2

INFORMATICA GIURIDICA

Collana coordinata da:
MARIO JORI - GIOVANNI SARTOR

STRUMENTI, DIRITTI, REGOLE E NUOVE RELAZIONI DI CURA

Il Paziente europeo protagonista nell'e-Health

a cura di
Carla Faralli, Raffaella Brighi, e Michele Martoni

G. Giappichelli Editore – Torino

C. Faralli - R. Brighi - M. Martoni (*a cura di*) – STRUMENTI, DIRITTI, REGOLE E NUOVE RELAZIONI DI CURA

ISBN/EAN
9 788892 100671

€ ??,00

INFORMATICA GIURIDICA

Collana coordinata da

MARIO JORI - GIOVANNI SARTOR

Serie Ricerca – 2

STRUMENTI, DIRITTI, REGOLE E NUOVE RELAZIONI DI CURA

Il Paziente europeo protagonista nell'e-Health

a cura di

Carla Faralli, Raffaella Brighi e Michele Martoni

G. Giappichelli Editore – Torino

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-0067-1

Il presente volume è stato pubblicato con il contributo dell'Alma Mater Studiorum – Università di Bologna, Centro Interdipertimentale di Ricerca in Storia del Diritto, Filosofia e Sociologia del Diritto e Informatica Giuridica "A. Gaudenzi – G. Fassò". Programma FARB – Finanziamenti dell'Alma Mater Studiorum – Università di Bologna alla Ricerca di Base.

Si ringraziano per l'attenta lettura i professori Evelina Lamma (Università di Ferrara-Dipartimento di Ingegneria) e Roberto Caso (Università degli Studi di Trento-Facoltà di Giurisprudenza).

Stampa: Stampatre s.r.l. - Torino

Indice

pag.

Parte seconda

Social Network Sanitari, *Mobile Health* e *App* mediche. I recenti sviluppi della condivisione del dato sanitario

Parte terza

Big data, Open data e riutilizzo dell'informazione sanitaria

pag.

Parte quarta
Risk management e relazione fra informatica sanitaria e informatica forense

Parte quinta
Esperienze di sanità elettronica

pag.

Parte sesta

Le nuove prospettive della sanità elettronica

2. L'implementazione dei processi organizzativi finalizzati alla gestione del rischio nell'ambito di strutture sanitarie

Donato Eugenio Caccavella [1], **Michele Ferrazzano** [2], **Federica Banorri** [3]

ABSTRACT. Nel presente lavoro sono illustrate le problematiche e le metodologie operative di implementazione ed ottimizzazione dei processi organizzativi in ambito sanitario, finalizzate al *risk management*, ponendo l'enfasi sulle peculiarità e complessità che contraddistinguono il contesto sanitario rispetto a quello di altre tipologie organizzative. La definizione del processo organizzativo si basa su esperienze maturate nella concreta gestione di incidenti. Le conclusioni cui il presente contributo porta muovono dalle considerazioni svolte intorno ai seguenti fattori: specificità dell'informatica sanitaria, insufficiente capacità di gestione dei rischi, importanza crescente dell'informatica forense, misure di sicurezza imposte dalle norme in materia di protezione dei dati personali particolarmente rigide nel trattamento dei dati con strumenti elettronici, necessità di un nuovo percorso organizzativo per la gestione del rischio.

1. Introduzione

I sistemi e le reti informatiche sono esposti ad un incremento di quantità e tipologia di minacce, dovute non solo a carenze di carattere tecnico ma anche – e molto più spesso di quanto sia immaginabile – ai limiti degli utenti umani che ne fanno uso. All'emersione di nuovi problemi di sicurezza occorre quindi rispondere con tempestività e precisione, aumentando la vigilanza e sviluppando un'autentica cultura del-

[1] Scuola di Medicina e Chirurgia, Università di Bologna. Consulente tecnico di informatica forense.

[2] CIRSFID, Università di Bologna. Consulente tecnico di informatica forense.

[3] Privacy Officer & Consulente della Privacy – Responsabile Ufficio Privacy, Azienda Ospedaliero-Universitaria di Bologna Policlinico Sant'Orsola-Malpighi.

la sicurezza, orientata a garantire la tutela dei dati come disponibilità a lungo termine e come riservatezza.

Nella strategia della sanità elettronica, la rilevanza della protezione dei dati si identifica in modo significativo con la sicurezza dei sistemi informatici e della trasmissione o condivisione elettronica dei dati, ovverosia con l'insieme delle misure preposte a garantire il rispetto dei noti principi legali della confidenzialità, dell'integrità, dell'autenticità e della disponibilità delle informazioni. È infatti doverosa l'adozione, in capo alle strutture sanitarie e agli operatori, di adeguate misure tecniche ed organizzative, anche individuali, per preservare le informazioni, istruendo adeguatamente il personale sulle procedure e sui rischi connessi al trattamento dei dati.

2. L'informatica sanitaria e l'informatica forense in ambito sanitario

I benefici derivanti dall'utilizzo dell'informatica hanno portato indubbi effetti positivi anche nel campo sanitario, svolgendo un ruolo di primissimo piano sia nella gestione delle pratiche sanitarie, sia negli strumenti utilizzati per la cura dei pazienti.

Una riflessione sul tema dei processi organizzativi basati sull'impiego di sistemi informatici e finalizzati alla gestione del rischio nell'ambito delle strutture sanitarie, non può prescindere da alcune osservazioni che rilevano in tema di tutela della riservatezza dell'individuo, poiché gli obblighi giuridici connessi a tale forma di garanzia possono essere percepiti come ostacoli all'esigenza prioritaria di garantire le migliori cure possibili al paziente.

Per come è stata definita dal legislatore attraverso il Codice Privacy[4], se ben concepita ed attuata nell'era della sanità elettronica in un'ottica di promozione della sicurezza, la protezione dei dati personali non ostacola affatto la presa in carico del paziente ma, al contrario, concorre a migliorarne l'efficacia: a tal proposito si segnalano le opportunità offerte dalla sanità elettronica e dai suoi strumenti e applicazioni, in particolare dal Fascicolo Sanitario Elettronico (FSE)[5] e dal

[4] D.lgs. 193/2003, Codice in materia di protezione dei dati personali.

[5] Cfr. art. 12, d.l. 18/10/2012, n. 179, convertito, con modificazioni, dall'art. 1, comma 1, legge 17/12/2012, n. 221.

Dossier (DSE) [6], che offrono alcuni spunti d'analisi per il tema in oggetto. In tal senso, i diversi interventi in tema di sanità elettronica riconducibili sia al Garante Privacy [7] che al Governo [8], evidenziano come, a fronte di un'adeguata informativa resa al paziente, la sensibilizzazione degli operatori sanitari alla gestione dei dati costituisca un passaggio fondamentale, da attuare secondo regole e criteri modulati sulla base del principio di necessità ed indispensabilità del trattamento, così come definito dall'art. 11 del Codice Privacy.

In quest'ottica, assumono rilevanza alcune specializzazioni dell'informatica: in primo luogo, come appena documentato con qualche esempio, l'informatica sanitaria che offre supporto a tutte le attività connesse alla pratica sanitaria, quali amministrazione, prevenzione, diagnosi, cura, terapia ed assistenza [9]. L'informatica sanitaria ha il compito di semplificare le attività umane, facilitando i processi di gestione delle informazioni, semplificando le attività di medici e infermieri e riducendo le possibilità di errore [10]: a tal proposito, è sufficiente pensare ai sistemi di analisi delle immagini per cogliere nella sua interezza la validità della riportata affermazione [11]. Posto che gli errori – siano essi dovuti a malfunzionamento degli apparecchi, a valutazioni errate o ad altre ragioni – non sono eliminabili in assoluto, i sistemi informatici sanitari sono rilevanti ai fini dell'individuazione delle cause e delle responsabilità su quanto accaduto, in virtù del fatto che al loro interno sono presenti dati utili ad accertare la vicenda.

Per i motivi sopra esposti, va ricordato come anche l'informatica fo-

---

[6] Cfr. *Linee guida in tema di Fascicolo sanitario elettronico (FSE) e di dossier sanitario*, provv. Garante del 16/07/2009 (G.U. n. 178 del 03/082009, doc. web n. 1634116).

[7] Cfr. *Linee guida in tema di referti on-line*, prov. Garante del 19/11/2009 (G.U. n. 288 del 11 dicembre 2009, doc. web n. 1679033). Cfr. *Dossier sanitario e trattamento dei dati personali dei pazienti*, provv. Garante del 10/01/2013 (doc. web n. 2284708).

[8] Cfr. D.P.C.M. del 08/08/2013 in tema di "Modalità di consegna, da parte delle Aziende sanitarie, dei referti medici tramite web, posta elettronica certificata e altre modalità digitali (...)".

[9] J. CAR-A. BLACK-C. ANANDAN-K. CRESSWELL-C. PAGLIARI-B. MCKINSTRY-R. PROCTER-A. MAJEED-A. SHEIKH, *The Impact of eHealth on the Quality & Safety of Healthcare*, Report for the NHS Connecting for Health Evaluation Programme, 2008. https://www.imperial.ac.uk/resources/32956FFC-BD76-47B7-94D2-FFAC56979B74/.

[10] C. CACCIA, *Management dei sistemi informativi in sanità*, McGraw-Hill, 2008.

[11] Basti pensare ai sistemi PACS (Picture Archiving and Communication System) che si compongono di hardware e software dedicati all'archiviazione, trasmissione, visualizzazione e stampa delle immagini diagnostiche digitali.

rense assuma un ruolo rilevante in caso di incidente sanitario [12]. L'informatica forense utilizza metodi, provati scientificamente, finalizzati all'identificazione, raccolta, conservazione, validazione, analisi, interpretazione, documentazione e presentazione delle fonti di prova digitale al fine di agevolare e promuovere la ricostruzione di fatti [13]: in altri termini, l'utilizzo dei dati registrati su sistemi informatici sanitari per accertare e documentare l'accadimento di fatti e responsabilità verificatisi in ambito sanitario.

Ponendo l'attenzione sulle organizzazioni sanitarie, va osservato come spesso la valutazione, la prevenzione e in generale la gestione del rischio non seguano logiche di insieme e di sistema, ma i vari rischi vengano analizzati singolarmente e in maniera frammentata, generando ridondanze operative con conseguente aumento dei costi e con frequenti conflittualità fra le aree di intersezione dei diversi gruppi di gestione del rischio.

Un ulteriore aspetto da evidenziare concerne l'intero processo organizzativo di prevenzione, il quale non solo dovrebbe essere predisposto in modo da ridurre al minimo il numero di "incidenti", ma, allo stesso tempo, posto che ogni incidente genera solitamente un risvolto di natura giudiziaria (civile e/o penale) o almeno disciplinare [14], avere anche la finalità di precostituire quegli elementi di prova da utilizzare in un eventuale contenzioso, per documentare le condotte degli operatori e le politiche di sicurezza dell'organizzazione, ovvero dar conto delle misure necessarie ad evitare l'incidente anche a tutela degli organi dirigenziali e di sorveglianza.

Va pertanto evidenziato che le discipline di maggiore rilevanza che convergono nella gestione del rischio di strutture in ambito sanitario attengono al diritto (penale, civile e del lavoro), alla medicina legale, alla privacy e all'informatica, quest'ultima non solo intesa come strumento di supporto dell'attività lavorativa (dunque informatica sanitaria e informatica in senso ampio), ma anche nell'accezione dell'interazione persona-computer [15] e dell'informatica forense.

---

[12] In argomento D.E. CACCAVELLA-A. GAMMAROTA, *L'Informatica Forense sanitaria per l'eHealth*, in questo stesso volume.

[13] DFRWS, *A Road Map for Digital Forensic Research*. Report From the First Digital Forensic Research Workshop (DFRWS), 7-8/08/2001. http://dfrws.org/2001/dfrws-rm-final.pdf.

[14] Cost., d.lgs. 165/2001, legge 190/2012, d.p.r. 62/2013.

[15] European Commission DG Health and Consumer, *Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices*, 06/01/2012. Online: http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf.

Quindi, a differenza delle discipline giuridiche e della medicina legale, l'informatica sanitaria e l'informatica forense assumono un ruolo fondamentale nel processo organizzativo di gestione del rischio, in quanto strumenti che consentono di tenere traccia ed analizzare gli eventi che si verificano all'interno di una struttura sanitaria.

3. Analisi dei rischi e degli eventi in ambito sanitario

Il riferimento agli eventi nell'esercizio di un'attività aziendale in ambito sanitario è rivolto alle seguenti tipologie:

- eventi correlati all'esercizio dell'attività aziendale;
- eventi correlati alla specializzazione dell'attività aziendale.

Nel primo caso il richiamo è ad attività di carattere più generico (ad esempio, amministrazione); nel secondo ad attività strettamente legate al *core business* dell'azienda e quindi al settore sanitario (ad esempio, la gestione delle immagini mediche).

Sulla base degli eventi verificabili vanno individuati i possibili rischi allo scopo di delineare il campo di prevenzione di eventuali incidenti. Occorre pertanto procedere:

- alla individuazione delle attività a rischio anche attraverso la definizione di eventi "sentinella" [16];
- alla definizione delle procedure interne decisionali in relazione ai rischi da prevenire;
- alla regolamentazione delle modalità di gestione delle risorse sanitarie, umane e tecnologiche ed organizzative finalizzate all'eliminazione (o almeno al contenimento) di incidenti;
- al supporto all'individuazione di protocolli di comunicazione nei confronti degli organismi di vigilanza.

Nella fase post-incidente, stante che il dato digitale è facilmente alterabile, occorre svolgere una vera e propria attività di informatica forense sui sistemi informatici sanitari [17], indirizzata ad individuare e recuperare elementi utili alle indagini. A tal proposito, nei sistemi infor-

---

[16] M. FERRAZZANO-D.E. CACCAVELLA, *Identificazione di furto (copia) di dati riservati tra analisi stocastica ed eventi sentinella*, in C. MAIOLI (a cura di) *Questioni di informatica forense*, Aracne, 2015.

[17] A. DASKALAKI, *Digital Forensics for the Health Sciences: Applications in Practice and Research*, IGI Global, 2011.

matici oggetto di attività di informatica forense rientrano a pieno titolo anche i dispositivi medico-chirurgici in virtù della circostanza per la quale la quasi totalità dei dati sanitari gestiti da detti supporti è in formato digitale. Pertanto, ogni sistema informatico, tradizionale o dispositivo medico-chirurgico, dovrà essere sottoposto ad attività di indagine informatica, procedendo:

- ad operazioni di individuazione, acquisizione ed analisi dei dati informatici rilevanti, secondo quanto previsto dallo standard ISO/IEC 27037:2012 [18];
- all'adozione di protocolli e procedure che offrano garanzie di autenticità, integrità e conservazione dei dati digitali sanitari individuati, acquisiti ed analizzati dai sistemi informatici, secondo quanto previsto dallo standard ISO 19011/2011 [19].

4. Definizione del processo organizzativo

Alla luce di quanto fin qui esposto, occorre definire il processo organizzativo finalizzato sia alla prevenzione che alla gestione del rischio in ambito sanitario. Tale processo richiede il coinvolgimento di diverse strutture dell'azienda sanitaria, quali: direzione sanitaria; medicina legale; ufficio legale ed ufficio privacy; servizi informatici.

Il personale-medico e non è parte integrante del processo organizzativo tanto nella fase di individuazione dei potenziali rischi, quanto nella fase di formazione e utilizzo. Infatti, l'analisi dei dati storici degli incidenti è una delle operazioni più utili ai fini di una corretta comprensione dei rischi ed andrebbe analizzata al fine di sottoporre quesiti al personale che li ha generati, studiando di concerto possibili soluzioni volte all'eliminazione, o almeno alla riduzione, degli stessi.

La sicurezza dei sistemi informatici che sottintende alla gestione di qualsiasi dato clinico dipende non solo da aspetti tecnici, ma anche e soprattutto da aspetti organizzativi. Alla luce di tale considerazione, è possibile affermare che la realizzazione di un sistema di sicurezza è riconducibile a tre specifiche funzioni: la definizione delle politiche di

[18] ISO:IEC 27037/2012 Guidelines for identification, collection, acquisition, and preservation of digital evidence.

[19] ISO 19011/2011 Linee guida per gli audit dei sistemi di gestione della qualità e/o ambientale.

sicurezza in materia informatica; l'attuazione di tali politiche; la verifica della corretta attuazione e della efficienza delle misure adottate attraverso "*audit*". Da un punto di vista implementativo, è necessario che ogni struttura dotata di sistemi informativi definisca un piano di sicurezza che preveda attività specifiche come l'analisi e la gestione del rischio, la definizione delle politiche di sicurezza e di un piano operativo, l'audit e la formazione. Le politiche della sicurezza dovrebbero riguardare alcuni aspetti importanti, quali la protezione fisica delle risorse (es. classificazione delle aree, accesso controllato e sorveglianza delle stesse, rilevazione tempestiva degli incidenti), la protezione logica (es. controllo dell'accesso alle informazioni, controllo delle porte di rete), il piano di continuità operativa (es. prevedere le risorse necessarie per il ripristino delle attività in caso di emergenza). L'applicazione delle politiche di sicurezza dovrebbe portare alla definizione pratica di quei processi composti da specifici passi e da precisi accorgimenti tecnologici che gli operatori devono seguire per raggiungere gli obiettivi.

Esemplificando, i dati memorizzati ed elaborati elettronicamente dovrebbero essere visionati, copiati, modificati e/o trasmessi solo da persone autorizzate a seconda delle reali mansioni assegnate: queste ultime, inoltre, devono potersi identificare in modo certo e univoco. I sistemi devono garantire che i dati siano disponibili, nella forma e nei contenuti, nel momento richiesto ed assicurare che essi non siano modificati o distrutti in modo accidentale o illecito. Inoltre, occorre poter documentare chi ha immesso, modificato o cancellato determinati dati nel sistema e garantire le necessarie procedure e protocolli. A tali accorgimenti occorre affiancare le procedure alla base della sicurezza di qualsiasi sistema informatico, quali *backup* dei dati, *disaster recovery*, utilizzo di *firewall*, uso della crittografia, della firma digitale, dell'autenticazione per l'accesso ai dati e di sistemi atti a rilevare programmi malevoli.

È auspicabile, quindi, un approccio sistemico al problema della sicurezza, mantenendolo sempre aggiornato. Inoltre, la tendenza delle strutture che trattano i dati informatici, e i dati sanitari in particolare, consiste nel riservare sempre più ingenti investimenti al settore della sicurezza perché un'interruzione o perdita di dati a causa di un'intrusione può provocare seri danni non sempre quantificabili a priori. Dalle considerazioni condotte emerge dunque come, tramite l'introduzione degli strumenti di sanità elettronica, sia possibile perseguire contemporaneamente la tutela della privacy [20] e migliorare la qualità delle cure, ge-

[20] Poiché i documenti sanitari contengono dati personali ascrivibili alla categoria dei

stendo opportunamente i processi organizzativi e riducendo gli incidenti.

Le esperienze maturate nell'ambito della verifica e miglioramento del trattamento dei dati sensibili hanno evidenziato alcune criticità trasversalmente comuni a diverse organizzazioni, palesando come il problema di un corretto trattamento dei dati sia di tipo essenzialmente culturale, piuttosto che basato su difficoltà tecniche contingenti.

Una prima criticità molto frequente consiste nella mancanza di un governo unico e reale del trattamento dei dati: molto spesso, infatti, le problematiche più significative si verificano in contesti in cui è presente una frammentazione delle responsabilità, talvolta funzionale a rendere maggiormente difficile l'individuazione di un responsabile in caso di incidente. Tuttavia, nel caso si dovessero verificare degli incidenti, tale assetto organizzativo non è condivisibile in quanto l'attività di indagine si rivolge inevitabilmente verso coloro i quali dispongono di autonomia dirigenziale ed economica per evitare l'evento, risalendo l'albero delle gerarchie aziendali: tale approccio metodologico è tuttavia scorretto.

Un ulteriore tentativo dell'ente di deresponsabilizzare, solitamente consiste nell'esternalizzare il servizio, tendendo però in tal modo a non assolvere all'obbligo di vigilanza sulle attività assegnate a terzi.

Una criticità alquanto frequente proviene dalla presenza di microsistemi informatici locali all'interno della organizzazione, retaggio dell'informatica anni '90 che, sull'onda dell'informatica distribuita, spingeva ad una dipartimentalizzazione dei sistemi informatici e informativi, creando all'interno dell'organizzazione delle zone di competenza, le quali, a distanza di venti anni sono diventate delle vere e proprie "sac-

dati sensibili, in quanto idonei a rilevare lo stato di salute o la vita sessuale degli interessati, devono essere trattati, così come espressamente contemplato dall'art. 11 del Codice Privacy, in modo lecito e con correttezza, per scopi ben determinati, espliciti e legittimi. Inoltre, gli stessi devono essere esatti, aggiornati, pertinenti, completi ma non eccedenti rispetto alle finalità da perseguire, nonché formulati in maniera da consentire l'identificazione solo per un tempo non superiore a quello necessario in base allo scopo. Prima del trattamento, l'interessato deve ricevere debita informativa, preferibilmente ma non necessariamente scritta; stesse prerogative anche per il consenso, da ottenere sempre prima del trattamento. Viceversa, è consentito provvedere successivamente, seppur senza ritardo, quando vi sia impossibilità fisica, incapacità di agire o di intendere o volere dell'interessato e non sia disponibile alcun'altra persona, abilitata all'espressione del consenso, ovvero sussista rischio grave, imminente e irreparabile per la salute o l'incolumità fisica dell'interessato, ovvero infine la previa acquisizione potrebbe compromettere l'efficacia o la tempestività della prestazione medica.

che di potere" non sempre rispondenti ad esigenze condivisibili anche a causa degli scarsi investimenti economici nell'area dell'informatica sanitaria. In tale contesto occorre evidenziare come il rischio di sfuggire a nuove e più rigorose logiche aziendali sia particolarmente elevato, con inevitabile e proporzionale rischio di incidenti.

La frammentazione delle responsabilità del controllo dei sistemi informativi di un'organizzazione sanitaria, al pari della presenza di sistemi "isolati e autonomi" al suo interno, inevitabilmente comporta pure un abbassamento dei livelli di controlli proattivi del rischio ed un elevato rischio di inquinamento.

Molto spesso, infatti, il responsabile dell'accadimento di un incidente informatico corrisponde al responsabile del sistema informatico su cui sono presenti i dati rilevanti per accertare il reale accadimento dei fatti, generando una coincidenza di profili che spinge inevitabilmente a severi giudizi in merito all'attendibilità dei dati in esso registrati [21]. Alla luce di quanto esposto e alla circostanza per la quale le criticità illustrate sono comuni a diverse realtà organizzative, consegue un problema di approccio al *risk management*, mirando all'individuazione delle responsabilità piuttosto che alla risoluzione delle problematiche: in altri termini, una cultura del "prescrivere regolamenti" a scapito del "comprendere il problema per risolverlo", che porta inevitabilmente ad una sicurezza formale ma non sostanziale.

Viceversa, una via alternativa e probabilmente più efficace sembra essere l'approccio di evangelizzazione della diffusione della cultura della sicurezza, dove le indicazioni tecniche e i regolamenti non vengono imposti dall'alto, con il rischio di paralizzare localmente l'organizzazione, ma coinvolgendo gli stessi interlocutori nella risoluzione dei problemi. A ciò, andrebbe affiancata una periodica attività di ispezione e verifica capillare, anche solo a campione, sulla reale applicazione delle normative e dei regolamenti dell'organizzazione, attività quasi sempre disattesa ma allo stesso tempo fondamentale e necessaria nel processo organizzativo di riduzione del rischio all'interno di una struttura sanitaria.

---

[21] Cfr. S. ATERNO-P. MAZZOTTA, *La perizia e la consulenza tecnica, Con un approfondimento in tema di Perizie Informatiche* (analisi e schede tecniche di D.E. CACCAVELLA), Cedam, 2006, pp. 195 ss.

Bibliografia

ATERNO S.-MAZZOTTA P., *La perizia e la consulenza tecnica, Con un approfondimento in tema di Perizie Informatiche* (analisi e schede tecniche di D. E. CACCAVELLA), Cedam, 2006.

CACCAVELLA D.E., *La Teledialisi può essere di aiuto per la gestione clinica del paziente in Emodialisi ?*, in *Medicina e informatica*, vol. 8, n. 2, aprile-giugno, 1991.

CACCIA C., *Management dei sistemi informativi in sanità*, McGraw-Hill, 2008.

CAR J.-BLACK A.-ANANDAN C.-CRESSWELL K.-PAGLIARI C.-MCKINSTRY B.-PROCTER R.-MAJEED A.-SHEIKH A., *The Impact of eHealth on the Quality & Safety of Healthcare*, Report for the NHS Connecting for Health Evalueation Programme, Imperial College London, March 2008.

DASKALAKI A., *Digital Forensics for the Health Sciences: Applications in Practice and Research*, IGI Global, 2011.

DFRWS, *A Road Map for Digital Forensic Research*. Report From the First Digital Forensic Research Workshop (DFRWS), 7-8/08/2001.

EUROPEAN COMMISSION DG HEALTH AND CONSUMER, *Guidelines on the qualification and classification of standalone software used in healthcare within the regulatory framework of medical devices*, 06/01/2012.

FERRAZZANO M.-CACCAVELLA D., *Identificazione di furto (copia) di dati riservati tra analisi stocastica ed eventi sentinella*, in C. MAIOLI (a cura di) *Questioni di informatica forense*, Aracne, 2015.