ICT E DIRITTO

Rubrica a cura di

Antonio Piva, David D'Agostini

Scopo di questa rubrica è di illustrare al lettore, in brevi articoli, le tematiche giuridiche più significative del settore ICT: dalla tutela del *domain name* al *copyright* nella rete, dalle licenze software alla *privacy* nell'era digitale. Ogni numero tratterà un argomento, inquadrandolo nel contesto normativo e focalizzandone gli aspetti di informatica giuridica.

La sicurezza delle informazioni in ambito sanitario

David D'Agostini, Antonio Piva, Attilio Rampazzo

1. Introduzione

L'Italia sta assistendo a un incremento dell'*Information and Communication Technology* (ICT) nel settore sanitario. Si va verso una nuova era, fondata sull'integrazione dei processi amministrativi, organizzativi e clinici tra le diverse strutture sanitarie e sull'avvio di reti regionali sanitarie, a supporto di modelli organizzativi innovativi, che promuovono la continuità delle cure e la centralità del servizio al cittadino. Si diffondono sempre con maggiore incidenza sistemi di supporto all'ospedalizzazione domiciliare, reti per patologia, portali istituzionali e telemedicina. Soprattutto si va verso un'integrazione complessiva di prodotti e servizi ICT, che porterà ad un impatto sistemico globale sul "Sistema Sanitario".

Le informazioni sanitarie, che sono principalmente dati sensibili, stanno mutando la loro memorizzazione da supporti cartacei a supporti digitali, un passaggio obbligato per le strutture sanitarie sia pubbliche che private.

Si rende necessario parlare di garanzie di sicurezza per gli utenti e anche per chi gestisce questa enorme mole di dati personali.

Risulta, pertanto, auspicabile che le strutture sanitarie applichino la normativa sulla tutela dei dati personali meglio conosciuta come Codice della privacy (d.lgs. 196/2003) e il relativo allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza" dove sono previsti diversi tipi di prescrizioni per il trattamento dei dati anche in relazione ai dati sensibili[1].

Già nell'ottobre 2008 sono state sollevate questioni di sicurezza sui dati sanitari italiani da una ricerca condotta dall'Osservatorio Nazionale per la Sicurezza Informatica: (www.osservatoriosicurezzainformatica.org). È emerso, infatti, un elevato rischio per la privacy dei pazienti considerando che il 60% delle ASL coinvolte nell'indagine dichiara di non disporre di strumenti adeguati per la protezione dei dati sensibili; un numero che indubbiamente fa riflettere ed è innegabile che per la tutela dei dati personali vi siano ancora ampi margini di miglioramento.

È sempre più diffuso l'utilizzo della rete internet per migliorare il servizio ai cittadini, per esempio prevedendo la possibilità di ricevere i referti o le cartelle cliniche attraverso il personal computer. Un servizio importante, che però espone le aziende sanitarie/ospedaliere a possibili problematiche di security.

Ecco i risultati della ricerca condotta su un campione di 50 ASL, dove emerge che:

- il 100% delle aziende ospedaliere usa internet;
- l'82% delle ASL dichiara di essere a norma con la legge sulla privacy, sia dal punto di vista formale che tecnico;

[1] Per una completa trattazione sulla Privacy si rinvia al numero 2 di giugno 2008, al numero 2 di giugno 2007 e al numero 1 di marzo 2004, all'interno della presente rubrica ICT e Diritto di Mondo Digitale.

- il 60% delle ASL ritiene comunque di non avere strumenti adeguati per la protezione dei dati sensibili;
- l'85% delle aziende ospedaliere hanno importanti problemi di budget da destinarsi all'IT.

La tecnologia oggi è in continua evoluzione e apre scenari sempre nuovi come la fruibilità del dato, nella sanità online. Il Garante della Privacy ha dimostrato grande attenzione al tema e nel 2009 gli interventi sulla cartella clinica, sul fascicolo sanitario elettronico, sui certificati medici hanno delineato delle linee guida comuni per gli operatori sanitari nella tutela della privacy dei cittadini.

2. I dati sanitari nel Codice della privacy

I dati personali idonei a rivelare lo stato di salute di un individuo rientrano nel novero dei cosiddetti "dati sensibili" rispetto ai quali, sin dalla legge n.675/96, l'attenzione del legislatore e la tutela approntata sono state maggiori.
All'interno dei dati sensibili si può addirittura sostenere che i dati sanitari siano "super-sensibili" tali sono le garanzie normative e le misure tecnologiche previste nel caso di loro trattamento.
Con l'approvazione del Codice della privacy, al trattamento di dati personali in ambito sanitario è stato dedicato un intero titolo (il titolo V della parte II contenente le disposizioni relative a specifici settori, dall'art. 75 all'art. 94).
Il principio cardine sancito in tali norme è che gli esercenti le professioni sanitarie e gli organismi sanitari pubblici trattano i dati personali idonei a rivelare lo stato di salute:

a. con il consenso dell'interessato e anche senza l'autorizzazione del Garante, se il trattamento riguarda dati e operazioni indispensabili per perseguire una finalità di tutela della salute o dell'incolumità fisica dell'interessato;

b. anche senza il consenso dell'interessato, previa autorizzazione rilasciata del Garante, sentito il Consiglio superiore di sanità, se tale finalità riguarda un terzo o la collettività.

In questi casi il consenso può essere prestato con modalità semplificate, vale a dire anziché con atto scritto dell'interessato, con un'unica dichiarazione, anche orale, che viene annotata dell'esercente la professione sanitaria o dell'organismo sanitario pubblico.
Naturalmente nel caso di emergenze sanitarie l'informativa e il consenso al trattamento dei dati personali possono intervenire successivamente alla prestazione, così pure nelle ipotesi in cui la prestazione medica possa essere pregiudicata dall'acquisizione preventiva del consenso, in termini di tempestività o efficacia e in particolare nei casi di tutela urgente della salute (bene primario costituzionalmente garantito e tutelato), ossia di:

a. impossibilità fisica, incapacità di agire o incapacità di intendere o di volere dell'interessato, quando non è possibile acquisire il consenso da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato;

b. rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato.

Il Codice della privacy dispone, altresì, che in ambito sanitario vengano adottate idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalle leggi e dai regolamenti in materia di modalità di trattamento dei dati sensibili e di misure minime di sicurezza.
In particolare vengono previste le seguenti misure:

a. soluzioni volte a rispettare, in relazione a prestazioni sanitarie o ad adempimenti amministrativi preceduti da un periodo di attesa all'interno di strutture, un ordine di precedenza e di chiamata degli interessati prescindendo dalla loro individuazione nominativa;

b. l'istituzione di appropriate distanze di cortesia, tenendo conto dell'eventuale uso di apparati vocali o di barriere;

c. soluzioni tali da prevenire, durante colloqui, l'indebita conoscenza da parte di terzi di informazioni idonee a rivelare lo stato di salute;

d. cautele volte ad evitare che le prestazioni sanitarie, ivi compresa l'eventuale documentazione di anamnesi, avvenga in situazioni di promiscuità derivanti dalle modalità o dai locali prescelti;

e. il rispetto della dignità dell'interessato in occasione della prestazione medica e in ogni operazione di trattamento dei dati;

f. la previsione di opportuni accorgimenti volti ad assicurare che, ove necessario, possa essere data correttamente notizia o conferma anche telefonica, ai soli terzi legittimati, di una prestazione di pronto soccorso;

g. la formale previsione, in conformità agli ordinamenti interni delle strutture ospedaliere e territoriali, di adeguate modalità per informare i terzi legittimati in occasione di visite sulla dislocazione degli interessati nell'ambito dei reparti, informandone previamente gli interessati e rispettando eventuali loro contrarie manifestazioni legittime di volontà;
h. la messa in atto di procedure, anche di formazione del personale, dirette a prevenire nei confronti di estranei un'esplicita correlazione tra l'interessato e reparti o strutture, indicativa dell'esistenza di un particolare stato di salute;
i. la sottoposizione degli incaricati che non sono tenuti per legge al segreto professionale a regole di condotta analoghe al segreto professionale.

Si ricorda, inoltre, che per determinati trattamenti di dati idonei a rivelare lo stato di salute effettuati da organismi sanitari, l'art. 34 del Codice della privacy impone l'adozione di tecniche di cifratura o di codici identificativi.

Particolare attenzione viene, poi, dedicata alle cartelle cliniche (documenti che per antonomasia contengono dati sanitari), per la cui redazione e conservazione gli organismi sanitari pubblici e privati devono adottare opportuni accorgimenti per assicurare la comprensibilità dei dati e per distinguere i dati relativi al paziente da quelli eventualmente riguardanti altri interessati.

Eventuali richieste di presa visione o di rilascio di copia della cartella e dell'acclusa scheda di dimissione ospedaliera da parte di soggetti diversi dall'interessato possono essere accolte, in tutto o in parte, solo se la richiesta è giustificata dalla documentata necessità:
a. di far valere o difendere un diritto in sede giudiziaria di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;
b. di tutelare, in conformità alla disciplina sull'accesso ai documenti amministrativi, una situazione giuridicamente rilevante di rango pari a quella dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile.

In questo ambito, come previsto dallo stesso Codice, è già intervenuto il Garante per la protezione dei dati personali, con provvedimenti a tutela dei diritti degli interessati.

3. Il Garante della privacy e il fascicolo sanitario elettronico

Nel documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)[2], adottato il 15 febbraio 2007, vengono fornite linee guida sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche; esso fornisce degli orientamenti sull'interpretazione del quadro giuridico in materia di protezione dei dati applicabile alle CCE, e spiega alcuni principi generali; fornisce altresì indicazioni sui requisiti relativi alla protezione dei dati richiesti per la costituzione delle CCE e sulle garanzie necessarie[3].

Di conseguenza il Garante della privacy ha pubblicato il 16 luglio 2009 (G.U. n. 178 del 3 agosto 2009) le "Linee guida in tema di Fascicolo sanitario elettronico e di dossier sanitario"[4].

Questo documento si inquadra all'interno del processo di ammodernamento della sanità pubblica e privata per il quale sono in atto numerose iniziative volte a migliorare l'efficienza del servizio sanitario attraverso un ulteriore sviluppo delle reti e una più ampia gestione informatica e telematica di atti, documenti e procedure. In tale contesto si collocano diverse iniziative volte ad archiviare, mediante nuove tecniche, la svariata documentazione di cui gli organismi sanitari si avvalgono a diverso titolo nei processi di cura dei pazienti come, per esempio, le più recenti esperienze di informatizzazione della cartella clinica e documento/dossier sanitario.

Le citate linee guida del Garante indicano diverse garanzie per l'interessato.

---

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/-wp-docs/2007/wp131_it.pdf

[3] Il documento del Gruppo europeo dei Garanti (cd. Gruppo Art. 29), emesso nel 2007, ha sicuramente il pregio di dare delle indicazioni di massima per una disciplina legislativa di diritto interno; si tratta in sostanza di linee guida valide per 27 Stati Membri contenenti perciò i principi generali e le soluzioni conformi, lasciando contempo agli Stati Membri un discreto margine di manovra per adottare una disciplina interna. Il Gruppo di lavoro formula undici raccomandazioni per gli ambiti in cui speciali garanzie risultano particolarmente necessarie per tutelare i diritti alla protezione dei dati dei pazienti e delle persone in genere.

[4] Il Fascicolo Sanitario Elettronico trae spunto dalla definizione di CCE e viene inteso come un documento formato con riferimento a dati sanitari originati da diversi titolari del trattamento e operanti di solito nella stessa regione o medesimo ambito territoriale.
Il *dossier* sanitario viene inteso come uno strumento costituito presso un organismo sanitario in qualità di unico titolare del trattamento (per esempio, ospedale o clinica privata) all'interno del quale operino più professionisti.

3.1. Diritto alla costituzione di un Fascicolo sanitario elettronico (Fse) o di un dossier sanitario

In base alle disposizioni contenute nel Codice dell'amministrazione digitale - d.lgs. 7 marzo 2005, n. 82[5] -, deve essere assicurata la disponibilità, la gestione, l'accesso, la trasmissione, la conservazione e la fruibilità dell'informazione in modalità digitale utilizzando le tecnologie dell'informazione e della comunicazione nel rispetto della disciplina rilevante in materia di trattamento dei dati personali. Il diritto alla costituzione o meno del Fse/dossier si deve, quindi, tradurre nella garanzia di decidere liberamente, sulla base del consenso, se acconsentire o meno alla costituzione di un documento che, come si è detto, raccoglie un'ampia storia sanitaria. Il consenso, anche se manifestato unitamente a quello previsto per il trattamento dei dati a fini di cura, deve essere autonomo e specifico.

3.2. Individuazione dei soggetti che possono trattare i dati

Il trattamento di dati personali effettuato attraverso il Fse/dossier, perseguendo esclusivamente fini di prevenzione, diagnosi e cura dell'interessato, deve essere realizzato esclusivamente da parte di soggetti operanti in ambito sanitario, con esclusione di periti, compagnie di assicurazione, datori di lavoro, associazioni o organizzazioni scientifiche e organismi amministrativi anche operanti in ambito sanitario. Inoltre, le persone fisiche legittimate a consultare il Fse/dossier devono essere adeguatamente edotte delle particolari modalità di creazione e utilizzazione di tali strumenti.

3.3. Accesso ai dati personali contenuti nel Fascicolo sanitario elettronico e nel Dossier sanitario

3.3.1. Diritti dell'interessato sui propri dati personali

Deve essere garantita la possibilità di esercitare in ogni momento i diritti previsti all'art. 7 del Codice della Privacy ed all'interessato devono essere garantite facili modalità di consultazione del proprio Fse/dossier.

3.4. Informativa e consenso

Per consentire all'interessato di esprimere scelte consapevoli, il titolare del trattamento deve fornire previamente un'idonea e chiara informativa, inoltre viene previsto lo specifico consenso.

3.5. Misure di sicurezza

Vengono imposti l'adozione di specifici accorgimenti tecnici per assicurare idonei livelli di sicurezza, ferme restando le misure minime che ciascun titolare del trattamento deve comunque adottare ai sensi del Codice della Privacy.
In particolare nell'utilizzo di sistemi di memorizzazione dei dati devono essere utilizzati idonei accorgimenti per la protezione dei dati registrati rispetto ai rischi di accesso abusivo, furto o smarrimento parziali o integrali dei supporti di memorizzazione o dei sistemi di elaborazione portatili o fissi (per esempio, attraverso l'applicazione anche parziale di tecnologie crittografiche a *file system* o *database*, oppure tramite l'adozione di altre misure di protezione che rendano i dati inintelligibili ai soggetti non legittimati).
Devono essere, inoltre, assicurati:

- ❑ idonei sistemi di autenticazione e di autorizzazione per gli incaricati in funzione dei ruoli e delle esigenze di accesso e trattamento (per esempio, in relazione alla possibilità di consultazione, modifica e integrazione dei dati);
- ❑ procedure per la verifica periodica della qualità e coerenza delle credenziali di autenticazione e dei profili di autorizzazione assegnati agli incaricati;
- ❑ individuazione di criteri per la cifratura o per la separazione dei dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali;
- ❑ tracciabilità degli accessi e delle operazioni effettuate;
- ❑ sistemi di *audit log* per il controllo degli accessi al *database* e per il rilevamento di eventuali anomalie.

Infine, per il Fascicolo Sanitario Elettronico, devono essere garantiti protocolli di comunicazione sicuri basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati tra i diversi titolari coinvolti.
Per quanto riguarda i Referti on-line, Il Garante della Privacy ha pubblicato un apposito provve-

[5] Per una completa trattazione sul Codice dell'Amministrazione digitale si rinvia al numero di dicembre 2005, all'interno della presente rubrica ICT di Diritto di Mondo Digitale.

dimento il 19 novembre 2009 denominato "Linee guida in tema di referti on-line"[6]. Le Linee guida in tema di referti on-line fissano rigorose misure a protezione dei dati sanitari dei pazienti che intendono ricevere referti medici e risultati di esami clinici (RX, analisi del sangue ecc.) in modalità telematica (via e-mail, e-mail certificata, o attraverso il collegamento con il sito web della struttura sanitaria).
I punti principali si possono riassumere:
- per fornire il servizio, le strutture sanitarie pubbliche e private dovranno adottare elevate misure di sicurezza tecnologica come per esempio utilizzo di standard crittografici, sistemi di autenticazione forte, convalida degli indirizzi e-mail con verifica on-line, uso di password per l'apertura del file[7];
- il referto può rimanere a disposizione on-line per un massimo di 45 giorni e dovrà essere accompagnato da un giudizio scritto e dalla disponibilità del medico a fornire ulteriori indicazioni su richiesta dell'interessato;
- l'adesione al servizio è facoltativa e il referto elettronico non sostituirà quello cartaceo che rimarrà comunque disponibile;
- l'Interessato dovrà dare il suo consenso sulla base di un'informativa chiara e trasparente che spieghi tutte le caratteristiche del servizio di "refertazione on-line";
- nel caso le strutture sanitarie offrano la possibilità di archiviare e continuare a consultare via web i referti, dovranno anche sottoporre ai pazienti un'ulteriore specifica informativa e acquisire un autonomo consenso.

A completamento, il Garante per la protezione dei dati personali ha licenziato lo schema di decreto sulle modalità di assorbimento della tessera sanitaria nella carta nazionale dei servizi, predisposto dal Ministro per la Pubblica Amministrazione e l'Innovazione, ma ha chiesto alcune garanzie per rafforzare la tutela dei dati dei cittadini: in particolare, misure di sicurezza e procedure uniformi per l'attivazione e la gestione della carta[8].
Il decreto consentirà alle Regioni, mediante il ricorso a un'unica tessera con microprocessore (*Smart Card*) che riunisce le funzioni di tessera sanitaria e carta nazionale dei servizi, di diffondere in maniera omogenea uno strumento sicuro per l'accesso ai servizi in rete. Sino a oggi tale strumento elettronico "multiuso" è stato adottato in forma sperimentale e con modalità diverse solo in alcuni Comuni e Regioni, permettendo ai cittadini, come previsto dal già citato Codice dell'Amministrazione digitale, l'accesso telematico ai differenti servizi di volta in volta offerti dalla pubblica amministrazione (prenotazione di prestazioni specialistiche, pagamenti di ticket sanitari on-line, accesso ai servizi dei centri per l'impiego, visualizzazione dei propri dati fiscali, verifica delle pratiche edilizie ecc.).

4. La gestione organizzativa della sicurezza delle informazioni

Il problema della sicurezza delle informazioni digitali, anche in ambito sanitario, sembra essere più di ordine organizzativo, che di tipo meramente legale o tecnologico.
Sebbene ogni anno negli Stati Uniti si stimi che siano alcune centinaia di migliaia le vittime di furto di identità, è bene ricordare che nella maggior parte dei casi la minaccia viene dall'interno delle strutture (*insider* e personale scontento). Purtroppo è la componente umana e non tecno-

[6] Il documento tiene conto di osservazioni e commenti formulati con una consultazione pubblica da organismi e professionisti sanitari pubblici e privati, medici di base, pediatri, organismi rappresentativi, associazioni di pazienti. Come è avvenuto in altri casi (esempio, per il Fascicolo sanitario elettronico) il Garante per la Protezione dei dati personali assolve con le Linee guida un ruolo di supplenza normativa in attesa di una legislazione che disciplini sulla base di regole chiare e uniformi un importante e innovativo processo di ammodernamento tecnologico.

[7] Protocolli di comunicazione sicuri, basati sull'utilizzo di standard crittografici per la comunicazione elettronica dei dati, con la certificazione digitale dell'identità dei sistemi che erogano il servizio in rete (protocolli https ssl – *Secure Socket Layer*);
- tecniche idonee ad evitare la possibile acquisizione delle informazioni contenute nel file elettronico nel caso di sua memorizzazione intermedia in sistemi di *caching*, locali o centralizzati, a seguito della sua consultazione on-line;
- utilizzo di idonei sistemi di autenticazione dell'interessato attraverso ordinarie credenziali o, preferibilmente, tramite procedure di *strong authentication*;
- possibilità da parte dell'utente di sottrarre alla visibilità in modalità on-line o di cancellare dal sistema di consultazione, in modo complessivo o selettivo, i referti che lo riguardano.

[8] Fonte: newsletter del Garante n. 336 del 18 marzo 2010.

logica a mostrare "punti deboli". L'adeguatezza dei sistemi di sicurezza deve ad ogni modo essere valutata e migliorata, tra l'altro gli strumenti per farlo già esistono. Il *security assessment*, la *vulnerability assessment* e la *risk analysis* sono metodologie ormai di dominio pubblico tra i gestori dei sistemi informativi che possono dimostrare la loro validità anche in ambito sanitario. Riguardo alla componente umana sarebbero sicuramente opportune attività di sensibilizzazione e di formazione interne alle strutture sanitarie, poiché gli operatori sanitari che accedono alle informazioni devono essere consapevoli delle norme di sicurezza e del corretto comportamento da tenere. A tale proposito è auspicabile la corretta definizione di policy interne con il duplice obiettivo di comunicare e di regolamentare l'uso delle tecnologie informatiche. Inoltre, sarebbe molto utile formare il personale utilizzando gli standard della certificazione ECDL Health, che assicura la competenza del personale nel gestire i dati sanitari e in generale i processi automatizzati attraverso l'uso di sistemi[9].
Già nell'articolo "Sicurezza delle Informazioni e norme ISO 27000" pubblicato sul n. 3/2008 di "Mondo Digitale" è stato trattato come attuare un corretto Sistema di Sicurezza delle Informazioni. Nel caso della Sanità, l'adozione delle norme della famiglia ISO 27000 è una delle più efficaci soluzioni per poter garantire riservatezza, integrità e disponibilità della molteplicità di informazioni trattate. Le stesse guide di CNIPA (ora DigitPA) consigliano l'adozione di queste norme internazionali al fine di attuare una corretta *governance* della Sicurezza delle Informazioni.
La famiglia di Norme ISO/IEC 27000, riferita alla Gestione alla Sicurezza delle Informazioni, comprende ad oggi 7 pubblicazioni (Tabella 1).
Queste norme sono il nocciolo di base per l'implementazione del sistema di gestione della sicurezza delle informazioni in un'organizzazione (sia essa impresa commerciale, organizzazione governativa, non profit o, appunto, un'organizzazione sanitaria privata/pubblica).
In particolare la ISO/IEC 27001 specifica i requisiti per la definizione, l'attuazione, il funzionamento, il monitoraggio, la verifica, il mantenimento e il miglioramento del sistema di gestione della sicurezza delle informazioni documentato nel contesto complessivo dei rischi aziendali. Sono inoltre specificati i requisiti per l'attuazione dei controlli di sicurezza su misura ri-

ISO/IEC 27000:2009	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements
ISO/IEC 27002:2005	Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 27003:2010	Information technology -- Security techniques -- Information security management system implementation guidance
ISO/IEC 27004:2009	Information technology -- Security techniques -- Information security management -- Measurement
ISO/IEC 27005:2008	Information technology -- Security techniques -- Information security risk management
ISO/IEC 27006:2007	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

TABELLA 1
Norme della famiglia ISO 27000 ad oggi pubblicate

[9] ECDL Health è una certificazione indirizzata agli utenti dei Sistemi Informativi Sanitari, comprendendo ruolo sanitario, tecnico, professionale e amministrativo e a studenti universitari di Facoltà di Scienze Mediche. La certificazione è motivata dalla crescente importanza che sta assumendo, a livello internazionale, l'informatica in ambito sanitario, e di conseguenza vengono riconosciuti anche i crediti ECM. Basandosi su un approccio centrato sul paziente una componente importante della certificazione Health è dedicata alla sicurezza, alla Privacy, alla riservatezza e alle autorizzazioni di accesso. (http://aicanet.net/certificazioni/ecdl/specialised-level/health/presentazione).

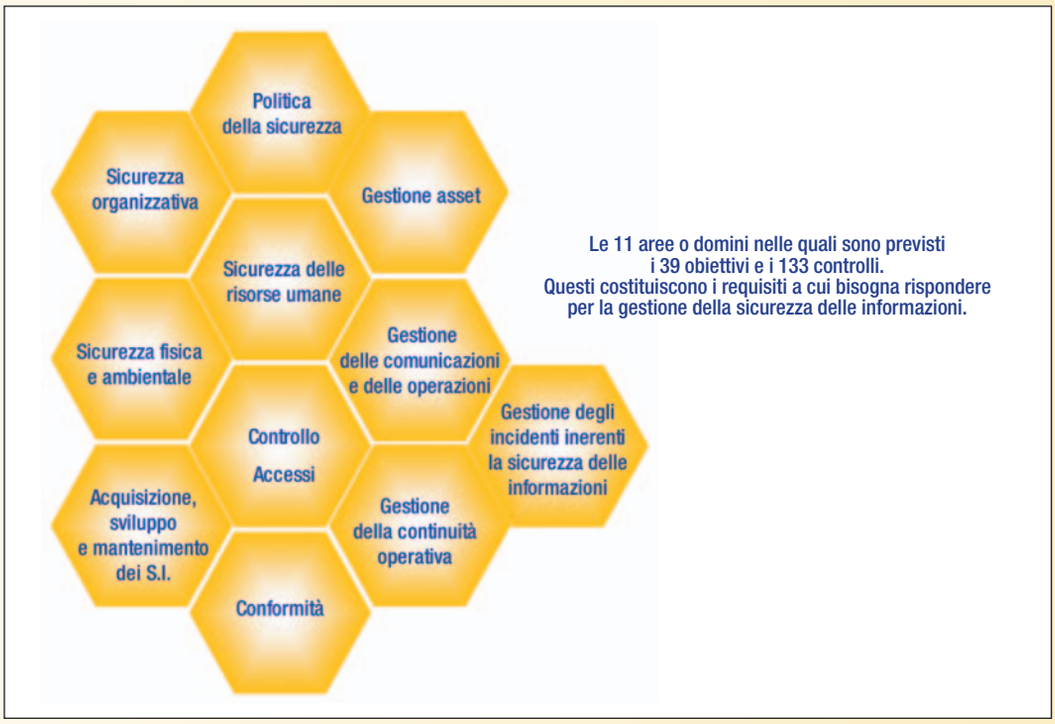

FIGURA 1
Le 11 aree di intervento

spetto alle esigenze delle singole organizzazioni o parti di esse.
L'ISO, seguendo una politica che si va diffondendo tra gli enti di normazione che è quella di emettere standard "*general purpose*" e poi far seguire documenti di approfondimento per i singoli settori applicativi, nel 2008 ha pubblicato la ISO 27799 (*Health Informatics – Information security management in health using ISO/IEC 27002*) con l'intento di guidare per mano all'applicazione in ambito sanitario della norma ISO/IEC 27002 per la sicurezza delle informazioni.
Come la ISO/IEC 27002:2005, la ISO 27799:2008 riporta quindi le raccomandazioni per la gestione della sicurezza in ambito sanitario, descrivendo undici aree di intervento e relativi "controlli", come indicazioni specifiche per la gestione della sicurezza.
Resta immutato il metodo per affrontare i rischi per la sicurezza delle informazioni che viene stabilito dalla ISO/IEC 27005:2008 prevedendo la netta distinzione tra la fase dell'analisi e quella della gestione. L'analisi può dirsi completa solo se esplora tutte le 11 aree di intervento previste (Figura 1) per l'individuazione delle contromisure.
Il capitolo 5 della Norma ISO 27799 è dedicato a tutti coloro che non hanno familiarità con la sicurezza delle informazioni sanitarie e i suoi obiettivi.
Nel capitolo 6 si può invece acquisire le linee guida su come implementare la Norma ISO/IEC 27001 nel settore sanitario tramite un piano di azione pratico. Nel capitolo non sono contenuti requisiti obbligatori ma, vengono forniti consigli e linee guida generali su come meglio implementare la norma 27002 nel settore sanitario. Il capitolo è organizzato secondo il ciclo di attività (Plan/Do/Check/Act) descritto nella Norma ISO/IEC 27001 che, se seguito, condurrà ad una robusta implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI).
Nel capitolo 7 si possono trovare validi consigli specifici sulle 11 aree di controllo e sui 39 obiettivi di controllo descritti nella Norma ISO/IEC 27002. Il capitolo descrive ciascuna delle 11 aree di controllo della ISO/IEC 27002 dove vengono specificati i requisiti minimi da applicare quando opportuno e, in alcuni casi, vengono fornite le linee guida sulla corretta attuazione di alcuni controlli di sicurezza della ISO/IEC 27002 per proteggere le informazioni sanitarie.
La norma conclude con tre allegati di carattere informativo:
- l'allegato A descrive le minacce generali alle informazioni sanitarie;
- l'allegato B descrive brevemente gli obiettivi e i documenti correlati del sistema di gestione della sicurezza delle informazioni;

• l'allegato C discute sui vantaggi dell'utilizzo delle strumentazioni di supporto come aiuto all'implementazione.

5. Conclusioni

Rispettare le normative vigenti e tutelare le informazioni personali dei cittadini/utenti del servizio oggi significa gestire il settore sanitario curando l'informatizzazione con particolare riguardo alla gestione della sicurezza delle informazioni trattate. Informatizzare un'organizzazione sanitaria e curarne gli aspetti legati alla sicurezza delle informazioni implica il pieno coinvolgimento e la sensibilizzazione di tutto il personale delle strutture sanitarie e in particolare del management. È quindi necessario uno sforzo eccezionale prima di tutto da parte del management per avvicinare tutti i soggetti coinvolti, specialisti, tecnici, medici, stakeholders, amministratori ecc. al concetto di conoscenza, consapevolezza e considerazione dell'importanza da dare al trattamento delle informazioni all'interno delle organizzazioni sanitarie. Non ultimo è da considerare che le organizzazioni che processano informazioni sanitarie, comprese quelle personali, devono avere una politica di gestione delle informazioni scritta, che sia approvata dalla direzione, pubblicata e successivamente comunicata a tutti i dipendenti e terze parti coinvolte.

David D'Agostini, avvocato, master in informatica giuridica e diritto delle nuove tecnologie, docente all'Università degli studi di Udine. Presiede la Commissione informatica dell'Ordine degli avvocati di Udine, è responsabile dell'area "Diritto& informatica" della rivista "Il foro friulano". Presiede l'Organismo di vigilanza di Autovie Venete SpA.
E-mail: studio@avvocatodagostini.it

Antonio Piva, laureato in Scienze dell'Informazione, *Vice Presidente dell'ALSI* (Associazione Nazionale Laureati in Scienze dell'Informazione ed Informatica) e Presidente della commissione di informatica giuridica. Docente a contratto di *diritto dell'ICT e qualità* all'Università di Udine. Consulente sistemi informatici e Governo Elettronico nella PA locale, valutatore di sistemi di qualità ISO9000 ed ispettore AICA.
E-mail: antonio@piva.mobi

Attilio Rampazzo, consulente di Sistemi Informativi e Sicurezza delle Informazioni in AlmavivA Finance Spa. Ha maturato un'esperienza più che trentennale nello sviluppo e conduzione di progetti informatici in ambito bancario e finanziario, nei quali la qualità e la sicurezza hanno ricoperto un ruolo determinante. È Vice Presidente del *Comitato AICQ "Qualità del Software e dei Servizi IT"*, *Valutatore Sistemi di Sicurezza delle Informazioni R.G.V.I.* (AICQ_SICEV cert. n.3), certificato CISA, Auditor ISO/IEC 20000, LoCSi e ITIL v.3 foundation. E' socio AIEA-Associazione Italiana Information Systems Auditor e AIPSI-A*ssociazione Italiana Professionisti Sicurezza Informatica*.
E-mail: attilio@rampazzo.it