PDTA e Data Protection:
normativa, organizzazione e tecnologia

a cura di

ASSOCIAZIONE ITALIANA
SISTEMI INFORMATIVI IN SANITÀ

Clusit

APiHM

PDTA e Data Protection: normativa, orgnizzazione e tecnologia

Cosa chiediamo all'Autorità, alle Direzioni Generali e alle Direzione ICT delle aziende sanitarie, ai Fornitori

Introduzione

Questa pubblicazione riprende le sfide poste ai partecipanti del convegno annuale di AISIS svoltosi a Napoli ad ottobre 2015, rilanciando il dibattito e suggerendo alcune risposte ai quesiti posti allora.

Come spesso è accaduto negli ultimi anni, al centro della discussione c'è il possibile conflitto tra il diritto alla Cura e il diritto alla Privacy, conflitto che rimanda immediatamente al ruolo dei sistemi informativi ed alla necessità urgente che questi si rinnovino non solo per cogliere le opportunità legate alla modernizzazione ma anche per concorrere a ricomporre quel conflitto, superando le arretratezze di oggi.

Questi due diritti non sono, infatti, inconciliabili: fare le cose "fatte bene", sia dal punto di vista organizzativo sia tecnologico, permette di innovare e rinnovare, di curare e tutelare, trovando anche un equilibrio sostenibile tra tutti gli interessi ed i diritti coinvolti nel percorso di cura.

Fare le cose bene permette di porre le domande giuste ai diversi *stakeholder* che condizionano moltissimo il rinnovamento e di ottenere risposte utili:

- nuove interpretazioni all'Autorità Garante per la protezione dei dati personali anche alla luce del nuovo Regolamento Europeo per la *Data Protection*;
- maggiore attenzione alla Direzione Generale per tutto quanto attiene allo sviluppo dei Sistemi Informativi considerando che essi sono, in tutti i settori industriali, sanità compresa, un fattore abilitante essenziale;
- un atteggiamento propositivo ai fornitori per aiutare le aziende sanitarie a capire le sfide tecnologiche e ad investire nella direzione giusta, lungo percorsi sostenibili sia sul piano economico sia su quello organizzativo.

I PDTA (Percorsi Diagnostici Terapeutici Assistenziali) sono al centro della riflessione di questo documento e della proposta di cui è portatore perché le sfide relative alla Cura e alla Privacy sono acuite nel contesto di trattamenti che attraversano i confini organizzativi e tecnologici di diversi soggetti coinvolti nella cura come ad esempio Medici, Ambulatori e Ospedali.

In questo senso i PDTA indicano oggi una strada che sarà percorsa, in vario modo, da tutta la sanità.

Il gruppo di lavoro che ha prodotto questo documento è nato dal dibattito di ottobre: un gruppo costituito da voci diverse, portatrici di punti di vista differenti. Si sono amalgamati avvocati e tecnologi, fornitori e clienti, consulenti e operatori senza che una voce particolare sovrastasse le altre, nella consapevolezza che le proposte debbano avere senso da ogni punto di vista.

In appendice si trovano i nomi degli autori, qui si ringraziano le Associazioni e le Aziende che l'hanno reso possibile:

AISIS - Associazione Italiana Sistemi Informativi in Sanità

APIHM - Associazione Privacy and Information Healthcare Manager

CLUSIT - Associazione Italiana per la Sicurezza Informatica

Azienda Unità Sanitaria Locale di Modena

Dedalus

Istituto Auxologico Italiano

NoemaLife

Oracle Italia

P4I

Studio Legale Stefanelli

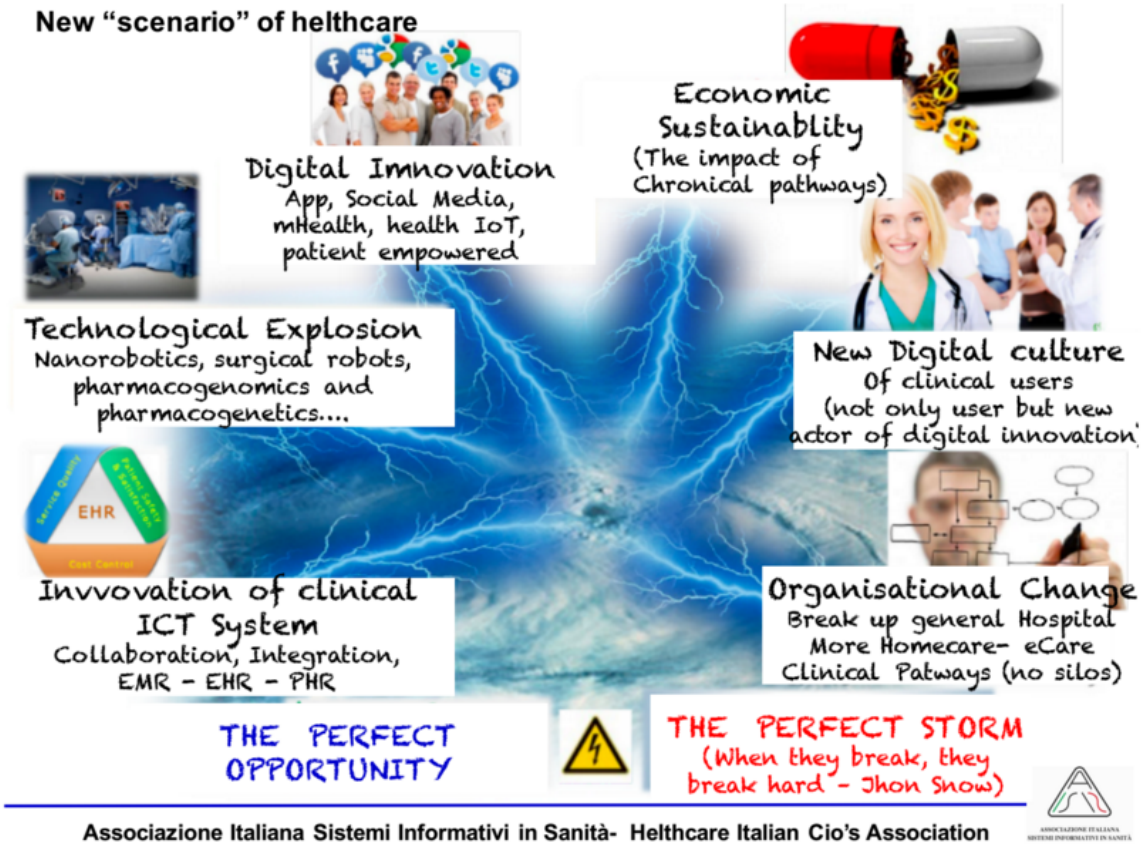
Studio Storti

Zeropiù

Sommario

Scenario

Ricerche empiriche e letteratura scientifica concordano sull'evidenza dell'**e-health** come nuovo paradigma culturale, organizzativo e tecnologico destinato, nei prossimi anni, a modificare sensibilmente la sanità a livello internazionale. Tale scenario, i cui tratti sono presenti anche nel sistema sanitario italiano, è caratterizzato da alcuni aspetti distintivi che sono sintetizzati nella figura seguente:



- esplosione dei costi (e conseguente pressione sul controllo) dovuti da un lato all'aumento progressivo dell'invecchiamento e delle malattie croniche multifattoriali e dall'altro dalla disponibilità di tecnologie (costose) fortemente orientate alla personalizzazione della salute;
- personalizzazione della salute che viene supportata da una consistente disponibilità di nuove tecnologie: dalla medicina predittiva, alla farmaco genetica-genomica, alla sperimentazione della chirurgia robotica, all'analisi di big data "clinici" per lo scoring diagnostico-terapeutico, con conseguente necessità di adottare modelli organizzativi in grado di riprogettare servizi e percorsi che consentono di affermare una prospettiva di presa in carico "totale" della persona che ha un problema di salute per la gestione della quale diventano sempre più necessari interventi multiprofessionali, multidisciplinari (dalla pre-

venzione alla riabilitazione alla assistenza) che avvengono in momenti e luoghi diversi e dal cui workflow dipende il risultato stesso del processo diagnostico terapeutico assistenziale;

- consolidamento ed espansione dell'innovazione digitale a tutti i livelli di vita professionale e personale, sanitaria compresa: apps, social media, m-health, Health IoT, weareable, che determinano un empowerment del cittadino/utilizzatore dei servizi digitali: un cittadino 2.0 che è disponibile a ricercare l'eccellenza del servizio, a valutare alternative per la gestione della propria cura-benessere, abituato ad un modello di servizi *on line* e *on time* che già utilizza in altri settori (prenotazione, pagamento e download online, chat multicanale, disponibilità informazioni 24x7), capace di adattare/modificare le proprie abitudini di vita in una logica di prevenzione supportata dalla tecnologia;
- nuova cultura digitale degli utilizzatori dell'ICT in sanità: clinici, infermieri, personale psico-socio assistenziale, cittadini stessi che richiedono nuovi servizi "information intensive" per gestire meglio il processo di presa in carico del cittadino che è sempre in misura maggiore un processo basato sulla mobilità sia del cittadino sia del team che lo prende in carico. In tale contesto l'ICT può consentire sia la realizzazione di nuove strategie organizzative necessarie per garantire percorsi di continuità assistenziale in una "rete trasversale" di servizi, sia nuove e più efficienti modalità di interazione 2.0 che facilitino l'accesso e la gestione proattiva della salute e dei dati clinici da parte dei cittadini, sia l'utilizzo di nuovi modelli di cura tramite dispositivi mobili in ospedale (BYOD), sia attraverso la realizzazione dell'Internet of Things (IoT) in sanità creando la nuova "smart health" in cui siano oggettivamente sostenibili processi B2P (Business to Person), P2P (Person to Person), P2M (Person to Machine) e M2M (Machine to Machine) in modalità facilitata e automatica riducendo errori di trascrizione/comunicazione e migliorando l'efficienza e la qualità dei dati clinici;
- passaggio da architetture "complesse" per lo scambio/consultazione/gestione delle informazioni cliniche e sociosanitarie del cittadino ad architetture "light" in una logica di Personal Health Record la cui proprietà del patrimonio informativo è del cittadino che in un approccio di gestione proattiva della propria salute (raccomandata dall'OMS) decide a chi, cosa e quando rendere disponibili i "propri" dati clinici;
- importanti modifiche nella struttura istituzionale-organizzativa del sistema sanitario (nazionale-regionali) dove si assiste ad una concentrazione dell'offerta (fusione di aziende sanitarie a formare bacini di utenza da 1.5ml di abitanti, fatturato intorno al 1 mld, 6-8.000 addetti), con specializzazione delle strutture ospedaliere e con un progressivo spostamento di una quota rilevante di attività sul territorio sino al domicilio del cittadino. In questo contesto si caratterizzano due tipologie di "pazienti":
    - cittadini orientati alla "self Health" che richiedono l'eccellenza della prestazione e sono disponibili a valutare l'equilibrio tra costi da sostenere (contribuzione diretta/assicurativa, disponibilità a spostarsi) e qualità della prestazione richiesta. In tale contesto non è eludibile il tema della "**sanità low cost/sanità privata**" considerando che circa 30 miliardi di euro vengono spesi dalle famiglie italiane per garantirsi il diritto alla salute, la cosiddetta "spesa sanitaria privata". Parliamo di

circa il 22% della spesa sanitaria totale. Il problema di un importante e crescente ricorso alla sanità privata determina impatti nella gestione dei dati clinici del paziente e pone interrogativi su come renderli disponibili al cittadino e ad altri *stakeholders* pubblici e privati che vengono coinvolti direttamente dal cittadino in un modello di self-health

- cittadini "fragili" che richiedono di essere presi in carico in un percorso di cura trasversale per loro predefinito. Tale approccio (PDTA) richiede la creazione di un nuovo modello organizzativo basato sulla gestione di workflow di processo che coinvolge attori diversi (sia personale sanitario, medico e/o infermieristico, sia personale socio-assistenziale, caregiver e cittadini stessi), in momenti diversi e in luoghi diversi, con l'obiettivo di migliorare la governance di domanda e offerta, di favorire l'economicità di sistema e, da ultimo, di realizzare un modello di "presa in carico" che favorisca l'empowerment del paziente migliorandone la proattività e la responsabilizzazione sul processo di cura e sulla gestione del suo stile di vita.

Mai come ora per l'e-Health si prospetta una grande opportunità di crescita (o viceversa la "tempesta perfetta") attraverso lo sviluppo di "servizi" che possono oggettivamente favorire nuove modalità di interazione con i cittadini, di loro presa in carico, di servizi efficienti per i professionisti che sono coinvolti nei loro processi di cura.

La rilevante complessità che scaturisce da questo scenario suggerisce cautele ed investimenti specifici almeno su tre aree critiche che, al contrario e con una certa frequenza nel mondo della sanità, non trovano adeguate attenzioni:

- **disponibilità 24x7 dei dati**: cittadini e professionisti sono abituati a poter accedere alle informazioni "sempre" e "da ogni luogo". Ciò richiede alle Aziende Sanitarie la capacità di poter disporre di infrastrutture tecnologiche che realizzino concretamente business continuity e disaster recovery. Recenti ricerche hanno dimostrato la fragilità e l'inadeguatezza delle server farm della PA ed in particolare delle strutture sanitarie. I nuovi processi di "fusione" delle Aziende Sanitarie possono essere un'opportunità per la qualificazione dell'infrastruttura tecnologica creando soluzioni anche tier6[1] laddove le componenti regionali consentano lo sviluppo sovrazonale di architetture per il Disaster Recovery;
- **privacy, sicurezza e integrità dei dati**: la qualità dei dati sociosanitari ed il livello della loro "sensibilità" in termini di privacy richiedono infrastrutture sicure, che garantiscano una gestione degli accessi all'infrastruttura e ai dati solo alle persone autorizzate (diffusione di adeguati sistemi di Identity Management), che consentano un'adeguata cifratura dei dati sia a livello di networking, sia a livello di file system o database. A maggior ragione dato che i processi organizzativi sia a livello ospedaliero (letto del paziente) sia a livello di percorsi trasversali ospedale-territorio (PDTA) verranno effettuati in mobilità e quindi con interscambio di informazioni tra persone diverse, in tempi e luoghi diversi.

[1] Linee Guida per il Disaster Recovery delle Pubbliche Amministrazioni, Agid, 2013

L'integrità dei dati, rafforzata dall'adozione di tecnologie ormai in uso corrente, come ad esempio la firma digitale, appare un requisito irrinunciabile di interoperabilità dei dati che vengono scambiati in queste nuove modalità organizzative;

- **customer experience**: come in altri settori verticali cittadini e professionisti richiedono servizi che valorizzino la loro esperienza d'uso. La customer experience è una capacità manageriale di gestire tutte le interazioni con i diversi "attori" del mondo sanitario al fine di coglierne le esigenze e di anticipare nuove modalità di servizi "information intensive". Perseverare nella fornitura di soluzioni che sono mediamente obsolete (anche in termini di presentation/frontend) tende a generare una disaffezione all'uso dell'innovazione digitale o a favorire proposte fantasiose come quella che siano i medici a sviluppare le applicazioni o i sistemi informativi per la sanità. L'attenzione agli aspetti di customer experience degli "utilizzAttori" delle tecnologie rappresenta l'unica possibilità di fornire servizi information intensive che qualificano nuove modalità organizzative di gestione dei processi sociosanitari, un'interazione efficiente tra cittadini e strutture sociosanitarie, interazioni efficaci tra professioni e cittadini con garanzie di continuità operativa, sicurezza e rispetto dei requisiti di privacy che tutelano professionisti e cittadini stessi.

La complessità crescente dei modelli organizzativi della sanità, illustrata nei paragrafi precedenti, impone una revisione delle architetture informatiche sottostanti, in particolare in quanto tale complessità deriva dalla necessità strutturale di condividere informazioni tra soggetti diversi, tutti coinvolti nell'erogazione dei medesimi servizi sanitari, al fine di assicurare al paziente un unico percorso di cura fortemente personalizzato.

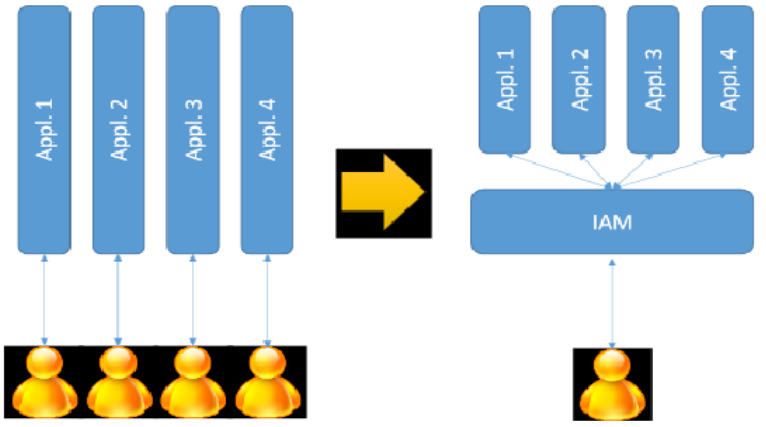


Figura 1 - Creare una piattaforma di IAM

Due aspetti, innanzitutto, caratterizzano questa esigenza.

Da un lato vi è la necessità di consentire l'accesso ai servizi a diverse categorie di utenti, garantendo nel tempo la coerenza dei diritti d'accesso con il ruolo effettivamente svolto da ciascuno in quel momento.

Tra questi, sia figure professionali, appartenenti a uno qualsiasi dei soggetti erogatori dei servizi che costituiscono il percorso di cura, sia utenti del servizio stesso, sia soggetti esterni coinvolti per motivi amministrativi o altro: ciascuna di queste categorie con privilegi coerenti con la funzione svolta.

Dall'altro vi è la necessità di gestire un percorso di cura che nasce trasversale alle diverse organizzazioni della sanità pubblica e privata che sono coinvolte nella sua erogazione anche quando appartengono a contesti territoriali distanti tra loro e sono soggetti ad amministrazioni diverse.

La continua evoluzione della tecnologia (in particolare cloud e dispositivi mobili) e delle abitudini d'uso della stessa da parte di cittadini e professionisti che ne conseguono, impone poi di considerare un ulteriore aspetto della trasformazione dei modelli operativi.

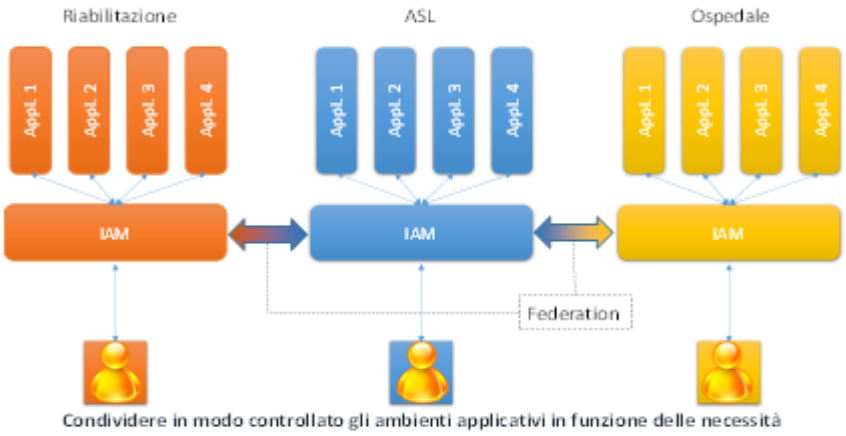


Figura 2 - Federare ambienti di diversi operatori

Non è un tema che riguarda il domani. Già oggi, infatti, non è possibile sottrarsi alla necessità di razionalizzare e controllare gli accessi ai diversi servizi da parte di applicazioni, che siano app fruite su dispositivo mobile o parte del patrimonio di organizzazioni terze, attivate da operatori professionali interni al SSN o da utenti del servizio stesso.

Per quanto riguarda i primi due temi, la risposta all'esigenza evidenziata consiste, innanzitutto, nel trasferimento delle logiche e dei processi di autenticazione e autorizzazione degli utenti dalle piattaforme applicative ad una piattaforma di Identity & Access Management posta a livello infrastrutturale (Figura 1).

Queste piattaforme, realizzate autonomamente da ciascun soggetto erogatore dei servizi possono essere fra loro federate per garantire il necessario livello di interoperabilità (Figura 2) fra tutte le organizzazioni interessate o coinvolte nel percorso di cura.

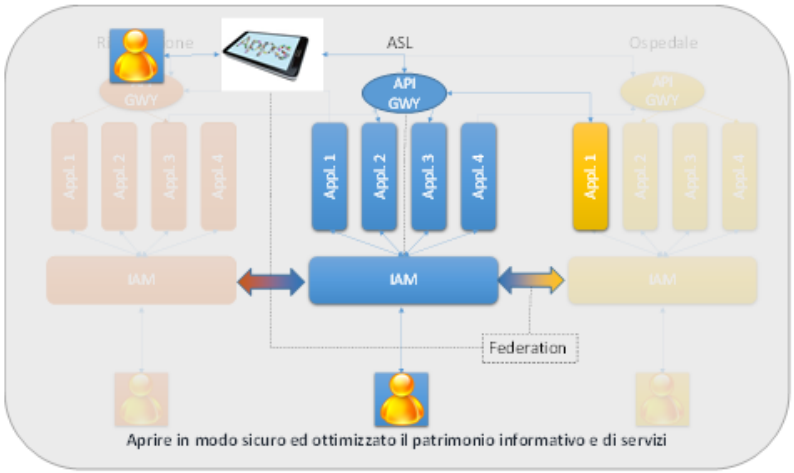


Figura 3 - Adottare un API Gateway

In questa direzione si muove, peraltro, l'intero mondo delle amministrazioni pubbliche, in ambito sanitario e non, con la realizzazione di SPID.

L'ulteriore tematica da considerare riguarda la crescente esigenza di consentire l'accesso a informazioni e servizi da parte di applicazioni esterne al perimetro di ciascuna organizzazione garantendo i medesimi standard di sicurezza e le medesime politiche di accesso.

Anche questa esigenza richiede una risposta infrastrutturale nuova, costituita da un API gateway centralizzato (Figura 3) che applichi alle richieste di accesso le policy operative e di sicurezza in vigore presso il soggetto interessato. Rientrano in questo scenario, ad esempio, le app

utilizzabili in mobilità da utenti del servizio e da operatori esterni alle organizzazioni erogatrici come professionisti privati, laboratori, farmacie, così come funzionalità eventualmente attivate da soggetti esterni come le amministrazioni locali competenti per territorio.

Il quadro legislativo di riferimento

La disciplina della privacy impatta fortemente in ambito sanitario in ragione della delicatezza delle informazioni trattate dagli operatori sanitari addetti ai percorsi di cura.

L'affermarsi di nuovi strumenti, processi e modelli organizzativi impone di affrontare e risolvere problematiche specifiche che assicurino che l'erogazione della cura sia al contempo efficace, economica e supportata da tecnologia avanzata ma che altresì rispetti contestualmente i diritti alla riservatezza e protezione dei dati del paziente.

Ciò vale anche per i Percorsi Diagnostici Terapeutici Assistenziali. Prima però di affrontare in dettaglio il tema specifico dei PDTA, è opportuno ripercorrere brevemente gli istituti generali della privacy approfondendo poi i temi specifici del settore sanità, con uno sguardo anche alla nuova disciplina che verrà introdotta dall'emenando nuovo Regolamento UE.

Il D.Lgs. 196/2003

Il D.Lgs 196/2003, comunemente conosciuto come Codice Privacy, attua nel nostro ordinamento la Direttiva 95/46/CEE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

Si tratta del testo cardine in materia di tutela dei dati, che deve però essere letto, interpretato ed applicato in maniera integrata con gli specifici provvedimenti emessi dal Garante per la Protezione dei Dati Personali. Nel seguito ne sono riportati alcuni punti chiave

a. I soggetti che operano in ambito privacy

Il Codice Privacy disciplina con precisione quali sono i soggetti che operano in ambito privacy:

- Il Titolare del trattamento (articolo 4, comma 1, lett. F Codice Privacy)

  è "*la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza*".

  La norma stabilisce che si qualifica come "titolare" il soggetto che decide ed effettua le scelte di fondo circa le finalità e le modalità di trattamento dei dati nonché i profili di sicurezza degli stessi [1].

  Questi può esercitare la funzione "*anche unitamente ad altro titolare*": quindi il Codice ammette, senza però introdurre alcuna disciplina specifica, la possibilità giuridica che più soggetti possano trovarsi contemporaneamente, ciascuno per la propria area di competenza, ad essere e agire come Titolare del trattamento: in tal caso [2] si ha la c.d. co-titolarità del trattamento dei dati.

- Il Responsabile del trattamento (articolo 4, comma 1, lett. g) Codice Privacy)

  è "l*a persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali*".

  E' figura non obbligatoria [3] che, se nominata, tratta i dati (con mandato più o meno ampio a seconda della necessità) secondo le direttive imposte dal Titolare [4], che ha l'obbligo di vigilare sulla loro puntuale osservanza e sul rispetto delle disposizioni in materia (articolo 29, comma 5 codice privacy) [5].

  Il Titolare mantiene una precisa responsabilità in *eligendo* e in *vigilando* tipica delle deleghe di funzioni [6] nei confronti del Responsabile del trattamento.

  Come sostenuto più volte dal Garante per individuare correttamente il responsabile del trattamento è necessario verificare *in quale modo* siano gestiti i dati in rapporto all'organizzazione interna della struttura (società o ente) titolare del trattamento anche alla luce dei rapporti con soggetti esterni di cui si serve per espletare le proprie funzioni [7].

- Gli Incaricati del trattamento, (articolo 4 comma 1 lett. h) Codice Privacy)

  Sono "*le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile*".

  Gli incaricati del trattamento sono esclusivamente persone fisiche (e non persone giuridiche o associazione) che materialmente trattano i dati in conformità alle istruzioni operative fornite dal titolare o dal responsabile, concretandosi così una diretta gerarchia tra titolare e/o responsabile ed incaricati

- Amministratori di Sistema

  L'amministratore di sistema è la figura professionale preposta alla gestione tecnica degli strumenti elettronici utilizzati nei trattamenti di dati personali.

  La disciplina non è contenuta nel Codice ma nel Provvedimento Garante Privacy 27 novembre del 2008 *"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"* con il quale vengono individuate le misure e gli adempimenti necessari per una corretta gestione tecnica degli strumenti elettronici.

b. Gli adempimenti relativi al trattamento dati

- Informativa (art 13, 78 e 79)

  L'informativa è la condizione che, dal punto di vista giuridico, legittima qualsiasi trattamento di dati: consiste nell'attività di informazione all'interessato sul trattamento che si va ad effettuare.

  L'art. 13 del Codice Privacy[10] stabilisce, in via generale, che il titolare del trattamento di dati è obbligato a dare informazioni all'interessato sulla natura obbligatoria o facoltativa del conferimento dei dati, sulle conseguenze di un rifiuto di rispondere, sull'ambito di diffusione dei dati, sui diritti dell'interessato e gli estremi identificativi del titolare del trattamento stesso.

Per quanto riguarda lo specifico ambito sanitario, l'informativa trova specifica disciplina agli art. 77, 78 e 79. Più precisamente l'art. 77 stabilisce, in via generale, la possibilità di una informativa semplificata rispetto a quella generale dell'art. 13 per il trattamento effettuato da esercenti le professioni sanitarie nonchè dalle strutture sanitarie pubbliche e private.

Il successivo art. 78 (relativo a medici di base e pediatri) regola poi le modalità di tale semplificazione. Più esattamente, per quanto rilevante in questa sede, stabilisce che l'informativa può riguardare:

- il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione;
- dati personali eventualmente raccolti presso terzi;
- i dati correlati in caso di sostituzione o per prestazione specialistica su richiesta del medico e del pediatra.

Lo stesso art. 78 stabilisce poi che nel caso in cui il trattamento dei dati presenti rischi specifici, questi ultimi devono essere evidenziati analiticamente: tra tali rischi è espressamente indicato il trattamento dei dati nell'ambito della teleassistenza o telemedicina nonché l'ipotesi in cui si forniscano altri beni o servizi attraverso una rete di comunicazione elettronica.

Di estrema importanza poi ai fini del presente lavoro è il successivo art. 79 che riguarda l'informativa da parte di strutture sanitarie pubbliche e private. La norma, oltre a stabilire che le stesse "possono" avvalersi delle modalità semplificate, ammette la possibilità di un'unica informativa in due ipotesi:

- nel caso di pluralità di prestazioni erogate all'interno di uno stesso organismo, anche in distinti reparti ed unità dello stesso;
- nel caso di pluralità di prestazioni erogate da più strutture ospedaliere o territoriali, a condizione che le stesse siano specificamente identificate.

Nei casi sopra individuati è necessario poi che l'organismo o le strutture annotino l'avvenuta informativa con modalità uniformi e tali da permettere una verifica da parte di altri reparti ed unità che, anche in tempi diversi, trattino dati relativi al medesimo interessato, in maniera tale che tutti i soggetti siano resi edotti e consapevoli dell'avvenuta informativa.

Inoltre lo stesso art. 79 al comma 4 stabilisce che, ove si adottino adeguate misure organizzative, le modalità semplificate possono essere utilizzate sia nel caso di più trattamenti dati effettuati nei casi disciplinato dallo stesso art. 79, sia nel caso di trattamento dati effettuato da altri soggetti pubblici operanti in ambito sanitario.

L'omissione o l'inidoneità dell'informativa possono comportare, nel caso di dati sensibili, una sanzione amministrativa da 5.000 a 30.000 euro (con possibilità di aumento sino al triplo) (art. 161 Codice Privacy).

- Consenso (art. 23, 81)

L’art. 23 sancisce la regola generale secondo la quale il trattamento di dati è ammesso solo con il consenso espresso dell'interessato che è una "manifestazione di volontà libera, specifica e informata"[12]. Lo stesso art. 23 stabilisce poi nel caso che il trattamento riguardi dati sensibili il consenso deve essere manifestato in forma scritta.

Seppure le pubbliche amministrazioni siano esonerate in via generale dall’acquisizione del consenso (art. 20), tale eccezione non opera per il trattamento di dati di salute per fini di cura, per il quale si torna alla disciplina generale dell’obbligo di acquisizione del consenso.

Per quanto riguarda poi tale obbligo in capo alle strutture sanitarie l’art. 81 stabilisce che le stesse possono raccogliere il consenso anche in forma orale, documentandolo con annotazione scritta dell'esercente la professione sanitaria o dell'organismo sanitario pubblico.

Per quanto rileva in questa sede, poi, quando l’informativa è resa per più soggetti, l’acquisizione del consenso è resa conoscibile ai medesimi soggetti attraverso adeguate modalità (ad esempio menzione, annotazione o apposizione di un bollino o tagliando su una carta elettronica o sulla tessera sanitaria) in modo tale da richiamare i trattamenti per i quali il consenso è stato acquisito nonchè eventuali diverse specificazioni apposte all'informativa (ad esempio il trattamento dei dati tramite sistemi di telemedicina o teleassistenza).

- Autorizzazione (art. 26)

  Il codice prevede che i dati sensibili possono essere oggetto di trattamento non solo con il consenso scritto dell'interessato, ma altresì previa autorizzazione del Garante (art. 26).

  Il Garante può adottare Autorizzazioni di carattere generale (art. 40) finalizzate a prescrivere misure uniformi a garanzia degli interessati, rendendo quindi superflua la richiesta di singoli provvedimenti di autorizzazione da parte di numerosi titolari del trattamento.

  Per le strutture sanitarie e gli esercenti le professioni sanitarie è oggi in vigore l’Autorizzazione n. 2/2014 – “Autorizzazione al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale per gli esercenti le professioni sanitarie” [13]. Il titolare per svolgere un trattamento che non rientra in una delle autorizzazioni generali, può richiedere al Garante un’autorizzazione “ad hoc”.

- Notificazione (art. 37)

  Il Titolare del trattamento è tenuto a notificare al Garante i trattamenti dei dati personali previsti dall’art. 37 del Codice. La notifica così effettuata è consultabile sull’apposito registro telematico; tra i casi di trattamenti da notificare di specifico interesse del settore sanitario possiamo citare, ad esempio quelli in cui il trattamento riguarda:

  - *dati genetici, biometrici o dati che indicano la posizione geografica di persone od oggetti mediante una rete di comunicazione elettronica;*
  - *dati idonei a rivelare lo stato di salute e la vita sessuale, trattati a fini di procreazione assistita, prestazione di servizi sanitari per via telematica relativi a banche*

di dati o alla fornitura di beni, indagini epidemiologiche, rilevazione di malattie mentali, infettive e diffusive, sieropositività, trapianto di organi e tessuti e monitoraggio della spesa sanitaria."

L'elenco di cui all'articolo 37 ha creato diversi problemi e dubbi interpretativi e per tale ragione il Garante è intervenuto a escludere esplicitamente alcune categorie di trattamento dall'obbligo di notifica e ad esplicitare l'applicazione dell'art. 37 attraverso il provvedimento n.1 del 31 marzo 2004[14] ed il parere del 23 aprile 2004[15].

c. Misure minime e idonee di sicurezza

Il Codice individua nell'apposito "Allegato B-Disciplinare tecnico in materia di misure minime di sicurezza" le misure di sicurezza di base (chiamate appunto "misure minime"), la cui osservanza da parte del Titolare è necessaria affinché sia assicurato un livello di protezione dei dati personali al di sotto del quale non si può scendere.

Questi però deve assicurare comunque che i dati personali siano "*custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta*" (art. 31).

In sintesi il Titolare è tenuto ad implementare il livello "minimo" di protezione che si realizza applicando le misure previste dal Codice con ulteriori misure di sicurezza non individuate specificatamente dal Codice che, tuttavia, si configurano come "idonee" (rectius necessarie) a meglio tutelare la riservatezza e l'integrità dei dati.

Sul punto si è espresso lo stesso Garante - parere 22 marzo 2004[17] – il quale ha precisato che mentre il rispetto delle "misure minime" vale a evitare le sanzioni penali, l'adozione di "misure ulteriori" consente di evitare anche il risarcimento del danno.

Il Garante poi, in forza del potere conferitogli dall'art. 154 comma 1 lett c), può intervenire, ove lo reputi necessario, per dettare specifiche regole e misure che alzino e garantiscano una maggior sicurezza nel trattamento dei dati: è il caso del Provvedimento 4 giugno 2015 sul Dossier Sanitario Elettronico, con il quale il Garante ha sancito l'obbligo di ulteriori misure di sicurezza necessarie o opportune per rendere sicuro il trattamento dei dati stessi.

Norme specifiche per la sanità: Fascicolo Sanitario Elettronico

Come sopra anticipato, nel corso del tempo sono state poi emanate discipline specifiche per il settore della sanità elettronica.

Con il Provvedimento del 16 luglio 2009 "Linee Guida in tema di Fascicolo Sanitario Elettronico (Fse) e di Dossier Sanitario" (http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116), il Garante, nelle more di un intervento legislativo, emanava specifiche regole per la gestione del FSE e del Dossier Sanitario; tali Linee Guida riportano di fatto la prima definizione e regolazione del Fascicolo e del Dossier Sanitario Elettronico.

Successivamente il Ministero della Salute, a seguito di una intesa della Conferenza Stato-Regioni, adottava in data 10 febbraio 2011 le “Linee Guida nazionali per la realizzazione di un sistema di Fascicolo Sanitario Elettronico”, con le quali venivano individuate le caratteristiche del FSE e del patient summary, gli aspetti infrastrutturali e gli standard tecnologici, i livelli di sicurezza e di protezione dei dati.

Con il successivo Decreto Legge 18 ottobre 2012, n.179, convertito con modificazioni dalla legge 17 dicembre 2012, n. 221 recante «Ulteriori misure urgenti per la crescita del Paese», il legislatore disciplinava il FSE come “l'insieme dei dati e documenti digitali di tipo sanitario e socio-sanitario generati da eventi clinici presenti e trascorsi, riguardanti l'assistito”.

L’art. 12 di tale legge, titolato appunto ”Fascicolo sanitario elettronico e sistemi di sorveglianza nel settore sanitario”, stabilisce l’architettura di massima del FSE, rinviando per la completa implementazione a successivi decreti, ancor oggi in corso di emanazione; la stessa norma sancisce poi che il FSE è istituito dalle regioni e province autonome, nel rispetto della normativa vigente in materia di protezione dei dati personali, ai fini di prevenzione, diagnosi, cura e riabilitazione, nonché studio e ricerca scientifica in campo medico, biomedico ed epidemiologico, programmazione sanitaria, verifica delle qualità delle cure e valutazione dell'assistenza sanitaria.

La stessa norma stabilisce poi che il FSE 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, nonchè con i dati medici in possesso dello stesso cittadino che può provvedere ad inserirli personalmente nel FSE, per la cui completa attivazione dovranno essere adottati taluni DPCM, di cui il primo è il n.178 del 29 settembre 2015,”Regolamento in materia di fascicolo sanitario elettronico”.

Norme specifiche per la sanità: il Dossier Sanitario Elettronico

Il Dossier Sanitario Elettronico è invece strumento di sanità digitale disciplinato oggi solo da due provvedimenti del Garante Privacy.

Il primo è il già citato Provvedimento del 16 luglio 2009 “Linee Guida in tema di Fascicolo Sanitario Elettronico (Fse) e di Dossier Sanitario” con il quale si definivano le caratteristiche e l’impianto regolatorio del Dossier (anche se in tale documento lo strumento Dossier pareva essere considerato di minor rilevanza rispetto al Fascicolo Sanitario).

Successivamente il Garante, anche a seguito di una serie di ispezioni svolte presso alcune aziende sanitarie nel corso delle quali erano emerse svariate non conformità nella creazione e gestione dei Dossier, ha ritenuto necessario ed opportuno adottare uno specifico Provvedimento titolato “Linee Guida in tema di Dossier Sanitario Elettronico” emanato il 4 giugno del 2015.

Il Dossier Sanitario Elettronico è “lo strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (es.: ospedale, azienda sanitaria, casa di cura) al cui interno operino più professionisti, attraverso il quale sono rese accessibili informazioni, inerenti allo stato di salute di un individuo, relative ad eventi clinici presenti e trascorsi (es.: referti di laboratorio, documentazione relativa a ricoveri, accessi al pronto soccorso), volte a documentarne la storia clinica”.

In sintesi, le caratteristiche del Dossier sono la titolarità unica, l'accessibilità da parte di più professionisti e la raccolta di eventi clinici presenti e trascorsi atti a documentare la storia clinica del paziente.

Per tale strumento le prescrizioni specifiche previste dal Garante sono le seguenti.

- Informativa al trattamento dei dati tramite Dossier

  Il Garante ritiene che il trattamento dei dati effettuato tramite il Dossier sanitario costituisca un trattamento ulteriore, autonomo, specifico e facoltativo rispetto a quello effettuato dal professionista sanitario con le informazioni acquisite in occasione della cura di un singolo evento clinico del paziente.

  Per tale motivo, il trattamento dei dati personali del Dossier sanitario necessita di una specifica informativa che contenga tutti gli elementi previsti dall'art. 13 del Codice Privacy e di un corrispondente consenso autonomo, specifico e facoltativo, ulteriore rispetto a quello già espresso per il trattamento di dati di salute a fini di cura.

  Nell'informativa, che deve essere fornita al paziente prima dell'acquisizione del consenso e deve essere facilmente consultabile da questi anche successivamente alla prestazione del consenso stesso, occorre inserire:

  - i soggetti o le categorie di soggetti ai quali i dati personali trattati mediante il Dossier sanitario possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati (compresi eventualmente i professionisti in regime di c.d. intramoenia);
  - gli specifici criteri di profilazione degli utenti adottati e una breve descrizione delle misure che sono state poste in essere per la protezione dei dati da specifici rischi di accesso non autorizzato e di trattamento non consentito, unitamente a quelle individuate per garantire l'esattezza, l'integrità e la continuità della fruibilità dei dati;
  - le persone fisiche legittimate a consultare il Dossier devono inoltre essere adeguatamente edotte in merito alle modalità di utilizzazione di tale strumento e delle misure adottate per la tutela dei dati personali trattati.

- Il consenso al trattamento dei dati

  Il paziente deve esprimere un autonomo consenso al trattamento dei dati tramite Dossier, in mancanza del quale questo non può essere utilizzato.

  Il titolare del trattamento, inoltre, deve acquisire una specifica manifestazione di volontà dell'interessato qualora nel Dossier siano inserite anche informazioni relative a prestazioni sanitarie offerte a soggetti nei cui confronti l'ordinamento vigente ha posto specifiche disposizioni a tutela della loro riservatezza e dignità personale: si tratta, in particolare, dei dati soggetti a maggiore tutela dell'anonimato, ovvero relativi ad atti di violenza sessuale o di pedofilia, all'infezioni da HIV o all'uso di sostanze stupefacenti, di sostanze psicotrope e di alcool, alle prestazioni erogate alle donne che si sottopongono a interventi di interruzione volontaria della gravidanza o che decidono di partorire in anonimato e ai servizi offerti dai consultori familiari.

- I diritti dell'interessato ed oscuramento dei dati

  L'interessato può richiedere l'oscuramento di parte del suo Dossier Sanitario. In questo caso dati ed informazioni restano comunque disponibili al professionista sanitario o alla struttura che li ha raccolti o elaborati (ad es.: referto accessibile tramite dossier da parte del professionista che lo ha redatto, cartella clinica accessibile da parte del reparto di ricovero). Il Titolare del trattamento dei dati del Dossier Sanitario deve informare i soggetti abilitati ad accedervi della possibilità che questo possa non essere completo in quanto l'interessato potrebbe aver esercitato il diritto di oscuramento.

- La sicurezza dei dati

  Il Garante, vista la particolare delicatezza dei dati personali trattati mediante il Dossier Sanitario, prescrive al Titolare di adottare specifiche misure di sicurezza, in particolare per:

  - proteggere l'identità del paziente e utilizzare canali di comunicazione sicuri;
  - adottare sistemi di autenticazione e autorizzazione che assicurino l'accesso selettivo ai dati in linea con i principi di necessità, pertinenza, non eccedenza e indispensabilità;
  - individuare criteri e modalità per la separazione e la cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale degli interessati;
  - registrare le operazioni di accesso in appositi file di log ai fini della verifica della liceità del trattamento dei dati;
  - assicurare l'integrità, la disponibilità dei dati e il ripristino degli stessi in caso di guasti, malfunzionamenti o eventi disastrosi.

- Data Breach (comunicazione delle violazioni di dati personali)

  Il provvedimento del Garante prevede poi che, nel caso anche solo potenziale in cui i dati del Dossier Sanitario abbiano subito violazioni (data breach) o vi siano stati incidenti informatici (ad es. accessi abusivi, azione di malware, etc.), il titolare debba comunicare l'accaduto al Garante netro 48 ore dalla conoscenza del fatto.

  Si tratta, come nel punto che segue, di una anticipazione di quanto previsto nel nuovo Regolamento Europeo, seppure con qualche differenza, che verosimilmente sarà eliminata, dovuta alla evoluzione del testo europeo dopo l'approvazione del provvedimento del Garante italiano.

- Data Protection Officer

  Da ultimo, si segnala che l'Autorità garante, anticipando quanto previsto nel progetto del nuovo Regolamento Europeo sulla privacy, auspica che i Titolari del trattamento individuino una figura di responsabile della protezione dei dati, c.d. Data Protection Officer. La definizione dei compiti e del profilo di questa figura , inevitabilmente rimanda al GDPR che dedica 3 articoli a questo scopo.

Il nuovo Regolamento UE sulla protezione dei dati personali (GDPR).

La riforma dell'impianto normativo europeo per la protezione dei dati, avviata nel 2012 dalla Commissione Europea, sta superando una fase critica con l'approvazione della General Data Protection Regulation (GDPR) pubblicato nel GUCE il 14.4. Il GDPR è un provvedimento normativo il cui impatto si preannuncia più o meno dirompente a seconda dei diversi ordinamenti nazionali. Nell'ordinamento italiano l'impatto del GDPR è commisurato alla portata altamente innovativa delle previsioni ivi contenute e alla sua natura regolamentare che lascia un ridotto margine di manovra ai singoli stati. Aspirando alla creazione di un impianto normativo omogeneo a livello continentale, il regolamento promuove la collaborazione tra autorità di controllo tramite un apposito meccanismo di coerenza (art.57-61) e tramite l'istituzione di un organismo di controllo, coerenza e cooperazione sovranazionale, il Comitato Europeo per la Protezione dei Dati (art. 64-72).

Un trattamento sistematico del testo del GDPR esula dagli obiettivi di questo documento e, pertanto, ci limitiamo qui ad indicare alcuni aspetti della nuova normativa che potrebbero avere impatti rilevanti per i temi trattati.

Per evitare fraintendimenti puramente terminologici, di seguito verranno usati i termini inglesi "*controller*" e "*processor*" per indicare i soggetti che, nella vigente normativa italiana, sono chiamati Titolare e Responsabile del trattamento. La figura attualmente definita Incaricato non è presente nel testo. In merito all'articolo 27 GDPR "*..any person acting under the autority of the controller or the processor who has access to the data*..." si conferma che anche le attività operative devono essere svolte dagli addetti secondo istruzioni e, dunque, sotto la responsabilità del controller o del processor.

Gli interessati, oltre ad essere tutelati mediante principi e diritti analoghi a quanto attualmente vigente, sono titolari di diritti introdotti *ex-novo* dal presente regolamento. Tra questi annoveriamo il diritto all'oblio (Art.17) e quello alla portabilità dei dati (Art.18): quest'ultimo rileva in materia di dati sanitari, per una sua efficace implementazione, l'uso di formati aperti e interoperabili, non solo con riguardo ai dati, ma anche eventuali metadati (ivi inclusi meccanismi per il tracciamento del consenso) e protocolli di comunicazione.

Inoltre dovranno essere previsti strumenti appositi per garantire questo diritto in caso, ad esempio, di trasferimento dell'interessato in un altro territorio.

Il GDPR introduce in modo formale ed esplicito il concetto di *Joint Controller* al primo comma dell'articolo 24: "*Where two or more controllers jointly determine the purposes and means of the processing of personal data, they are joint controllers."*

Ad una prima lettura, il concetto di joint controller consente di inquadrare il PDTA come un trattamento che si svolge sotto la responsabilità condivisa di più soggetti, ognuno dei quali è intestatario di un ruolo specifico, codificato in un accordo formale che deve essere messo a disposizione dell'interessato, concetto che sarà ripreso nel seguito del documento. Da notare come la distribuzione delle responsabilità tra i joint controller ha valore tra le parti, mentre l'interessato può far valere i propri i propri diritti *"in respect of and against each of the controllers"* a prescindere dal sopracitato accordo.

Per quanto riguarda la sicurezza, il GDPR cambia l'approccio da prescrittivo ad organizzativo, introducendo in capo al Controller la responsabilità di implementare sistemi che garantiscano il rispetto dei principi di *Data Protection by design* e *by default*, il *Record of processing activities* ed in alcuni casi il *Data Protection impact assessment* costituito da un analisi e valutazione sistematica dei trattamenti e dall'analisi dei rischi.

Altra novità in tema di sicurezza è l'obbligo di comunicazione dei *data breach* entro 72 ore dalla scoperta, all'autorità di controllo (art.31) o agli interessati (art.32), a seconda della gravità della violazione e delle misure di sicurezza adottate.

Queste prescrizioni sono tanto più significative in quanto precedute dall'art. 22 il quale sancisce che "*the controller shall implement appropriate technical and organisational measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation*": quello che ne deriva è la necessità di un cambio di atteggiamento radicale nell'approccio all'intera tematica della compliance, necessità rafforzata da sanzioni assai significative (fino a 20 Ml€ o al 4% del fatturato globale) e da un profilo di responsabilità verso terzi assai più impegnativo, anche per i processor eventualmente coinvolti nel trattamento.

A completare il quadro, coerentemente con quanto sopra esposto, vi è la figura del Data Protection Officer (DPO) che sarà obbligatoria in caso di trattamento di dati sanitari.

Il DPO è una figura interna o esterna all'organizzazione, designata dal controller e/o dal processor per la sua competenza specifica che agisce in assenza di conflitto di interessi e senza ricevere istruzioni, informando e consigliando Controller e Processor, verificando la corretta applicazione delle disposizioni del GDPR e fungendo da punto di contatto per gli interessati e l'autorità di controllo.

Un ruolo cardine nell'impianto del regolamento è svolto dalla cosiddetta *Soft Law* costituita da Certificazioni e Linee guida. Se per le prime è necessario l'intervento di organismi di certificazione accreditati, ex regolamento 765/2008, per i codici di condotta l'onere-onore di curarne la redazione e di proporli all'autorità garante è demandato alle associazioni di categoria. Essendo il regolamento per sua natura generale ed astratto, quindi applicabile ad attività di trattamento estremamente eterogenee, le associazioni dei *Controller* e *Processor* sono nella posizione migliore per poter valutare le *best practices* da adottare a seconda dell'ambito di applicazione (in tale contesto si segnala che AISIS e APIHM sono associazione di categoria).

I due anni concessi dal testo per dare attuazione alle prescrizioni, sono, dunque, un lasso di tempo congruo e non sovrabbondante, per dare forma e sostanza ai tanti cambiamenti richiesti.

Per quanto di nuovo dovesse essere posto in essere dopo la pubblicazione in Gazzetta Ufficiale, il nuovo regolamento sarà comunque un riferimento normativo obbligato da subito.

Profili privacy nella gestione del PDTA

Il Garante Privacy è molto attento al controllo della gestione e della sicurezza dei dati nell'ambito della sanità elettronica: tale interesse è palesato anche dall'inserimento di tale settore nell'ambito delle verifiche ispettive per il primo semestre del 2016.

Questa informazione conferma ancora una volta la necessità di valutare anche per il PDTA, strumento per il quale mancano ad oggi specifiche misure in ambito di privacy, quali debbano essere le misure idonee ed opportune da adottare nel caso di attivazione di questo specifico strumento clinico.

Tale valutazione terrà conto delle indicazioni che il Garante Privacy ha prescritto nel corso degli ultimi anni relativamente alle problematiche della sanità elettronica nonché delle prescrizioni contenuti nel nuovo Regolamento UE.

In particolare è necessario, al riguardo, fare riferimento ai Provvedimenti che hanno interessato il Dossier Sanitario Elettronico.

Gli specifici accertamenti e verifiche ispettive del Garante sono stati finalizzati a verificare se i sistemi informativi che questi ha classificato come Dossier Sanitario fossero configurati in modo da rispettare le misure previste dalla legge privacy in generale e dalle specifiche Linee Guida.

Gli esiti di tali accertamenti e verifiche hanno evidenziato, anche nelle realtà sanitarie più avanzate sotto il profilo dell'utilizzo di sistemi di e-health, una sostanziale non corrispondenza con le succitate misure.

Le ispezioni e i conseguenti Provvedimenti hanno preso in esame i Dossier costituiti presso le Aziende Sanitarie Ospedaliero-Universitarie di Trieste, Bologna, Roma e le aziende sanitarie territoriali di Empoli e Bolzano.

Nell'ultimo caso l'attività del Garante Privacy, è stata avviata a seguito della comunicazione da parte del giudice di una sentenza che, nel riconoscere una violazione di segreto d'ufficio, evidenziava che la commissione di tale reato era stata resa possibile anche approfittando di una organizzazione del sistema informativo non del tutto adeguata; negli altri casi invece il Garante ha ricevuto delle segnalazioni da parte degli assistiti che lamentavano, in generale, di non essere stati informati e di non aver autorizzato il trattamento dei propri dati con modalità tali da consentire un accesso per via elettronica ad una serie di operatori delle strutture sanitarie alle quali si erano rivolti per le cure.

Il PDTA: esigenze cliniche e tutela dei dati personali

Sotto il profilo delle tutele e delle misure da adottare per assicurare un corretto ed efficiente trattamento di dati nel caso di PDTA , occorre tener presente la seguente situazione:

- il paziente viene inserito nell'ambito di un percorso di cura in ragione del suo specifico stato di salute, nel quale possono avere rilevanza anche i dati di salute pregressi disponibili presso altri attori del sistema sanitario;

- il percorso di PDTA vede coinvolti più soggetti che, solitamente, sono funzionalmente collegati a pubbliche amministrazioni sanitarie diverse (es. Ospedale, ASL, medico di medicina generale, specialista ambulatoriale ecc.);
- tali soggetti sanitari, a loro volta, generano dati sanitari che possono/devono essere conosciuti da tutti gli altri soggetti che intervengono nel percorso diagnostico terapeutico assistenziale.

Ci troviamo, quindi, nell'ambito di un trattamento di dati complesso che, purtroppo, non trova spontaneamente inquadramento né nella fattispecie del Dossier né in quella del Fascicolo Sanitario Elettronico (FSE), come precisato nel seguito:

a. Distinzione tra Dossier e PDTA

   La caratteristica del Dossier Sanitario è quella di raccogliere i dati anagrafici e sensibili, in particolare dati sanitari prodotti da "più processi di cura", presenti e passati relativi ad un unico paziente, ma generati da una stessa struttura sanitaria. In altre parole, nel caso del Dossier Sanitario il trattamento di dati viene gestito da un unico Titolare che tratta i dati sanitari generatisi anche nell'ambito dell'erogazione di cure relativi ad eventi clinici diversi ed anche in momenti temporali diversi.

   Il PDTA invece può essere concepito come un "unico processo di cura", ovvero relativo ad un univoco servizio nell'erogazione del quale però i dati sanitari vengono generati da soggetti diversi, ovvero titolari del trattamento diversi.

b. Distinzione tra FSE e PDTA

   Il FSE previsto dal D.L.gs 179 del 2012 è finalizzato a raccogliere a livello nazionale le informazioni relative all'intera storia clinica del paziente generatasi lungo tutta la vita dello stesso.

   Il PDTA invece raccoglie senza dubbio (come il FSE) dati generatisi anche a livello "sovra-aziendale" (cioè prodotti e conservati presso più titolari), ma questi sono relativi ad "un solo processo di cura" disegnato nello specifico percorso diagnostico terapeutico assistenziale.

In sostanza, dal punto di vista della tutela del dato, il PDTA presenta le seguenti caratteristiche:

- è un processo di cura, con unica finalità di trattamento, disegnato in via preventiva e che quindi consente di identificare con chiarezza in fase preventiva i co-titolari del trattamento;
- produce dati sanitari da parte di soggetti sanitari diversi – titolari del trattamento - ed in momenti temporalmente diversi;
- prevede la condivisione dei dati tra i soggetti che partecipano al percorso diagnostico terapeutico assistenziale;
- Il trattamento di tali dati avviene, quasi esclusivamente, attraverso strumenti informatici.

Dato atto, quindi, che il PDTA non rientra, sotto un profilo di fatto, né nell'ambito del FSE né in quello del Dossier, occorre ragionare su quali debbano essere i corretti adempimenti da imple-

mentare che siano in linea con la disciplina del Codice Privacy e con le posizioni assunte dal Garante in materia di sanità digitale.

Al fine quindi di individuare la corretta procedura di gestione del dato, analizziamo prima i profili soggettivi poi i possibili adempimenti.

Attori del PDTA

Si ritiene che una soluzione giuridicamente corretta, che rispecchia la realtà dei fatti, sia la previsione della gestione dei dati del PDTA in regime di co-titolarità, ove i diversi titolari saranno le diverse realtà sanitarie che intervengono nel percorso clinico.

La possibilità di gestire dati in cotitolarità è già oggi sancita - in maniera molto generica - dall'attuale Codice privacy ove all'art. 4 lett f) si stabilisce che il titolare può agire "anche unicamente ad altro titolare".

Nell'emanando Regolamento UE, poi, la possibilità di co-titolarità non solo è ribadita ma è altresì molto più ampiamente disciplinata all'art. 24, titolato (appunto) Corresponsabili del Trattamento.

Più precisamente tale norma, che nel caso del PDTA appare opportuno seguire seppure oggi non ancora obbligatoria, stabilisce che i co-titolari:

- stabiliscono congiuntamente le finalità ed i mezzi di trattamento dei dati personali;
- determinano attraverso un accordo interno le rispettive responsabilità in merito al rispetto degli obblighi derivanti dal regolamento.

Preme poi precisare che l'accordo interno richiamato dalla norma (che dovrà essere scritto) deve essere redatto con estrema attenzione: dal punto di vista giuridico infatti è il pilastro da cui si fanno discendere i diversi obblighi circa il rispetto della disciplina e, di conseguenza, le diverse responsabilità, anche sotto il profilo dell'eventuale risarcimento danno.

PDTA: definizione ed inquadramento proposto

Dopo queste premesse è dunque possibile dare una definizione precisa del PDTA in relazione al trattamento dei dati personali e trarne le conseguenze sul piano della conformità alla normativa vigente.

Il PDTA può essere configurato a tutti gli effetti come un trattamento sanitario di durata definita, effettuato da una entità virtuale costituita da una pluralità di soggetti legati da un contratto specifico che ne definisce ruoli e responsabilità.

La definizione di co-titolarità presente nel GDPR all'art. 24 si attaglia esattamente al PDTA così descritto e consente di impostare sia l'informativa che il consenso in modo conseguente: **un'unica informativa ed un solo consenso che riguardano l'intero PDTA.**

Dalla definizione di cui sopra discende anche che il paziente, concedendo il proprio consenso al PDTA, acconsente al fatto che i dati detenuti dai singoli co-titolari vengano fra essi condivisi e resi accessibili ai fini della gestione del PDTA.

Il PDTA, dunque, è equiparabile ad un ricovero ospedaliero con la relativa cartella clinica elettronica: di conseguenza tutti i dati facenti parte del PDTA sono consultabili dagli attori coinvolti nella gestione del PDTA per come questa si svilupperà in base alle esigenze cliniche e per la sola sua durata.

Di fatto quindi, così come la cartella clinica è l'insieme dei dati sanitari che afferiscono ad un unico episodio di cura, accessibili quindi a tutti i professionisti coinvolti nella cura del paziente fintanto che il paziente è "in cura", analogamente un PDTA raccoglie dati nell'ambito di un intervallo di tempo all'interno del quale diversi professionisti operano in modo contemporaneo o sequenziale (anche non continuativo) per curare il paziente in un unico percorso che ha un momento (evento) di inizio e un momento (evento) di chiusura. Fra questi due istanti di tempo (inizio e fine) il paziente è "in cura" nel PDTA e pertanto i dati del PDTA sono accessibili da parte di tutti i professionisti coinvolti in questo specifico processo di cura (PDTA).

In tale contesto si evidenzia che il PDTA, a differenza del ricovero, tende ad essere una "vista aggregata" di dati sociosanitari, alcuni di essi già esistenti nei Dossier dei diversi co-titolari, ovviamente nel rispetto dei consensi espressi dall'assistito in merito ai Dossier dei singoli co-titolari e degli eventuali oscuramenti sui dati in essi contenuti. Non si tratta in effetti di creare un ulteriore "dossier fisico" o una sorta di "cartella clinica di PDTA" ma di realizzare una restituzione "intelligente" di informazioni disponibili in sistemi già in uso (cartelle cliniche e infermieristiche, cartelle dei MMG, cartelle ambulatoriali, Dossier...) aggregando le informazioni sui "workflow dei PDTA" attraverso l'utilizzo di motori di integrazione (Enterprise Service Bus) ampiamente utilizzati in altri settori merceologici, consentendo così l'accesso anche ad informazioni non prodotte all'interno del PDTA che potessero risultare utili per ridurre la necessità di ulteriori esami o trattamenti previsti dal protocollo ma già effettuati per altre ragioni.

L'insieme dei dati necessari per la gestione del PDTA si costituisce quindi solo in modo virtuale e la condivisione/consultazione dei dati, che viene consentita ai co-titolari, viene dichiarata nello specifico consenso richiesto al paziente nella fase di "accettazione all'arruolamento" nel PDTA.

Laddove tale scelta non fosse possibile sotto il profilo tecnologico e si dovesse rendere necessaria la costituzione "fisica" di un Dossier a supporto del PDTA, sarà necessario dichiarare tale modalità operativa nell'informativa ed acquisire uno specifico consenso alla costituzione di uno specifico Dossier del PDTA stesso.

Adempimenti preliminari all'attivazione di un PDTA.

Sono analizzati nel seguito gli adempimenti derivanti dall'impostazione e dalle definizioni proposte nei paragrafi precedenti, alla luce della normativa vigente e del nuovo regolamento UE che, seppur troverà piena e completa efficacia tra due anni, si ritiene costituisca già oggi un riferimento da cui non si può prescindere.

Valutazione d'impatto per la protezione dei dati personali (DPIA).

Si tratta di una misura introdotta dal nuovo regolamento UE all'articolo 33 che, oltre ad essere opportuna per la criticità del tema, appare obbligatoria in base al comma 2, lettera b) dello stesso articolo.

In sintesi, la valutazione deve contenere almeno:

- una descrizione sistematica dei trattamenti e delle finalità;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- una valutazione dei rischi;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al regolamento.

Designazione del DPO del/dei PDTA

I corresponsabili del trattamento, cioè il titolare plurimo sopra individuato, trattando dati sanitari rientrano nell'obbligo di designare il DPO.

Può essere opportuno, per ragioni di costo ma anche per ragioni di efficienza e per garantire una unitarietà di impostazione che il DPO del PDTA coincida con quello dell'organizzazione maggiormente coinvolta nell'esecuzione del PDTA.

Funzionale all'attività del DPO, può essere considerata l'istituzione di un sito dedicato al PDTA, come ambito di comunicazione con gli interessati.

Informativa e consenso al trattamento dei dati

Nella proposta avanzata da questo documento, il PDTA è un trattamento effettuato da una pluralità di soggetti corresponsabili. E' pertanto necessario fornire una specifica informativa e raccogliere un apposito consenso.

Nell'informativa al paziente, oltre agli elementi indicati nell'articolo 13 del Decreto Legislativo 196/03, dovranno essere indicati:

- i soggetti o le categorie di soggetti ai quali i dati del PDTA possono essere comunicati o che possono venirne a conoscenza;
- il loro ruolo;
- gli specifici criteri di profilazione adottati;
- le misure poste in essere per proteggere i dati dagli specifici rischi individuati dal DPIA di cui sopra.

Il consenso specifico deve essere raccolto all'atto dell'accettazione del paziente ad essere inserito ("arruolato") nel PDTA per autorizzare il team multi-professionale che seguirà il PDTA alla consultazione dei dati del cittadino che verranno prodotti da diversi soggetti (MMG, medici spe-

cialisti di primo livello, clinici specialisti di secondo livello, personale infermieristico e di assistenza, dati acquisti da device wearable, dati resi disponibili dal paziente…) per la sola durata del PDTA.

Come anticipato, la realizzazione dei PDTA non prevede la costituzione di un "dossier sanitario di tipo fisico" essendo un'aggregazione di dati sociosanitari anche già esistenti. Laddove, per svariati ordini di motivi, sia renda necessaria la costituzione di un dossier fisico a supporto del singolo PDTA, si torna a segnalare che il consenso al PDTA non può includere il consenso alla realizzazione del relativo Dossier Sanitario che dovrà essere pertanto raccolto in forma separata.

Tutto questo presuppone che l'informativa sia coerente con l'impostazione complessiva, sia per quanto riguarda i titolari corresponsabili, sia per la tenuta dell'eventuale Dossier (fisico) ed in tal caso per la relativa gestione, compreso il diritto all'oscuramento dati.

Appare poi opportuno che nell'accordo interno di co-responsabilità sia anche stabilito quali dei co-titolari siano tenuti o possano fornire l'informativa al paziente nonché acquisire il consenso, stabilendo altresì le modalità idonee attraverso cui garantire agli altri co-titolari la corretta esecuzione di tali adempimenti (tale previsione ricalca peraltro la prescrizione di cui all'art. 79 comma 2 dell'attuale Codice Privacy).

Misure di sicurezza

Circa le misure di sicurezza da adottare per l'attivazione del PDTA si ritiene necessario che, oltre agli adempimenti generali, ovvero le misure di sicurezza previste dal D.Lgs.196/2003 e gli adempimenti relativi all'amministratore di Sistema (Provvedimento Garante 27 novembre 2008), dovranno essere assunte tutte le misure di sicurezza individuate dal DPIA, adottando l'approccio descritto dall'articolo 30 del Regolamento UE.

Tra queste misure, nel caso di attivazione di un Dossier Sanitario, dovranno essere certamente attivate anche le misure di sicurezza previste dallo specifico provvedimento adottato dal Garante (Linee guida in materia di Dossier Sanitario – 4 giugno 2015), fra le quali:

- misure a protezione dell'identità del paziente e utilizzazione di canali di comunicazione sicuri;
- adozione di sistemi di autenticazione e autorizzazione che assicurino l'accesso selettivo ai dati in linea con i principi di necessità, pertinenza, non eccedenza e indispensabilità;
- individuazione di criteri e modalità per la separazione e la cifratura dei dati idonei a rivelare lo stato di salute e la vita sessuale degli interessati;
- registrazione delle operazioni di accesso in appositi file di log ai fini della verifica della liceità del trattamento dei dati
- realizzazione di procedure per assicurare l'integrità, la disponibilità dei dati e il ripristino degli stessi in caso di guasti, malfunzionamenti o eventi disastrosi.

Occorrerà, quindi, definire una procedura, eventualmente supportata da adeguati strumenti tecnologici, per gestire in modo efficace l'obbligo di comunicazione al Garante ed, eventualmente,

anche agli interessati dell'eventualità del verificarsi di violazioni dei dati (data breach) o incidenti informatici (accessi abusivi, azione di malware...) che, pur non avendo un impatto diretto sui dati stessi, possano comunque esporli a rischi di violazione.

Tale obbligo è previsto sia dal citato provvedimento del Garante sul Dossier Sanitario, sia dal nuovo Regolamento Europeo.

Aspetti tecnologici

La possibilità di gestire i PDTA secondo il modello sopra descritto in modo efficiente e rispettoso dei diritti si basa sulla disponibilità di soluzioni tecnologiche adeguate che assumano fin dalla progettazione l'obiettivo di corrispondere a queste esigenze.

Non si tratta, dunque, di sovrapporre nuovi strati tecnologici a vecchie soluzioni ma di riprogettare l'architettura complessiva, tenendo conto delle opportunità della tecnologia di oggi e di quella che si intravede per domani: dalla mobilità al cloud, dai social media ai big data, all'internet delle cose (IoT), in un quadro in cui la sicurezza di un contesto non più confinabile all'interno di un perimetro non è un elemento accessorio ma un prerequisito progettuale.

Dall'applicazione all'infrastruttura

Il sistema informativo di una struttura sanitaria è estremamente articolato e con requisiti funzionali impegnativi, dati dal tipo di attività supportate, dall'eterogeneità dei sistemi e dagli ambienti in cui deve essere utilizzato.

A fronte di questa complessità, le esigenze di sicurezza sono particolarmente stringenti, e specialmente quelle previste dalla normativa vigente.

A questo si aggiunge la necessità di adeguarsi ad una evoluzione veloce ed importante:

- del modello organizzativo e di erogazione dei servizi da parte delle strutture della socio-sanità, e quindi dei requisiti per il sistema informativo;
- delle tecnologie utilizzate;
- della normativa di settore, in particolare in riferimento al trattamento dei dati personali.

Per contro, il sistema informativo delle strutture sanitarie si appoggia ad un'infrastruttura che spesso ha origini "antiche", dato che molte strutture si sono informatizzate nel tempo, e che è cresciuta per sedimentazioni successive. Lo stesso si può dire per il parco applicativo, eterogeneo e spesso poco integrato.

Seppure questi siano problemi comuni ai sistemi informativi di molti comparti, nell'ambito della socio-sanità i requisiti stringenti e complessi di sicurezza e normativi, uniti alle peculiari esigenze organizzative, di operatività e di responsabilità, rendono particolarmente difficile la gestione dell'adeguamento all'evoluzione tecnologica e normativa.

Si pone quindi il problema di quali soluzioni possano essere adottate, per facilitare l'evoluzione del sistema informativo e l'adeguamento alle esigenze normative ed operative.

In sistemi complessi come quelli qui discussi, può essere di aiuto spostare a livello di infrastruttura molte funzionalità e componenti che debbano essere utilizzati in modo coordinato o diffuso per i diversi sistemi e applicazioni. Il caso più evidente è quello del sistema di gestione delle identità e degli accessi (Identity and Access Management, IAM).

Avere un unico sistema centralizzato, con il quale i singoli applicativi siano interfacciati, permette di gestire le identità, l'autenticazione e i profili utente su questo unico sistema. I vantaggi sono molti:

- ogni utente è definito un'unica volta su questo sistema; oltre ad essere più veloce e meno oneroso, questo evita disallineamenti fra le identità definite sui diversi sistemi;
- questo sistema favorisce l'utilizzo di ruoli: un utente è associato ad esempio al ruolo "infermiere"; a quel ruolo è associata ad esempio la possibilità di accedere ad alcune applicazioni ma non ad altre; le applicazioni, a loro volta, acquisiscono dal sistema di IAM il ruolo "infermiere" per quell'utente, e permettono quindi di accedere ad alcune funzionalità e informazioni, ma non ad altre, con una gestione quindi molto più semplice e strutturata;
- è più immediato identificare delle responsabilità di gestione delle identità, e definire delle procedure ad esempio di allineamento fra l'ufficio del personale e la gestione tecnica delle identità, sia per la creazione e cancellazione delle identità, che per la definizione o le variazioni dei profili/ruoli;
- porta con maggiore facilità a sistemi di Single Sign On (SSO), discussi più avanti, in cui l'utente si autentica una sola volta al sistema informativo (ovvero al sistema di IAM), e questa autenticazione permette poi di accedere a tutte le applicazioni, senza doversi riautenticare quando si passa dall'una all'altra;
- l'integrazione di nuove applicazioni richiede solo di "agganciarle" al sistema di IAM, senza dover definire nuove identità;
- qualora l'azienda decida di adottare un diverso sistema di autenticazione, questa differenza sarà vista solo dal sistema di IAM, dato che le singole applicazioni non se ne occupano
- le applicazioni, svuotate del componente di IAM diventano più semplici e leggere, e complessivamente meno onerose da realizzare e mantenere;

Vediamo più nel dettaglio il caso del SSO in ambito DS e FSE.

Le applicazioni che permettono l'accesso al DS e al FSE devono consentire di disciplinare i permessi di lettura e di scrittura sugli archivi dati secondo una policy definita a livello direzionale.

Vanno definite le categorie di utilizzatori (medici, infermieri, amministrativi ecc.) e per ciascuna categoria definite le funzioni ed i programmi disponibili.

Ogni utente del sistema deve essere identificato univocamente da credenziali, ad esempio username e password, generate con un sufficiente grado di affidabilità; le credenziali devono essere custodite dai singoli utenti con una attenzione maggiore a quella che una buona parte di

utenti pone oggi, tenendo presente fra l'altro che tutte le operazioni di accesso al DS e al FSE verranno tracciate, come ribadito dalla recente normativa, riportando anche l'identificativo dell'utente che ha effettuato l'accesso.

Il motivo principale che induce l'utente a non gestire correttamente le proprie credenziali, a parte a volte la scarsa sensibilità riguardo all'argomento, è che deve ricordarsi username e password quasi sempre diverse per ogni applicazione, pertanto tende ad esempio a lasciare in bianco la password (questo è comunque un problema di non corretta impostazione dell'applicazione, che non dovrebbe permetterlo) o a scriverla su foglietti facilmente accessibili da altri.

Un sistema basato sul single-sign-on (SSO) permette una semplificazione nella gestione dell'identità degli utenti, che possono utilizzare una sola coppia di username e password per accedere a qualsiasi applicazione sul sistema.

Il SSO ha infatti la funzione di gestire in modo centralizzato le credenziali dell'utente, inviando alle singole applicazioni le informazioni necessarie a comporre opportunamente le credenziali di cui ogni applicazione necessita. Il SSO prevede inoltre che, in aggiunta a questa autenticazione centralizzata, l'utente si autentichi un'unica volta, e venga poi riconosciuto come autenticato dalle ulteriori applicazioni a cui accede nella medesima sessione.

Come detto sopra, la centralizzazione della gestione delle credenziali consente di affrontare a livello centrale e, dunque, senza impatti sugli applicativi, le esigenze di differenziazione della tipologia di credenziali utilizzabili e del numero di credenziali utilizzabili in funzione del livello di protezione che si ritiene necessario per le funzioni applicative o i dati a cui queste danno accesso ovvero della possibilità di semplificare l'accesso senza pregiudicarne la sicurezza.

Attivare funzioni di autenticazione forte, inserire meccanismi di autenticazione condizionale che verifichino anche il contesto in cui la richiesta di autenticazione viene posta (ad es. dalla intranet o dall'esterno, in orario di lavoro o al di fuori, …), utilizzare la biometria per ridurre l'utilizzo di elementi mnemonici o di dispositivi fisici a integrazione diventa così una scelta infrastrutturale con un impatto tecnico limitato sul contesto applicativo.

Con l'avvio di SPID, il servizio pubblico per l'identità digitale, alla necessità di predisporre un layer di autenticazione locale si affianca l'opportunità di utilizzare servizi esterni per l'autenticazione come quelli forniti dagli operatori convenzionati con SPID.

Particolare attenzione va posta dall'utente quando si allontana dalla postazione, ricordando che deve effettuare il logout dall'applicazione; in ogni caso è opportuno configurare opportunamente il tempo massimo di inattività della postazione dopo il quale è necessario reinserire le credenziali per accedere al sistema. Anche per questo aspetto, l'utilizzo di card, chiavi usb o anche cellulari con rilevazione della prossimità, porta con sé il vantaggio che il logout può essere automatico quando l'utente si allontana portando con sè lo strumento di autenticazione.

Una volta definiti i profili degli utenti, va composta una matrice che permetta di incrociare i profili degli utenti con le tipologie di accesso (nessuna, lettura, scrittura) per ogni funzione che tratti gli archivi di dati relativi al DS e al FSE; le applicazioni dovranno consultare tale matrice ogni volta che un utente effettua un'operazione sulla base dati, sempre che il cittadino/paziente abbia dato il consenso al trattamento dei suoi dati tramite DS e/o FSE.

Si vede quindi come la corretta configurazione del sistema e la corretta scelta degli applicativi, che dipende da scelte della Direzione Aziendale e della Direzione ICT, siano dunque elementi importanti nel determinare il grado di sicurezza del Sistema Informativo e la sua rispondenza alle norme.

Tutto quanto discusso in merito alla tematica dell'Identity and Access Management (IAM) si può estendere a molti altri componenti di base di un sistema informativo.

Un esempio importante è quello del Database Management System (DBMS). L'utilizzo di un sistema centralizzato, anziché di database distribuiti e spesso in formati proprietari delle singole applicazioni, offre molti vantaggi:

- possibilità di una gestione uniforme e centralizzata di aspetti come i backup;
- possibilità di usufruire di funzionalità sofisticate, disponibili in sistemi centralizzati ma difficilmente disponibili per le singole applicazioni; un esempio importante sono le funzionalità di cifratura, anche a basso livello, del database o di singoli record, che è un aspetto di conformità normativa importante;
- riduzione della duplicazione dei dati fra diversi database; oltre a ridurre la complessità della sincronizzazione e lo spazio necessario, costituisce anche un aspetto di conformità alle logiche di data minimization, e quindi di privacy by design, previste dal nuovo Regolamento europeo sul trattamento dei dati personali
- maggiore portabilità dei dati, sia in caso di sostituzione di un prodotto che in caso di integrazione di nuovi servizi e funzionalità
- maggiore controllo sugli accessi ai dati da parte degli amministratori di sistema che in alcuni casi possono essere abilitati alle funzioni tecniche di amministrazione del DBMS senza poter accedere ai dati in esso contenuti.
- Possibilità di mascherare i dati in modo irreversibile per estrarre dai Database di produzione dati di test, da utilizzare nello sviluppo e nella manutenzione degli applicativi, che non contengano dati personali

Questi stessi concetti possono essere estesi ad altri strumenti e funzionalità che possono essere centralizzati. Ad esempio, la centralizzazione dei meccanismi di logging e tracciamento facilita la conformità ai requisiti di tracciamento delle operazioni (seppure le singole applicazioni debbano essere adeguate per generare le informazioni per il tracciamento, possono poi ignorare gli uteriori aspetti di memorizzazione e conservazione a norma), e soprattutto al requisito di implementare un sistema di anomaly detection, previsti ad esempio dalle Linee Guida in Materia di Dossier Sanitario emesse dal Garante a giugno 2015. Requisiti di questo tipo sono sempre più comuni nelle normative generale e di settore, e la capacità di adeguare il sistema informativo nel suo complesso con interventi il meno estesi possibile diventa fondamentale.

Portare tutti questi componenti e servizi a livello di infrastruttura, tipicamente centralizzandoli, libera le applicazioni dalla necessità di gestirli, semplificando sia le applicazioni che la gestione del sistema informativo. Tuttavia, questa evoluzione ha come requisito fondamentale un'elevata affidabilità dell'infrastruttura stessa, che deve essere ben disegnata, realizzata e gestita dal punto di vista della capacità, dell'affidabilità e della sicurezza. Si tratta comunque di un requisito

in generale più semplice da soddisfare che garantire gli stessi requisiti per le singole applicazioni.

Il ruolo di SPID e dei gestori di attributi

L'introduzione di SPID, in particolare presso le Pubbliche Amministrazioni, comporta la necessità di implementare delle soluzioni che consentano l'accesso ai servizi attraverso questo sistema di autenticazione, almeno per quanto riguarda l'interfaccia verso i cittadini. Nel momento in cui una tale interfaccia debba essere implementata, sarebbe naturale utilizzarla anche per l'interazione fra i diversi soggetti partecipanti al PDTA. I vantaggi sarebbero sostanzialmente gli stessi previsti per l'utilizzo della SPID in altri contesti, ovvero principalmente:

- La disponibilità immediata di un sistema federato utilizzabile nella collaborazione con altre Pubbliche Amministrazioni o strutture private, anche fuori regione, senza dover implementare nuove soluzioni o arruolare gli utenti
- La delega ai Gestori di Identità Digitali di molte delle responsabilità legate all'autenticazione di soggetti esterni che accedano ai servizi della struttura (con riflessi, almeno per le strutture private, anche in riferimento al Dlgs. 231/2001)

Per un utilizzo efficace di SPID nell'interazione fra strutture partecipanti ad un PDTA, è però necessario avere la possibilità di dare visibilità del ruolo dei diversi utenti all'interno del PDTA.

Questo può essere ottenuto mediante l'utilizzo di "server di attributi", che rendano disponibili le informazioni necessarie al momento dell'autenticazione. Una prima possibilità sarebbe quella di utilizzare i Gestori di Attributi previsti dalla normativa SPID. Tuttavia, il ruolo e l'effettivo utilizzo di questi gestori non è ancora ben chiaro, e potrebbero risultare adatti allo scopo come anche no.

Una possibilità alternativa è che le singole strutture partecipanti al PDTA espongano agli altri partecipanti un servizio analogo, gestito internamente. Anche in questo caso, sempre nell'ottica di unificare a livello infrastrutturale i componenti che lo consentano, questo servizio dovrebbe, per quanto possibile, offrire un'interfaccia analoga a quella dei servizi offerti dai gestori di Attributi, in modo da poter essere interrogato attraverso gli stessi strumenti.

L'utilizzo di un tale servizio è discusso nella sezione seguente sui modelli di supporto per i PDTA.

Modelli di supporto per i PDTA

In generale, sono ipotizzabili due modelli principali di implementazione del PDTA: nel primo, il PDTA si appoggia esclusivamente ai sistemi informativi delle strutture sanitarie coinvolte. In analogia con le indicazioni di HIMSS e del Medical Record Institute chiameremo questo modello **Electronic Health Record** (che in letteratura è descritto come un modello di integrazione di Electronic Medical Record creati a livello di singole strutture sanitarie). Nel secondo, si considera anche la possibilità della realizzazione di piattaforme di servizi orientati al cittadino definiti come **Personal Health Record**. Questo secondo scenario è una possibilità che può essere svi-

luppata, in conformità con la normativa, e può determinare una semplificazione delle problematiche legate alla protezione dei dati anche se non è diffusa nella realtà italiana attuale.

Modello con Electronic Health Record (EHR)

In questo primo modello, i titolari corresponsabili gestiscono interamente nell'ambito dei propri sistemi informativi la documentazione relativa al PDTA. Come già detto precedentemente si ipotizza che al momento dell'arruolamento nel PDTA, il paziente fornisca il consenso per il PDTA ed alla condivisione dei dati fra tutte le strutture coinvolte. Ne consegue che al momento dell'accesso ai documenti, anche fra diverse strutture partecipanti, non è necessaria la verifica del consenso ma solo quella dell'arruolamento nel PDTA. Qualora il paziente debba integrare la documentazione, ad esempio con referti prodotti presso strutture non partecipanti al PDTA, ne consegnerà una copia alle strutture partecipanti, o li renderà disponibili attraverso il FSE, sezione “taccuino”, dove possibile. La gestione del PDTA consente quindi di accedere a tutta la documentazione sanitaria disponibile per quel paziente presso tutti i titolari corresponsabili del PDTA ma solo per la durata del PDTA.

Facendo riferimento all'architettura generale descritta nel documento AISIS "Innovazione Digitale a supporto dei Percorsi Diagnostici Terapeutici Assistenziali", e sintetizzata nella figura che segue, ci concentriamo sui componenti PDTA Viewer, PDTA Engine e Data Repository.

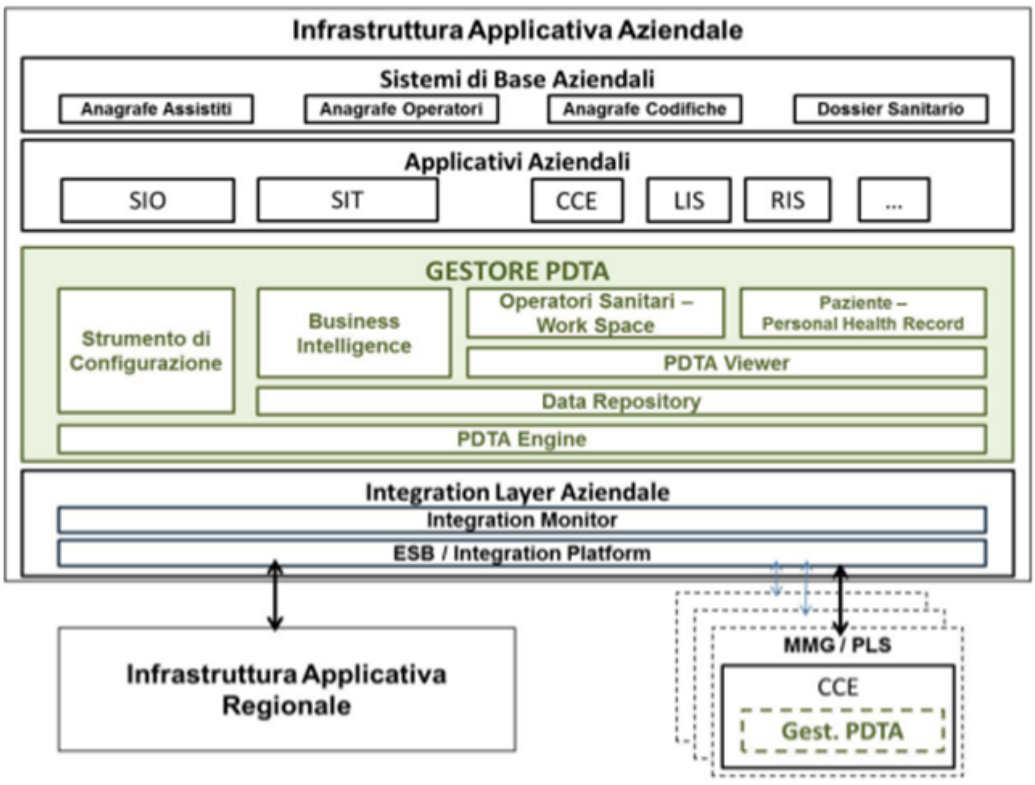
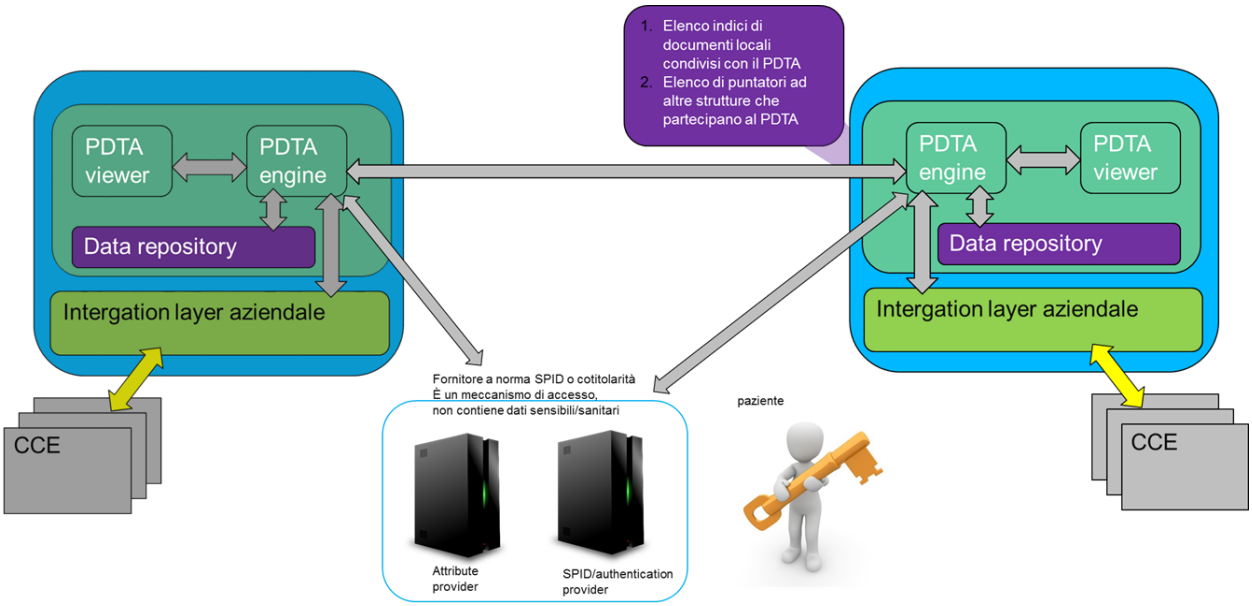


Figura 24 - Architettura Applicativa - Scenario AZIENDA-CENTRICO

Nel Data Repository viene definito il PDTA e si costituisce “l’aggregazione virtuale” dei dati delle diverse strutture partecipanti: esso contiene quindi solo le informazioni necessarie alla corretta gestione del PDTA e non i referti ed altri dati sanitari che invece rimangono nei Dossier delle singole strutture.

Nel momento in cui uno qualunque dei professionisti coinvolti nella gestione del PDTA (il medico, l'infermiere, l'amministrativo...) abbia la necessità di consultare i documenti relativi al PDTA, accede al PDTA Viewer, si autentica (presumibilmente attraverso un sistema di SSO della propria struttura) e richiede i dati del paziente. Il PDTA Engine, sulla base del profilo dell'utente, recupera dal Repository locale le informazioni a cui l’utente ha titolo ad accedere. Per quanto riguarda l'accesso alle altre strutture partecipanti al PDTA, si può ipotizzare uno schema basato su tre fasi. Queste fasi dovranno essere integrate in un framework coerente, tendenzialmente basato su webservices. Uno schema generale di questo modello si può vedere in figura:



Autenticazione

In questa fase, l'utente si può autenticare alla struttura remota in diverse modalità, di cui discutiamo alcuni casi significativi:

- l'utente non si autentica direttamente alla struttura remota: l'utente si autentica localmente, e poi viene utilizzata un'utenza tecnica in una comunicazione machine-to-machine per indicare l'identificativo dell'utente e accedere ai dati; si tratta di una soluzione relativamente semplice, ma è anche molto debole sia dal punto di vista architetturale che in termini di tracciamento e gestione delle responsabilità in caso di violazione;
- le strutture che partecipano al PDTA realizzano un sistema di identità federato che permette ai singoli utenti (compresi i medici di medicina generale) di autenticarsi e poi accedere ai servizi delle diverse strutture: si tratta di una soluzione più corretta in termini di gestione delle autorizzazioni e più chiaro in termini di responsabilità, ma può risultare complesso, particolarmente quando una struttura che partecipi a più PDTA debba adottare meccanismi diversi a seconda delle altre strutture coinvolte;

- l'utente si autentica mediante SPID: si tratta sostanzialmente di un caso particolare di sistema di identità federato, in cui specifici soggetti (gli Identity Provider) gestiscono l'autenticazione. In questo caso un unico framework è direttamente disponibile per i medici delle strutture partecipanti, per i medici di medicina generale e per i pazienti. Dato che le strutture dovranno già implementare questo tipo di autenticazione per i cittadini, l'adozione anche per più PDTA che coinvolgano diverse strutture, può avere un costo limitato. In questo caso però, non è probabilmente possibile utilizzare meccanismi di SSO fra diverse strutture.

Autorizzazione

Pur ipotizzando il consenso al trattamento all'interno del PDTA, ogni soggetto (medico, infermiere, amministrativo, MMG) che vi partecipa dovrà avere la possibilità di accedere alle sole informazioni necessarie, in base al proprio ruolo nel PDTA. Questo ruolo, definito e gestito dalla struttura di appartenenza, dovrà essere visibile anche alle altre strutture partecipanti al PDTA, che in base a tale ruolo gli renderanno accessibili informazioni diverse. È utile sottolineare come non sia praticabile una soluzione che preveda l'invio da parte della struttura remota di set di informazioni eccedenti, da selezionare poi localmente in base al ruolo dell'utente: questa pratica sarebbe in contrasto con i principi di privacy by design, ed in particolare di data minimization, previsti dal nuovo Regolamento Europeo.

La necessità di esporre a strutture e soggetti esterni dei ruoli, ed in generale degli attributi degli utenti, potrebbe suggerire l'utilizzo dei servizi di Gestori di Attributi SPID. Anche quando si ritenga preferibile gestire internamente un tale servizio, può essere opportuno esporre un'interfaccia analoga a quella dei gestori di attributi SPID, in modo da permettere alle controparti l'utilizzo di strumenti uniformi, e naturalmente centralizzati per la struttura, in entrambi i casi.

Un'ulteriore opzione può prevedere l'invio degli attributi all'interno del protocollo utilizzato per l'accesso alle informazioni, ma nuovamente, la soluzione può essere meno flessibile, ad esempio in caso di partecipazione della struttura a più PDTA.

In ogni caso, gli attributi esposti devono permettere di stabilire il ruolo del soggetto nel PDTA, e quindi quali siano le informazioni a cui ha accesso. Questa esigenza si presta a definire modelli di controllo accessi basati su combinazioni di attributi (ABAC) anziché su ruoli (RBAC), ad esempio consentendo l’accesso a un medico appartenente ad un reparto specifico di una struttura partecipante al PDTA (combinazione di attributi) senza che questo richieda di definire uno specifico ruolo.

Accesso e presentazione

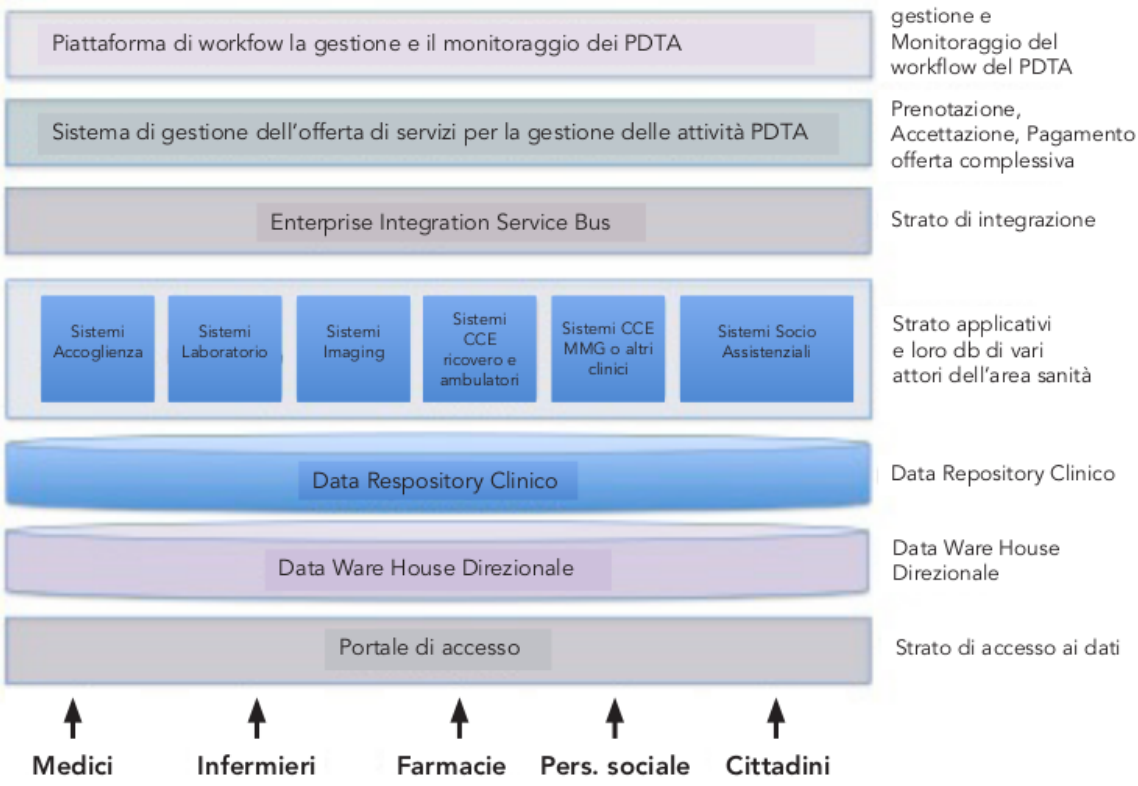
Una volta che la struttura remota abbia autenticato l'utente e autorizzato l'accesso ad un set di informazioni, queste informazioni devono essere presentate all'utente. Anche in questo caso, abbiamo diverse possibilità.

La prima, più semplice dal punto di vista implementativo, è che l'utente acceda direttamente ad un'interfaccia (tipicamente) web della struttura remota, dove visualizzare le informazioni. Questo vorrebbe dire però che, dovendo interagire con più strutture, si troverebbe a dover utilizzare più

interfacce distinte e disomogenee, una soluzione decisamente poco ergonomica. È quindi più ragionevole ipotizzare che il PDTA Engine della struttura a cui appartiene l'utente acquisisca dal PDTA Engine della struttura remota le informazioni, e le presenti all'utente in modo omogeneo attraverso il PDTA Viewer.

L'acquisizione delle informazioni potrà essere fatta attraverso web services, presumibilmente utilizzando il protocollo HL7.

Se facciamo riferimento alla figura seguente, tratta dal documento AISIS "Innovazione Digitale a supporto dei Percorsi Diagnostici Terapeutici Assistenziali" si vede come i diversi soggetti che devono accedere alle informazioni lo possano fare attraverso dei servizi di portale che selezionano le informazioni da presentare in funzione del profilo dell'utente. In un'ottica di offerta multicanale, già comune in altri contesti, portali web di questo tipo si appoggiano ad un back-end comune a tutti i canali (mobile, telefonico o altro). I diversi canali rappresentano quindi solo una diversa interfaccia verso un unico servizio. In quest'ottica, l'accesso tramite web services potrebbe essere sono un'ulteriore interfaccia verso lo stesso servizio. Si vede quindi come diventi più naturale l'utilizzo di SPID, che già dovrà essere offerto come strumento di autenticazione dallo stesso servizio almeno ai cittadini.



Modello con Personal Health Record (PHR)

In questo modello il problema della protezione dei dati viene di fatto delegata direttamente al cittadino o a provider da lui scelti secondo un modello di Self Health ormai diffuso in altri Paesi e che sta crescendo anche in Italia.

Il cittadino o il suo care-giver tengono presso di sé, essendone nei fatti responsabili, i dati che le strutture sanitarie producono e devono essere in grado di trasmettere in formato digitale e sicuro al cittadino stesso. Sarà dunque il cittadino che, direttamente o tramite un proprio provider rende disponibili ai team sociosanitari che si prendono cura di lui i propri dati clinici decidendo, in modo autoderminato e proattivo, come prevedono le indicazioni dei Garanti Europei, le modalità e i tempi di consultazione degli stessi da parte di terzi.

L'implementazione e l'utilizzo di servizi di Personal Health Record potrebbe rappresentare una soluzione più generale di molti problemi legati alla concessione del consenso in tutti i casi in cui, come nel PDTA, il percorso di cura coinvolga una pluralità di soggetti non sempre definibili a priori. Analogamente verrebbe risolto il tema della gestione del diritto all'oscuramento. Le strutture sanitarie, inoltre, verrebbero liberate da molti oneri e complessità legati alla titolarità dei dati ed alla loro conservazione.

Lo sviluppo di servizi per il cittadino quali la PEC, la firma digitale ecc., seppure con i loro limiti in termini di adozione, hanno fatto sì che si siano sviluppate delle infrastrutture che offrono elevate garanzie in termini di accessibilità, controllo accessi e conservazione dei documenti.

Si può quindi considerare realisticamente la possibilità per il cittadino di gestire autonomamente documenti e referti in un Personal Health Record che si appoggi a tali infrastrutture.

Il fornitore di un tale servizio di PHR dovrebbe essenzialmente implementare le stesse interfacce già descritte per le strutture sanitarie partecipanti ad un PDTA (sinteticamente: autenticazione mediante SPID, controllo accessi basato su attributi, accesso ai dati mediante web services e interfaccia di consultazione multicanale). La differenza sostanziale sarebbe che questo fornitore, in aggiunta, dovrebbe integrare nell'interfaccia web services anche delle funzionalità per caricare i documenti da parte di soggetti autorizzati dal paziente, o direttamente dal paziente tramite web.

In questo modello, al momento della produzione di un documento/referto, la struttura sanitaria lo potrebbe "consegnare" (eventualmente in copia) al paziente presso il suo PHR utilizzando tale interfaccia. Al termine di un ricovero quindi, una volta chiusa la cartella clinica, la struttura si libererebbe della necessità di gestirla, ed in particolare di conservarla, se non come archiviazione per gli obblighi di legge ma senza necessità di mantenerla fruibile successivamente ai reparti. Il paziente potrebbe a sua volta caricare nel proprio PHR documenti che abbia ottenuto per altri canali.

A questo punto, al momento dell'arruolamento nel PDTA, il paziente dovrebbe autorizzare le strutture partecipanti all'accesso al proprio PHR per le stesse tipologie di documenti già previste dal piano nella condivisione fra le strutture aderenti, nonché ad eventuali altre tipologie di do-

cumenti o referti che ritenga rilevanti. Il fornitore di PHR si integrerebbe quindi nel PDTA, dal punto di vista tecnologico, come una delle strutture partecipanti, ma essendo solo un fornitore di un servizio di conservazione per il paziente, dal punto di vista della titolarità dei dati non avrebbe alcun ruolo, dato che il "titolare" sarebbe comunque il paziente.

Per tornare all'esempio iniziale, al momento della programmazione di un ECG per un paziente arruolato in un PDTA, l'utente che ha in carico tale attività potrebbe accedere al PHR del paziente stesso, autenticandosi con SPID e presentandosi con i propri attributi (gestiti dalla struttura autorizzata dal paziente al momento dell'arruolamento), ottenendo quindi da gestore del servizio di PHR la possibilità di verificare se non sia già disponibile un referto di ECG abbastanza recente, caricato dal paziente o da un'altra struttura, aderente o meno al PDTA.

La gestione dei Data Breach

L'obbligo di notificare i casi di "data breach", cioè le violazioni di sicurezza, al Garante e, in taluni casi, agli interessati, oltre ad essere inclusa nel provvedimento del giugno 2015 sul Dossier Sanitario è previsto anche dal nuovo regolamento europeo come obbligo per tutti i responsabili di trattamento e, dunque, non solo nel caso di Dossier Sanitari.

E' da notare che la notifica non può essere un processo auto-contenuto: perché sia possibile notificare una data breach, è necessario esserne venuti a conoscenza, averlo analizzato e valutato nelle sue conseguenze, averlo contrastato ponendo anche in essere azioni volte alla limitazione delle conseguenze dello stesso.

Per corrispondere a questa norma dovranno essere posti in essere:

- Strumenti di monitoraggio dell'infrastruttura IT e servizi in grado di valutare le informazioni raccolte in modo tempestivo
- Procedure di gestione degli eventi in grado di valutare la gravità e di differenziare conseguentemente la reazione, attivando le azioni di contrasto e di mitigazione del danno appropriate
- Strumenti e procedure per la documentazione delle attività e per la produzione della documentazione da notificare

Nel caso del PDTA deve essere opportunamente valutato il fatto che le attività appena descritte attraversano le infrastrutture IT ed i processi di organizzazioni diverse, con differenti livelli di automazione e diverse procedure organizzative.

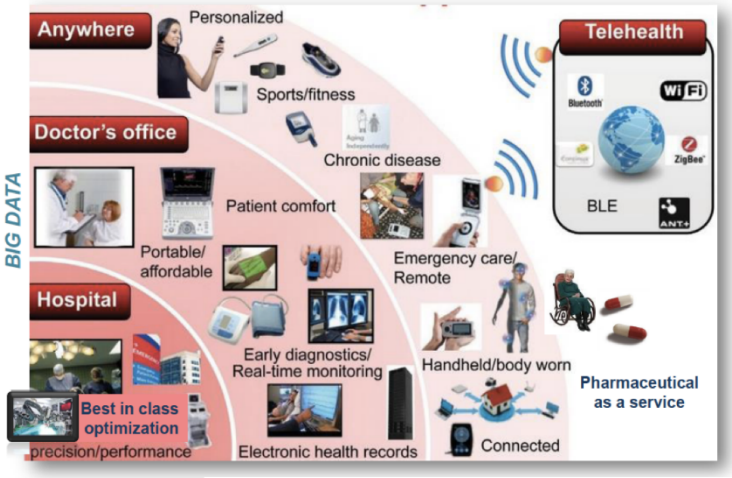
In particolare, deve essere tenuto presente che la sicurezza complessiva è condizionata da quella dell'anello più debole che può presentare criticità in grado di compromettere tutte le realtà a cui è collegato.

Conclusioni

Come abbiamo visto, la sanità, a livello non solo italiano, sta attraversando un momento di cambiamento importante che si traduce in:

- nuovi assetti istituzionali-organizzativi (concentrazione delle aziende sanitarie pubbliche e private),
- nuovi modelli di pianificazione e gestione dei setting assistenziali (maggior prevalenza di attività in ambito ambulatoriale, al domicilio del paziente, in strutture territoriali),attraverso l'utilizzo dei PDTA
- disponibilità di un volume crescente di dati clinici a disposizione del paziente e del team che lo ha preso in carico

L'IoT cambierà i paradigmi della sanità in tutto il mondo



...ma le piattaforme, le applicazioni, i dati risiederanno sul Cloud

Conseguenza diretta di questi cambiamenti sono la necessità di nuove architetture per la gestione delle attività cliniche e delle informazioni connesse e, al contempo, la crescita dell'importanza della protezione dei dati personali ed in generale della sicurezza delle infrastrutture e delle applicazioni.

Punti attenzione: l'innovazione originata dall'utente

Uno dei tratti strutturali dell'innovazione tecnologica di questi anni è quello di rendere disponibili al singolo strumenti potentissimi di comunicazione di relazione con altre persone o organizzazioni senza alcuna mediazione da parte di soggetti organizzati pubblici o privati. Questo fenomeno che ha trasformato molti aspetti delle relazioni sociali ed economiche ha investito anche la sanità.

Appare allora necessario evidenziare il gap esistente tra normativa/attenzione alla privacy e efficienza-efficacia dell'azione dei team clinici: se da un lato la normativa giustamente pone limiti ad un utilizzo indiscriminato di dati particolarmente sensibili, individuando architetture organizzative, metodologie, linee guida per la gestione delle responsabilità in termini di trattamento dei dati sociosanitari, dall'altro i team sociosanitari utilizzano, in misura sempre maggiore, soluzioni "semplici" e "user friendly" per la costituzione di architetture light e molto efficienti per la condivisione di dati sociosanitari.

Uno tra i tanti esempi è la costituzione di gruppi di lavoro "team clinici e pazienti oncologici" su whatsapp: l'adesione del paziente è certa e volontaria, altrettanto quella del team che segue il paziente, il paziente interagisce direttamente con il team che lo segue, vengono scambiati con

questo strumento informazioni cliniche soggettive o oggettive (immagini, referti, rilevazione di parametri bio-metrici).

Posti di fronte alla alternativa tra garantire un elevato livello di privacy e l'efficacia dell'azione del team sociosanitario, pazienti e team scelgono, senza alcun dubbio, la seconda, accettando un rischio maggiore sulla tutela delle proprie informazioni cliniche.

La propensione all'accettazione di un livello maggiore di rischio nella gestione privacy dei propri dati clinici se posta in alternativa rispetto alla efficienza e efficacia dell'azione socio-sanitaria è stata recentemente confermata da una survey di Accenture, condotta in 10 Paesi tra cui l'Italia, dalla quale emerge che l'**83%** del campione segnala la necessità e il diritto ad utilizzare i propri dati clinici (di questi il 90% ritiene di doverne avere il controllo) e che il **66%** del campione ritiene che i benefici derivanti dall'avere accesso ai propri dati supera i rischi per la privacy.[2]

Nel ripensare le proprie architetture organizzative e tecnologiche, la sanità - e dunque anche il modello di gestione dei PDTA - deve dunque porsi *obiettivi di efficienza, di efficacia e di qualità della customer experience tali da evitare il rischio che, a fronte di procedure ufficiali strutturate e perfettamente conformi alla normativa ma di complessa gestione, si sviluppino procedure informali e non controllate ma efficaci e di semplice utilizzo che la tecnologia normalmente utilizzata nella vita quotidiana rendono non solo possibili ma "naturali".*

Questo aspetto deve essere al centro dell'attenzione anche del legislatore e del Garante in quanto interessati a garantire una tutela effettiva e non solo formale dei diritti.

Punti di attenzione: "modello EHR" vs "modello PHR"

a. Scenario EHR

   Questo scenario, che resta confinato nel mondo del sistema socio-sanitario prevalentemente pubblico, è basato sul presupposto che l'organizzazione che eroga i servizi sanitari detenga il controllo sulle informazioni ad essi funzionali.

   E' dunque l'organizzazione sanitaria, pubblica o privata, che deve garantire il rispetto della normativa sulla Data Protection, assicurando gli standard di sicurezza e di gestione necessari.

   Il modello organizzativo del PDTA descritto in questo documento appartiene a questo scenario. La proposta contenuta in questo documento consente di dare risposte efficaci ed anche efficienti, attraverso una lettura innovativa della normativa coerente con le esigenze operative poste dalle nuove modalità di cura.

b. Scenario PHR

   Un secondo scenario riguarda un possibile nuovo modello, legato alla creazione di piattaforme di Personal Health Record, la cui Titolarietà e gestione dei dati viene affidata direttamente al cittadino-paziente che, grazie alle nuove tecnologie oggi disponibili, anche in termini di gestione on line del consenso e dell'informativa a terzi, possa accedere o avere co-

[2] Patient engagement survey, Accenture, 2014

pia dei propri dati clinici gestendoli in prima persona e autodeterminando a chi e quando renderli disponibili.

Le strutture sanitarie, pubbliche, private accreditate o private (quest'ultime utilizzate in misura sempre maggiore) saranno quindi chiamate a rendere fruibili i dati clinici in formato digitale, in qualità di produttore del dato clinico, al cittadino che si farà carico, direttamente o tramite un proprio provider, di gestirli e di renderli disponibili al team o al professionista che lo ha preso in cura.

L'attuale tecnologia consente modalità di protezione dei dati su device fissi o mobili che il cittadino o il suo caregiver sono in grado di gestire. In tale architettura la singola struttura è titolare dei soli dati prodotti che il cittadino ricompone nel proprio Personal Health Record.

Punti di attenzione: la tecnologia

La spinta informatica della modernizzazione, che trova nel PDTA una serie di ulteriori requisiti, richiede un'attenzione importante verso i sistemi informativi e la modernizzazione degli stessi secondo i principi di modularizzazione, coesione e disaccoppiamento. E' importante comprendere che il Sistema Informatico deve essere progettato nella sua architettura per livelli che forniscono servizi ai livelli superiori e specializzando le funzioni. E' una costante dell'evoluzione tecnologica IT: si usa sempre di più del software specializzato rispetto alla funzione da espletare. Per esempio per l'accesso ai dati si usano (ormai da molto tempo) i Database Management System, per il reporting i sistemi di Business Intelligence, e così via passando dai Workflow Management System, Portali ecc.

Rispetto alla protezione del dato (cioè alla Data Protection / Privacy) tali moduli riguardano:

- la gestione centralizzata dell'identità dei pazienti e degli operatori (Identity Management),
- le autorizzazioni di accesso cosiddette "a grana fine" (Access Management, Strong Authentication e Single SignOn),
- la gestione dei log e l'analisi degli stessi (Log Management e Security Information and Event Management),
- la cifratura (Encryption), la pseudonimizzazione (Masking) e in generale le pratiche (best practice) e le tecnologie che permettono il rispetto dei principali criteri di sicurezza come ad esempio il privilegio minimo, la separazione dei compiti (SoD), l'attribuzione e la possibilità di attribuzione di responsabilità (accountability), il controllo dell'operato degli utenti e degli amministratori.
- l'interoperabilità, attraverso architetture orientate a servizi (Service Oriented Architecture) e tecnologie per lo scambio sicuro di dati tra piattaforme diverse (API - Application Programming Interface - management)

I due scenari (quello attuale e quello PHR) devono usare un mix leggermente differente delle stesse tecnologie. Nel PHR assumono ancora più rilevanza le recenti iniziative relative all'autenticazione dei cittadini (SPID) e le piattaforme di interoperabilità (API e SOA).

A prescindere però dai dettagli delle tecnologie da adottare, *è evidente che è necessario riprendere ad investire nell' ICT aziendale e in primis sulla qualità delle risorse preposte alla sua gestione ed evoluzione.* Il CIO dell'ospedale moderno è un manager a tutti gli effetti in grado di comprendere e gestire queste sfide.

Inoltre la specializzazione dei mestieri dell'informatica richiede alle aziende sanitarie di approvvigionarsi anche di figure preposte alla protezione dei dati, dei sistemi e degli altri "asset" aziendali.

La raccomandazione è che la Direzione Generale ponga nell'organigramma il Chief Information Security Officer[3] (come avviene negli altri settori industriali) e il Data Protection Officer (come avverrà a seguito dell'applicazione del nuovo regolamento Europeo ma è già suggerito nel provvedimento sui Dossier Sanitari).

La notizia positiva è che la modernizzazione dell'IT permette di abilitare un nuovo modo di fare business anche in un settore, come è quello della sanità perfino pubblica, che solo apparentemente è poco esposto alle sfide della Digital Trasformation. Questa è, di fatto, una strada obbligata se si vogliono coniugare la crescente domanda di salute con i budget disponibili.

Punti di attenzione: le soluzioni applicative per la sanità

I cambiamenti in atto nel mondo della sanità disegnano uno scenario in cui difficilmente nuove soluzioni applicative per la sanità possono essere disegnate indipendentemente ed inconsapevolmente rispetto a determinate tematiche, trasversali alle singole specificità di dominio, che si stanno affermando in maniera imprescindibile richiedendo un cambio di paradigma nella progettazione e nello sviluppo delle applicazioni.

La sicurezza del dato e la garanzia della privacy per il cittadino è uno di questi aspetti trasversali che, seppur richiesto a livello di Normativa e di Linee Guida ormai da diversi anni, è stato finora alquanto sottovalutato nel mondo della sanità. Come noto e come già detto nell'ambito del presente documento, da un paio di anni a questa parte, il Garante della Privacy ha intrapreso una serie di azioni che gradualmente hanno richiamato sempre di più su questo tema l'attenzione dei diversi attori coinvolti nella gestione dei dati sanitari, compresi i fornitori di software.

Per arrivare a definire un breve elenco delle attenzioni da riservare alla progettazione ed allo sviluppo di software a supporto dell'implementazione dei PDTA secondo i due scenari prospettati, garantendo il rispetto delle regole di *Data Protection*, è opportuno fare una premessa che inquadri il contesto operativo.

Fino ad oggi i fornitori di software in ambito sanitario hanno sviluppato varie applicazioni a supporto dell'operatività dei diversi professionisti sanitari nell'ottica di garantire al meglio le funzionalità necessarie ad ogni singolo professionista nello svolgimento delle proprie mansioni (*best-of-breed*) cercando allo stesso tempo di garantire la condivisione trasversale di parte delle in-

[3] I primi 100 giorni del Responsabile della Sicurezza delle Informazioni http://100giorni.clusit.it/#/

formazioni trattate dal singolo strumento software secondo protocolli (es.: HL7, XDS) e strumenti (es.: Dossier, FSE) concordati.

L'obiettivo è sempre stato quello di garantire al meglio la gestione del percorso di cura del singolo cittadino assistito.

Gli investimenti dei fornitori di software si sono pertanto concentrati nella realizzazione di:

- Dossier
- Portali (per cittadini, medici di medicina generale...)
- FSE
- Applicazioni Mobile Health
- Controlli di appropriatezza prescrittiva, della cura, della terapia
- Piattaforme *open source* per affermare autonomia e riusabilità del software e garantire una riduzione dei costi anche su indicazione della Pubblica Amministrazione

I primi provvedimenti sanzionatori emessi dal Garante della Privacy nei confronti di alcune ben note strutture sanitarie su tutto il territorio nazionale hanno generato un certo disorientamento iniziale, anche a fronte di un rilevante margine di incertezza nell'interpretazione di alcune parti delle Linee Guida che ha reso complessa l'operazione di individuare tempestivamente quali fossero le misure più opportune da adottare.

Contestualmente si è aperta una fase di chiarimento e di conseguente razionalizzazione dei requisiti in materia di *Data Protection* grazie alle attività di confronto, approfondimento e collaborazione fra i diversi attori coinvolti (in particolare autorità, aziende sanitarie, consulenti legali,

fornitori pubblici e privati) nell'ambito di svariati gruppi di lavoro coordinati da associazioni di categoria e società di settore a livello regionale e nazionale.

La prima risposta ai provvedimenti sanzionatori emessi dal Garante è stata quindi l'attuazione delle misure necessarie per garantire i livelli minimi di sicurezza dei dati in relazione alla particolare gestione degli stessi all'interno dei singoli e numerosi applicativi utilizzati nell'ambito delle strutture sanitarie. Si è trattato sostanzialmente di interventi organizzativi, di modifica della configurazione dei software utilizzati e di adeguamento degli stessi. In particolare, le aziende fornitrici di software, in estrema sintesi, sono intervenute con attività di consulenza specifica e di adeguamento sul proprio venduto e sulle proprie soluzioni.

Possiamo ragionevolmente affermare che sia maturata la consapevolezza comune che, lo svolgimento delle prime attività in risposta ai provvedimenti del Garante sia stato solo un primo passo (dovuto) di un percorso che deve evolvere nell'ottica di una maggiore strutturazione e standardizzazione delle azioni, con un conseguente maggiore controllo degli investimenti e minore dispersione delle risorse disponibili.

Condizione necessaria affinché questa evoluzione si possa realizzare è la diffusione di una "cultura condivisa della privacy" guidata dalla definizione di indicazioni attuative comuni a livello sovraregionale per il recepimento e l'applicazione delle indicazioni del Garante su tutto il territorio nazionale in modo quanto più possibile omogeneo per consentire investimenti correttamente indirizzati sia da parte delle regioni e delle strutture sanitarie, sia da parte dei fornitori, evidenziando al tempo stesso criticità e/o eventuali aspetti che necessitino di ulteriori approfondimenti e chiarimenti.

Il presente documento vuole essere uno dei contributi in tal senso.

Parliamo di un cambiamento sostanziale ed "epocale", paragonabile, nel suo *incipit* e per impatto, a quanto si verificò in passato con le attività che si resero necessarie per far fronte al "millennium bug" ed al "passaggio all'euro".

Come già evidenziato nell'ambito del presente documento, la sfida è quella di passare da un'ottica di burocratizzazione del sistema ad una nuova concezione del sistema stesso, agendo a livello:

- Organizzativo e Culturale
- Architetturale e tecnologico
    - infrastrutturale
    - applicativo

Focalizzando l'attenzione sul tema della protezione dei dati, in ottica quindi di sicurezza e privacy dei dati sanitari, il software deve garantire idonei meccanismi architetturali e tecnologici di:

- autenticazione ed autorizzazione utenti del sistema
- protezione dei dati in termini di separazione fra dati anagrafici e dati sensibili, nonché di cifratura dei dati sensibili (ad es., attraverso l'applicazione anche parziale di tecnologie crittografiche a file system o database), al fine di rendere gli stessi intelligibili

- tracciabilità delle operazioni effettuate, sia di scrittura (inserimento, modifica, cancellazione logica) sia di lettura/consultazione
- accesso ai dati consentito solo se sussistono i presupposti di liceità per l'accesso agli stessi, di norma consentito agli utenti autorizzati solo se al momento coinvolti nella cura del paziente (paziente "in cura"), salvo eccezioni che devono essere motivate e tracciate
- gestione dei consensi: raccolta e registrazione, modifica del valore precedentemente espresso, applicazione delle regole previste per la visibilità dei dati di concerto con la tipologia di dati trattati e con il valore di consenso espresso
- gestione degli oscuramenti (automatici e volontari): raccolta e registrazione, modifica del valore precedentemente espresso, applicazione delle regole previste per la visibilità dei dati, di concerto con la tipologia di dati trattati e con il valore di oscuramento registrato. L'oscuramento (e l'eventuale oscuramento dell'oscuramento) è sempre associato ad un evento clinico in modo da consentirne la visibilità solo ed esclusivamente agli utenti autorizzati. Da un punto di vista informatico un evento clinico corrisponde ad un oggetto che rappresenta un episodio di cura, una richiesta o un documento
- flessibilità a livello di configurazione del sistema per supportare diversi modelli organizzativi quali strutture multi-presidio, servizi di area vasta, co-titolarità nel trattamento dati, organizzazione per intensità di cura
- flessibilità a livello di configurazione del sistema per consentire deroghe alle regole previste in caso di eccezioni (contemplate o estemporanee) che richiedano una modalità di azione specifica limitata ad un singolo caso (es.: autocertificazione di un utente per l'accesso ad un reparto non assegnato o per l'accesso al Dossier di un paziente non in cura)

Considerando uno scenario "allargato" in cui la gestione della cura e dell'assistenza al cittadino coinvolge diverse realtà dislocate sul territorio (aziende sanitarie, ospedaliere e strutture che erogano servizi socio-sanitari e assistenziali) si aggiunge la necessità di prestare particolare attenzione all'architettura complessiva del sistema spostando, come già detto nell'ambito del presente documento, a livello di infrastruttura funzionalità e componenti che devono essere utilizzati in modo coordinato o diffuso per le diverse applicazioni e migliorando i meccanismi di cooperazione applicativa. Da questo deriva quindi il requisito che le applicazioni siano in grado di interfacciare, utilizzare e fornire, servizi in uno scenario HIE (Health Information Exchange) nel quale ovviamente i requisiti di interoperabilità e di interazione fra le diverse applicazioni e componenti coinvolti sono imprescindibili.

Titolo qualificante è l'aderenza a standard di comunicazione e scambio dati già ampiamente diffusi o emergenti quali ad esempio:

- HL7
- XDS
- REST Web services
- FHIR (Fast Healthcare Interoperability Resources - https://www.hl7.org/fhir)

Considerazioni finali

Questo documento non ha l'obiettivo di trovare la soluzione dei problemi della sanità in questi tempi di grandi trasformazioni sociali, economiche e tecnologiche.

L'obiettivo è quello di porre in evidenza alcuni aspetti e questioni aperte, provando a fare delle ipotesi e dare qualche suggerimento ma soprattutto ponendo molte domande: per questo i livelli di approfondimento sono, forse, disomogenei, alcuni temi sono trattati in modo parziale e molte cose rimangono da approfondire.

Quello che serve è uno sforzo collettivo nella direzione giusta che speriamo di aver indicato, almeno quella, con sufficiente chiarezza.

Allegato 1

Hanno partecipato a questo lavoro:

Armani Fiorella; Dedalus
Caccia Claudio; Presidente AISIS
Faggioli Gabriele; Presidente CLUSIT, CEO P4I
Fumagalli Sergio; Vicepresidente Zeropiù, Direttivo CLUSIT
Ghedini Pierfrancesco; CIO Azienda Unità Sanitaria Locale di Modena, delegato AISIS
Marrali Michele; Legale, Studio Storti
Polito Filomena; Presidente APIHM, DPO
Ronchi Alberto; CIO Istituto Auxologico Italiano, delegato AISIS
Stefanelli Silvia; Avvocato, Studio Legale Stefanelli
Telmon Claudio; Security Consultant; Direttivo CLUSIT
Tibaldi Raffaella; NoemaLife
Vallega Alessandro; Director Oracle, Direttivo Clusit

In rappresentanza di

AISIS - Associazione Italiana Sistemi Informativi in Sanità
APIHM - Associazione Privacy and Information Healthcare Manager
CLUSIT - Associazione Italiana per la Sicurezza Informatica

E di: Azienda Unità Sanitaria Locale di Modena, Dedalus, Istituto Auxologico Italiano, NoemaLife, Oracle Italia, P4I, Studio Legale Stefanelli, Studio Storti, Zeropiù.

Note

[1] Comunicato stampa del Garante dell'11 dicembre 1997, in Boll. n. 2. p. 75, disponibile sul sito internet: http://www.interlex.it/675/tutela/c971211.htm, si veda anche il provvedimento Titolare, responsabile e incaricato - Individuazione del 'titolare del trattamento' - 9 dicembre 1997, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/30915

[2] In tema di co-titolarità si segnala un parere del Gruppo di lavoro ex art. 29, sul trattamento di dati personali effettuato da SWIFT (Society for Worldwide Interbank Financial Telecommunication), http://194.242.234.211/documents/10160/10704/1367590 disponibile in sintesi in italiano sul sito del Garante, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1367582.

[3] Sul ruolo e nozione di di responsabile e di incaricato del trattamento si veda il parere n. 1/2010 WP 169 adottato il 16 febbraio 2010 dal Gruppo di lavoro art. 29 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_it.pdf) il cui il Gruppo di esperti ha precisato, tra l'altro, che ai fini dell'individuazione della titolarità concretamente esercitata occorre esaminare anche "elementi extracontrattuali, quali il controllo reale esercitato da una parte, l'immagine data agli interessati e il legittimo affidamento di questi ultimi sulla base di questa visibilità";

[4] Si ritiene applicabile alla delega al Responsabile del trattamento i principi sanciti dalla Corte di Cassazione in tema di validità: *"... perché la delega di attribuzioni all'interno dell'azienda sia seria e reale, e non un mezzo artificioso per scaricare la responsabilità a livelli mansionali inferiori e comunque inadeguati a sopportarli, è necessario che:*

a) essa abbia forma espressa (non tacita) e contenuto chiaro, in modo che il delegato sia messo in grado di conoscere le responsabilità che gli sono attribuite;

b) il delegato sia dotato di autonomia gestionale e di capacità di spesa nella materia delegata, in modo che sia messo in grado di esercitare effettivamente la responsabilità assunta;

c) il delegato sia dotato di idoneità tecnica, in modo che possa esercitare la responsabilità con la dovuta professionalità." (Cassazione Penale, Sez. 3, 13 marzo 2003, n. 22931)

[5] In merito all'obbligo del responsabile di attenersi alle istruzioni del titolare, si veda provvedimento Garante 12 luglio 2000.

[6] Si veda per tutti la sentenza Cassazione penale , sez. IV, sentenza 19.10.2012 n° 41063 secondo cui: "*La delega di funzioni non esclude l'obbligo di vigilanza del datore di lavoro in ordine al corretto espletamento da parte del delegato delle funzioni trasferite in ordine alla correttezza della complessiva gestione del rischio da parte del delegato*"
http://www.altalex.com/index.php?idnot=59572

[7] Sul punto si veda il provvedimento 15 giugno 2011, "Titolarità del trattamento di dati personali in capo ai soggetti che si avvalgono di agenti per attività promozionali" (Pubblicato sulla Gazzetta Ufficiale n. 153 del 4 luglio 2011)
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1821257.

[8] Roberto Tommasi, La difesa della privacy nella sanità, ed. Maggioli.

[9] Gli adempimenti specifici sono descritti nella la parte seconda, titolo V del Codice Privacy, intitolato, appunto "TRATTAMENTO DI DATI PERSONALI IN AMBITO SANITARIO

[10] *Art. 13. Informativa*

"1. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;

b) la natura obbligatoria o facoltativa del conferimento dei dati;

c) le conseguenze di un eventuale rifiuto di rispondere;

d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;

e) i diritti di cui all'articolo 7;

f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'articolo 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'articolo 7, è indicato tale responsabile.

2. L'informativa di cui al comma 1 contiene anche gli elementi previsti da specifiche disposizioni del presente codice e può non comprendere gli elementi già noti alla persona che fornisce i dati o la cui conoscenza può ostacolare in concreto l'espletamento, da parte di un soggetto pubblico, di funzioni ispettive o di controllo svolte per finalità di difesa o sicurezza dello Stato oppure di prevenzione, accertamento o repressione di reati.

3. Il Garante può individuare con proprio provvedimento modalità semplificate per l'informativa fornita in particolare da servizi telefonici di assistenza e informazione al pubblico.

4. Se i dati personali non sono raccolti presso l'interessato, l'informativa di cui al comma 1, comprensiva delle categorie di dati trattati, è data al medesimo interessato all'atto della registrazione dei dati o, quando è prevista la loro comunicazione, non oltre la prima comunicazione.

5. La disposizione di cui al comma 4 non si applica quando:

a) i dati sono trattati in base ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria;

b) i dati sono trattati ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento;

c) l'informativa all'interessato comporta un impiego di mezzi che il Garante, prescrivendo eventuali misure appropriate, dichiari manifestamente sproporzionati rispetto al diritto tutelato, ovvero si riveli, a giudizio del Garante, impossibile.

5-bis. L'informativa di cui al comma 1 non è dovuta in caso di ricezione di curricula spontaneamente trasmessi dagli interessati ai fini dell'eventuale instaurazione di un rapporto di lavoro. Al momento del primo contatto successivo all'invio del curriculum,

il titolare è tenuto a fornire all'interessato, anche oralmente, una informativa breve contenente almeno gli elementi di cui al comma 1, lettere a), d) ed f). (1)"

[11] Art. 78. Informativa del medico di medicina generale o del pediatra

"*1. Il medico di medicina generale o il pediatra di libera scelta informano l'interessato relativamente al trattamento dei dati personali, in forma chiara e tale da rendere agevolmente comprensibili gli elementi indicati nell'articolo 13, comma 1.*

2. L'informativa può essere fornita per il complessivo trattamento dei dati personali necessario per attività di prevenzione, diagnosi, cura e riabilitazione, svolte dal medico o dal pediatra a tutela della salute o dell'incolumità fisica dell'interessato, su richiesta dello stesso o di cui questi è informato in quanto effettuate nel suo interesse.

3. L'informativa può riguardare, altresì, dati personali eventualmente raccolti presso terzi, ed è fornita preferibilmente per iscritto, anche attraverso carte tascabili con eventuali allegati pieghevoli, includendo almeno gli elementi indicati dal Garante ai sensi dell'articolo 13, comma 3, eventualmente integrati anche oralmente in relazione a particolari caratteristiche del trattamento.

4. L'informativa, se non è diversamente specificato dal medico o dal pediatra, riguarda anche il trattamento di dati correlato a quello effettuato dal medico di medicina generale o dal pediatra di libera scelta, effettuato da un professionista o da altro soggetto, parimenti individuabile in base alla prestazione richiesta, che:

a) sostituisce temporaneamente il medico o il pediatra;

b) fornisce una prestazione specialistica su richiesta del medico e del pediatra;

c) può trattare lecitamente i dati nell'ambito di un'attività professionale prestata in forma associata;

d) fornisce farmaci prescritti;

e) comunica dati personali al medico o pediatra in conformità alla disciplina applicabile.

5. L'informativa resa ai sensi del presente articolo evidenzia analiticamente eventuali trattamenti di dati personali che presentano rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in particolare in caso di trattamenti effettuati:

a) per scopi scientifici, anche di ricerca scientifica e di sperimentazione clinica controllata di medicinali, in conformità alle leggi e ai regolamenti, ponendo in particolare evidenza che il consenso, ove richiesto, è manifestato liberamente;

b) nell'ambito della teleassistenza o telemedicina;

c) per fornire altri beni o servizi all'interessato attraverso una rete di comunicazione elettronica."

[12] Sul consenso al trattamento dati, vedi Parere 15/2011 del Gruppo di lavoro "articolo 29" sulla definizione di consenso (luglio 2011), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_it.pdf.

[13] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3619954

[14] Provvedimento relativo ai casi da sottrarre all'obbligo di notificazione - Delibera n. 1 del 31 marzo 2004 - [852561], http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/852561

[15] Chiarimenti sui trattamenti da notificare al Garante - 23 aprile 2004 [993385], http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/993385

[16] Circa il trattamento effettuato con l'ausilio di mezzi elettronici l'art. 34 prescrive l'adozione delle seguenti misure minime:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

[17] Obblighi di sicurezza e documento programmatico: al 30 giugno la redazione del 'dps' - 22 marzo 2004 [771307], http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/771307