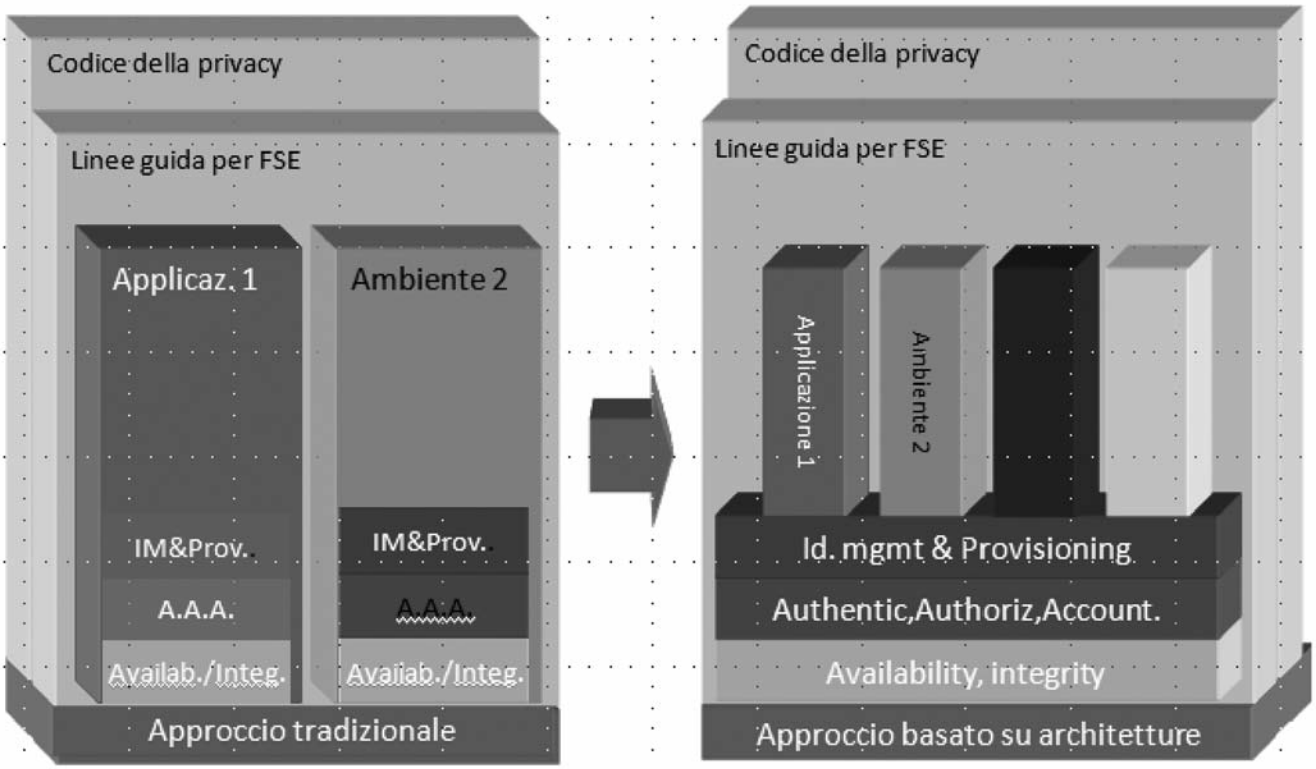
- un elevato livello di interoperabilità
- la capacità di resistere alle attuali e future minacce informatiche
- la trasparenza della sicurezza per l'utilizzatore (la user experience)
- la sostenibilità, nel tempo, dei costi operativi

Solo un approccio architetturale consente di affrontare in modo unitario questi temi e quindi di traguardare con successo i diversi livelli di gestione e fruizione del FSE declinati in tutti i livelli territoriali coinvolti nella tutela della salute del cittadino.

Infatti, se da un lato le aziende sanitarie creano i contenuti, dall'altro enti terzi ne gestiscono ed erogano il servizio verso i diversi fruitori (pazienti e altri titolari). Affrontare le tematiche di sicurezza con questo approccio significa, inoltre, garantire i livelli di flessibilità e di indipendenza necessari per una costante innovazione.

Il presente documento è destinato alle strutture sanitarie, agli enti regionali e alle società in house coinvolte nella realizzazione e nella gestione del FSE, oltre agli attori dell'offerta di applicazioni e servizi professionali che contribuiscono alla soluzione degli aspetti applicativi e gestionali.

Fig.1 Modello di riferimento Architetturale



Riferimenti normativi

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.

In questo quadro si inserisce il provvedimento dell'Autorità Garante del 16 luglio 2009.
L'Autorità ha adottato le linee guida in seguito alle segnalazioni, ai confronti con gli operatori, alle proprie attività di approfondimento ed alla constatazione dell'esistenza di alcune iniziative volte a favorire

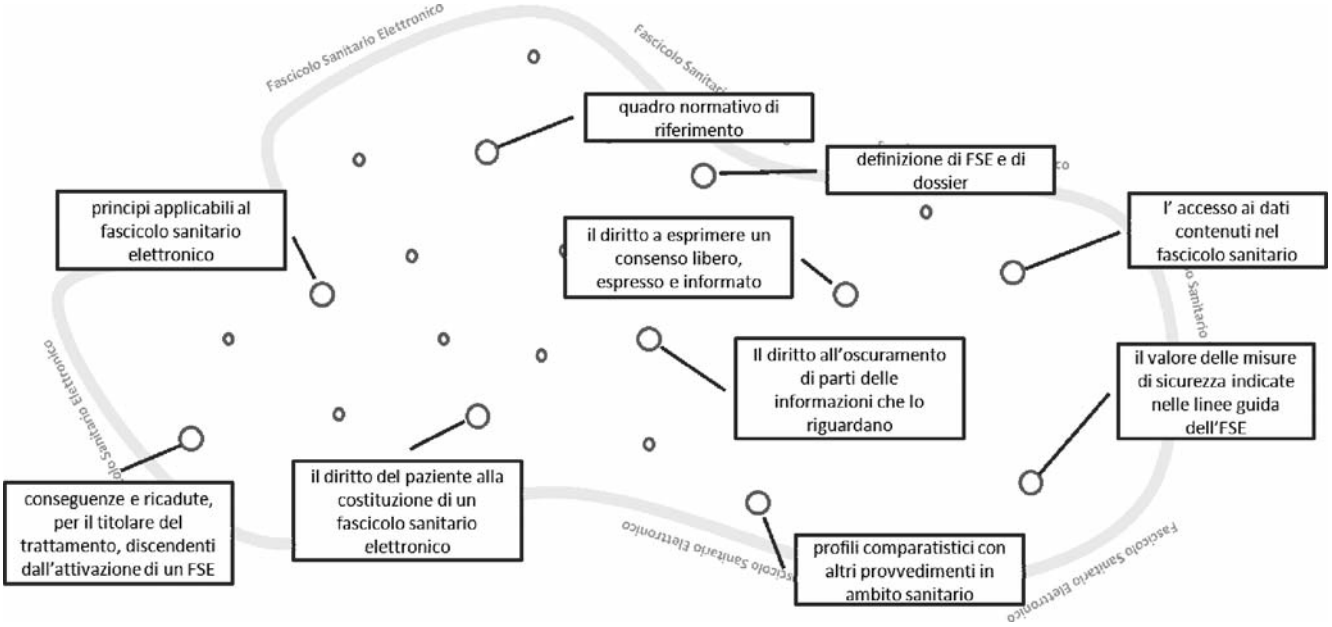
> *la condivisione informatica, da parte di distinti organismi o professionisti, di dati e documenti sanitari che vengono formati, integrati e aggiornati nel tempo da più soggetti, al fine di documentare in modo unitario e in termini il più possibile completi un'intera gamma di diversi eventi sanitari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

Non essendo, ad oggi, disponibile un preciso quadro volto a regolamentare quest'aspetto della "modernizzazione" della realtà sanitaria, 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.

Le linee guida, pur non costituendo normativa cogente, individuano un insieme di misure "idonee e preventive" (ex art. 31) che non possono essere nè eluse nè ignorate, stanti i possibili impatti sotto diversi profili di responsabilità. Inoltre, la volontà di legittimare la costituzione del FSE con una norma di rango primario ha portato alla recente presentazione al Consiglio dei Ministri di uno schema di disegno di legge su «Sperimentazione clinica e altre disposizioni in materia sanitaria».

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 nel documento (figura successiva), alla cui lettura si rimanda per ogni approfondimento:

Implicazioni tecnologiche dei requisiti normativi e delle linee guida



Riprendendo gli aspetti individuati nel capitolo precedente, 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 di 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.

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

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 ed 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 derivano alcune caratteristiche infrastrutturali:

- i dati risiedono, nella responsabilità del Titolare, quando sono stati generati e vengono acceduti da altri Titolari/Titolati via rete.
    - o 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.
    - o 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 non trascurabile 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 (art. 2) le informazioni risiedono nel perimetro organizzativo del Titolare che le ha raccolte e, dunque, non sono duplicate. 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 riguarda l'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 che l'infrastruttura che erogherà 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 FSE/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 (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 adottando soluzioni architettura di sicurezza che interagiscono con 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 FSE/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 all'ERLCM, cioè alla gestione del ciclo di vita dell'identità digitale (Cittadino/Paziente) 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 Titolar e- 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.

E' 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.

- Punti chiave / tecnologie: la Strong Authentication e l'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.

- Punti chiave / tecnologie: la 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 (es. 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)".

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 a livello applicativo comporta una duplicazione di informazioni e di attività di gestione delle 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 (es. ASL, Ospedale, laboratorio, …) o ente erogatore (es. Società In House), quindi, a livello del sistema sanitario Regionale 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.

L'architettura per una soluzione sostenibile

La soluzione architetturale per il FSE si colloca all'interno di una impostazione coerente con la SOA (Service Oriented Architecture), come indicato in figura.

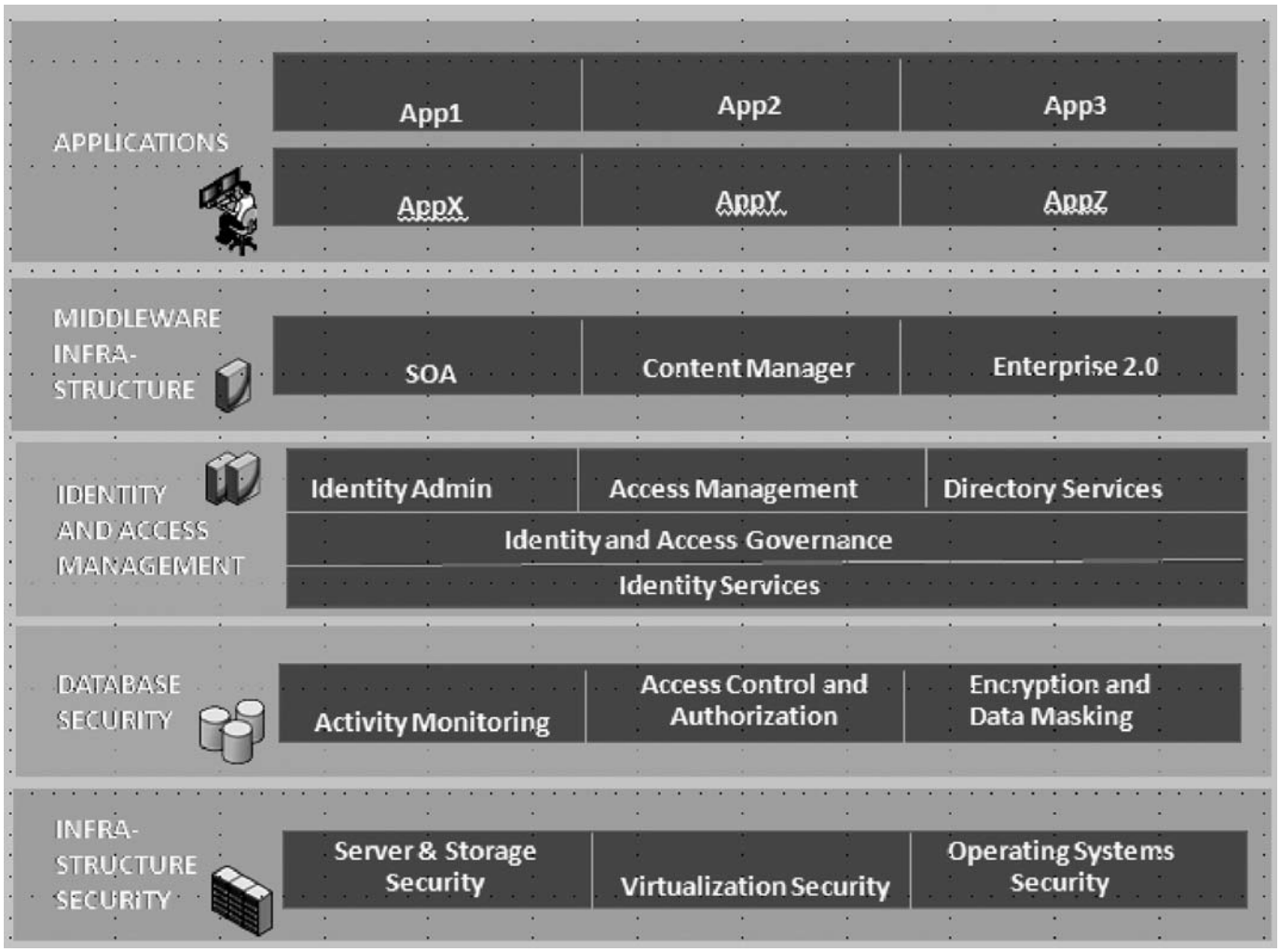
Fig. 3 - Infrastruttura di interoperabilità sicura

In questo contesto le tematiche della sicurezza descritte nei capitoli precedenti trovano una collocazione organica ed indirizzano i seguenti aspetti:

- La sicurezza del dato (nel database, nel file system, nei documenti e nei loro backup)
- la sicurezza della rete (nella intranet, nella extranet e su internet)
- la sicurezza dell'accesso (autenticazione, ruoli, identità, privilegi)
- la gestione e il controllo dell'infrastruttura (log management, change e configuration management)
- l'auditing e la compliance

Il modello architetturale proposto è rappresentato nella figura successiva declinando i singoli strati tecnologici necessari e sufficienti a garantire una reale e coerente implementazione del l'FSE rispetto alla sua sostenibilità sul piano dei costi e della gestione.

Fig. 4 - Tecnologie di interoperabilità sicura



Tale modello offre una risposta a tutto tondo alle tematiche poste dall'implementazione del FSE.

Da un lato, poggia sulle solide fondamenta dell'infrastruttura fisica, i cui vari componenti possono essere raggruppati in Sistemi Operativi, Soluzioni di Virtualizzazione, Server e Storage. Anche in quest'area è possibile scegliere tecnologie progettate e costruite con un'elevata attenzione agli aspetti di sicurezza.

Dall'altro lato, troviamo le specifiche applicazioni sviluppate sfruttando l'infrastruttura di middleware dove è possibile trovare una ricca gamma di servizi comuni e condivisi per facilitare lo sviluppo e l'interoperabilità delle applicazioni. Al centro si collocano le componenti più specificatamente rivolte alla sicurezza del dato e delle identità.

Per quanto riguarda la sicurezza del dato sono disponibili molteplici tecnologie che rispondono alle differenti esigenze di protezione delle informazioni strutturate:

- proteggere e crittografare i dati sensibili in ambienti di produzione
- mascherare i dati sensibili negli ambienti non di produzione
- crittografare il traffico dei dati in rete
- controllare l'accesso ai dati degli utenti e in particolare degli utenti con privilegi
- impedire l'accesso da parte degli utenti non del database
- tenere traccia delle modifiche del database e fare audit delle attività sui dati
- controllare e bloccare le minacce prima che raggiungano il database

Per quanto riguarda l'infrastruttura di sicurezza delle identità, questa si appoggia su un layer comune di servizi su cui si poggiano le seguenti macro aree funzionali:

- l'Identity Administration, che racchiude tutte le tecnologie che afferiscono alle funzioni di user provisioning e la gestione del ciclo di vita di ruoli e identità
- l'Access Management che comprende tutte le tecnologie relative al controllo degli accessi: autenticazione, autorizzazione, Single Sign-On e federazione. Inoltre, in quest'area afferiscono anche le tecnologie di controllo di accesso basato sul rischio, di gestione delle autorizzazioni a grana fine, per la sicurezza dei servizi Web e di information rights management per la protezione delle informazioni di business non strutturate
- infine, vi sono i servizi di directory per la centralizzazione e il consolidamento della identità degli utenti.

A completamento di questo layer ha particolare rilevanza la presenza di strumenti per l'Identity & Access Governace che consentono di monitorare centralmente, analizzare, rivedere e governare l'accesso degli utenti al fine di mitigare il rischio, costruire la trasparenza, e soddisfare gli obblighi di conformità alle normative con rapidità ed efficacia

Quanto più le funzioni di sicurezza sono risolte dall'architettura dedicata, tanto più sarà efficiente e sostenibile la soluzione complessiva del FSE; tale sostenibilità si gioca sui diversi parametri di costo della gestione operativa e del controllo di durata dell'investimento in relazione all'obsolescenza tecnologica e sul costo dell'evoluzione tecnologica.

Minacce di sicurezza

La progettazione di una soluzione di sicurezza non può prescindere dalla predisposizione delle contromisure necessarie per contrastare le minacce derivanti dal contesto esterno al FSE, minacce che possono derivare sia da agenti esterni sia interni all'organizzazione.

Nel caso specifico del settore della sanità, 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 un business in piena espansione per i criminali informatici.

Nel rapporto si evidenzia 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, né è rivolto ad un tipo specifico di organizzazione sanitaria.

Lo studio ha dimostrato come i criminali siano stati in grado di sfruttare le informazioni trafugate dalle cartelle cliniche per commettere frodi quattro volte maggiore rispetto ad altri tipi di furto di identità. Infatti, con l'accesso ad informazioni relative ad esempio a carte di credito un truffatore può effettuare specifici tipi di frode, ma con l'abilitazione indebita a profili di informazioni più completi i tipi di inganno che possono essere commessi utilizzando l'identità di una persona sono illimitati. Questo è uno dei motivi per cui le organizzazioni sanitarie stanno diventando un target privilegiato per i criminali informatici.

Negli Stati Uniti uno dei modi in cui viene perpetrata la frode sanitaria è presentare false indicazioni agli assicuratori e alle agenzie pubbliche che forniscono servizi sanitari. Per esempio, accedendo indebitamente ai dati contenuti all'interno di cartelle cliniche elettroniche, un criminale informatico può avvalersi di tale informazioni per fatturare servizi che non sono mai stati resi.

In Italia i cittadini possono 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. Oppure gli interessati potrebbero essere coinvolti in indagini penali per abuso di prestazioni mediche (es. acquisti di farmaci) effettuate a loro insaputa. Infine, i cybercriminali possono tentare di ricattare o di estorcere denaro, minacciando di esporre dati sensibili riguardanti la salute o la situazione famigliare.

Tra i più comuni tipi di attacchi intenzionali si identificano:

1. accesso illecito ai dati
2. modifica / eliminazione / corruzione dei dati
3. denial of service

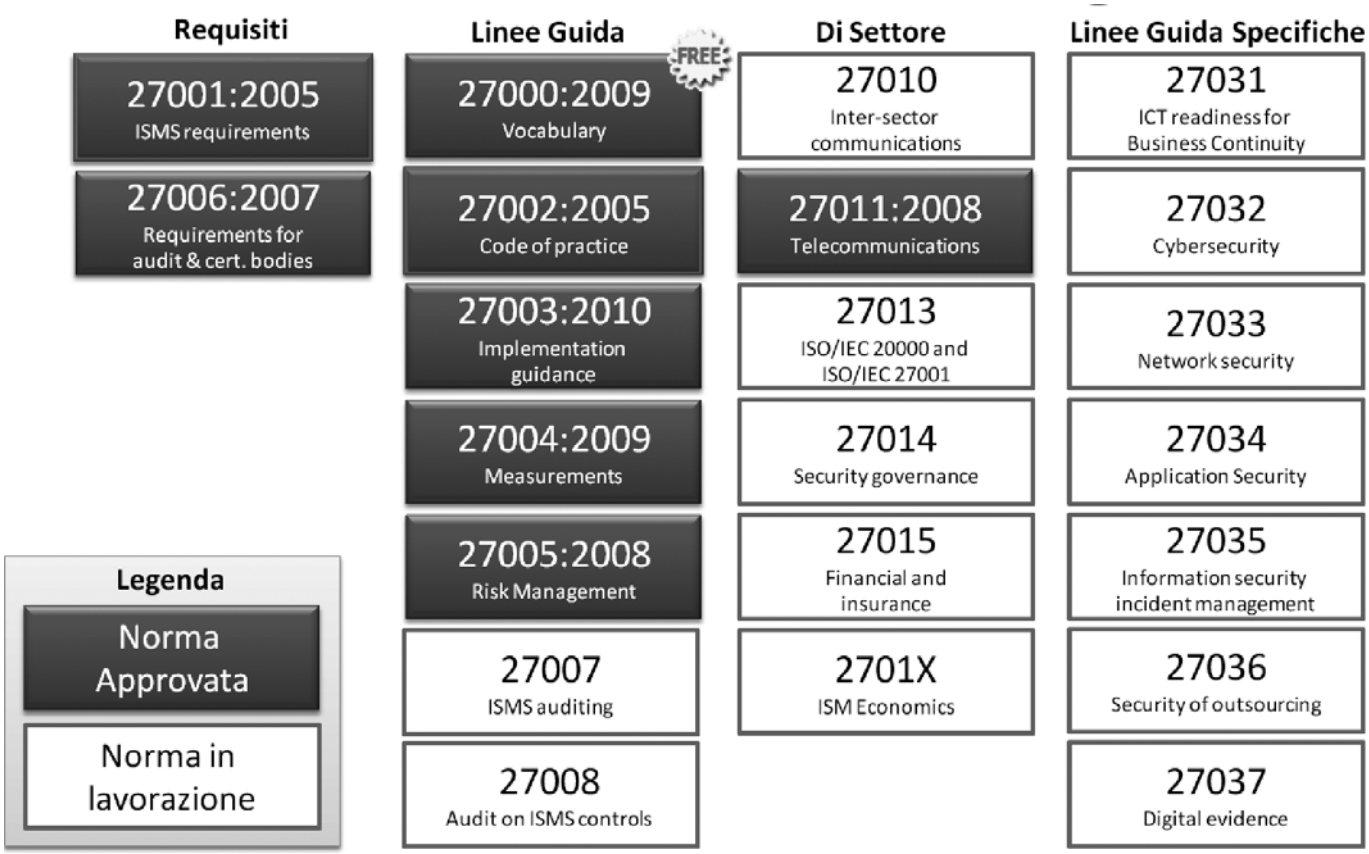
Nel sito web dedicato http://fse.clusit.it vengono presentati alcuni scenari di attacco ad una ipotetica infrastruttura di gestione di un FSE. Essi sono descritt i utilizzando una consolidata metodologia di analisi dei rischi, fanno riferimento ad azioni deliberate volte a trafugare, alterare o rendere indisponibili i dati sanitari contenuti nel fascicolo sanitario elettronico.

Best practices internazionali

Le linee guida del Garante, per quanto riguarda i requisiti di sicurezza e alcune garanzie sui 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 abbraccia 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 e le norme specifiche ISO/CD 27789 - Audit trails for electronic health records; ISO 27799:2008 - Information security management in health using ISO/IEC 27002 e ISO/HL7 27931:2009 - Data Exchange Standards – Health Level Seven Version 2.5 – An application protocol for electronic data exchange in healthcare environments.

Fig. 5 - Gli standard della famiglia ISO 27000 (fonte UNINFO, @mediaservice)



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.

E' opportuno ricordare che la sicurezza delle informazioni si declina nelle categorie della riservatezza, della integrità e della disponibilità. Tali categorie possono essere così definite:

- riservatezza: che le informazioni riservate lo rimangano, che tutti e solo quelli che ne hanno bisogno e diritto vi possano accedere
- integrità: che nessuno possa alterare le informazioni in maniera accidentale o fraudolenta
- disponibilità: che le informazioni siano disponibili secondo necessità e livelli di servizio concordati

La corretta traduzione dei requisiti del Garante non può prescindere da questi concetti, universalmente accettati, e che stanno alla base di un'implementazione coerente con le esigenze di utilizzo del FSE.

Indice del materiale disponibile sul minisito

Come anticipato, è stato realizzato un minisito al quale gli interessati possono fare riferimento per avere maggiori informazioni, ottenere le versioni aggiornate di questo documento ed ulteriore materiale di supporto prodotto dal gruppo di lavoro. Inoltre ogni commento è gradito.

I contributi disponibili sono organizzati per argomenti come:

- la Customer Experience ed il cittadino al centro del sistema
- gli aspetti legali del Fascicolo Sanitario Elettronico ed il quadro normativo
- i dati del Fascicolo Sanitario Elettronico, che elenca le tipologie di dati da proteggere
- gli scenari d'uso, ovvero una elencazione puntuale tramite una notazione formale dei processi di accesso e di gestione delle credenziali delle identità digitali
- minacce informatiche, ovvero una disamina di tipo puntuale e statistico degli attacchi che avvengono a livello globale e per il settore della sanità
- componenti tecnologiche, un'elencazione di prodotti e classi di prodotto
- glossario dei termini
- mappatura del FSE (in particolare art.10) con CobiT ed ISO27002 per ricondurre il FSE ai sistemi di gestione della sicurezza
- elenco delle aziende contributrici e autori

L'indirizzo del minisito è il seguente *http://fse.clusit.it;*

Per ulteriori informazioni si può scrivere a *fse@clusit.it*

A cura di


AIEA


Clusit
Associazione Italiana
per la Sicurezza Informatica


Deloitte.


GRUPPO
TERASYSTEM


KELYAN
GRUPPO COMDATA


KPMG


mediaservice.net


ORACLE


present


protiviti
Risk & Business Consulting.
Internal Audit.


Reply
spike


SiNfo
ONE


Abeti


Tech Gap
ITALIA


ZEROPIU
Difference as value