LA DEMATERIALIZZAZIONE DEI DOCUMENTI SANITARI

* * *

1. INTRODUZIONE

E' recente l'entrata in vigore del D.Lgs. 30 dicembre 2010, n. 235[1], rubricato "*Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69*". Trattasi di un decreto correttivo particolarmente importante e di ampio respiro, dopo che già un primo intervento di tipo riformatore, risalente al 2006[2], aveva pesantemente impattato sul testo storico del c.d. "*Codice dell'Amministrazione Digitale*" o "*CAD*" ed è indubbio che oggi più di allora debba essere data una spinta decisiva ai processi di digitalizzazione dei rapporti tra Pubbliche Amministrazioni *inter se*, tra P.A. e cittadini, nonché tra P.A e imprese. Esigenze di trasparenza, efficienza, efficacia, economicità, semplificazione e snellimento dell'azione amministrativa depongono in tal senso, stante anche quanto previsto dall'artt. 1[3] e 3-bis[4] della L. 7 agosto 1990, n. 241 in materia di procedimento amministrativo e dall'art. 3[5] del CAD medesimo.

Alla base v'è l'ambizioso e ormai non più celato obbiettivo, in un futuro non remoto, di abbattere i costi di gestione e di conservazione dell'immensa mole di "carta" che negli anni si è accumulata nei magazzini delle P.A. (nonché dei privati) e che rischierà di aumentare vertiginosamente nel futuro, se non si prenderà decisamente atto della necessità (ma anche se non si avrà il coraggio) di "dematerializzare" e dunque di "virtualizzare" rapporti, documenti, transazioni e ogni altra attività e/o servizio giuridicamente rilevante. In tale ottica vanno letti i vari interventi legislativi, regolamentari e di disciplina settoriale che negli anni si sono succeduti fino ad oggi, a partire dal 1997, data di entrata in vigore della c.d. "*prima legge Bassanini*"[6], il cui art. 15, comma 2, riconosceva per la prima volta agli atti, dati e documenti formati dalla P.A. e dai privati con strumenti informatici o telematici, ai contratti stipulati nelle medesime forme, nonché alla loro archiviazione e trasmissione con strumenti informatici, validità e rilevanza a tutti gli effetti di legge. Se ne ricordano i più significativi:

---

1 In G.U. n. 6 del 10 gennaio 2011, Suppl. Ord. n. 8, in vigore dal 25 gennaio 2011.

2 Cfr. il D.Lgs. 4 aprile 2006, n. 159, "***Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale*".**

3 Il comma 1 di siffatta disposizione così dispone: "***L'attività amministrativa persegue i fini determinati dalla legge ed è retta da criteri di economicità, di efficacia, di imparzialità, di pubblicità e di trasparenza secondo le modalità previste dalla presente legge e dalle altre disposizioni che disciplinano singoli procedimenti, nonché dai princìpi dell'ordinamento comunitario*".**

4 Tale disposizione concerne specificamente l'uso della telematica: "***Per conseguire maggiore efficienza nella loro attività, le amministrazioni pubbliche incentivano l'uso della telematica, nei rapporti interni, tra le diverse amministrazioni e tra queste e i privati*".**

5 La disposizione si riferisce al c.d. "***diritto all'uso delle tecnologie*", in virtù del quale i cittadini e le imprese hanno diritto a richiedere ed ottenere l'uso delle tecnologie telematiche nelle comunicazioni con le P.A., con le società, interamente partecipate da enti pubblici o con prevalente capitale pubblico inserite nel conto economico consolidato della pubblica amministrazione (come individuate dall'ISTAT ai sensi dell'art. 1, comma 5, della L. 30 dicembre 2004, n. 311) e con i gestori di pubblici servizi.**

6 L. 15 marzo 1997, n. 59, recante la "***Delega al Governo per il conferimento di funzioni e compiti alle regioni ed enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa*".**

- il d.P.R. 10 novembre 1997, n. 513, "*Regolamento recante criteri e modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici, a norma dell'articolo 15, comma 2, della legge 15 marzo 1997, n.59*";

il d.P.R. 28 dicembre 2000, n. 445, noto anche come "*Testo Unico in materia di Documentazione Amministrativa*" o "T.U.D.A.", il cui art. 1, comma 1, lett. b), offriva la definizione di "*documento informatico*", ancora oggi presente nel CAD, quale "*rappresentazione informatica di atti, dati, fatti giuridicamente rilevanti*";

il d.P.R. 13 febbraio 2001 n.123, "*Regolamento recante disciplina sull'uso degli strumenti informatici e telematici nel processo civile, nel processo amministrativo e nel processo dinanzi alle sezioni giurisdizionali della Corte dei Conti*"[7];

il D.Lgs. 23 gennaio 2002, n. 10, recante la "*Attuazione della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche*";

il D.M.E.F. 23 gennaio 2004, "*Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione in diversi tipi di supporto*";

Deliberazione CNIPA del 19 febbraio 2004, n. 11, "*Regole tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali - Art. 6, commi 1 e 2, del testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa, di cui al decreto del Presidente della Repubblica 28 dicembre 2000, n. 445*";

il D.Lgs. 20 febbraio 2004, n. 52, "*Attuazione della direttiva 2001/115/CE che semplifica ed armonizza le modalità di fatturazione in materia di IVA*";

il d.P.R. 11 febbraio 2005, n. 68 contiene il "*Regolamento recante disposizioni per l'utilizzo della posta elettronica certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3*"[8];

il CAD per l'appunto (D.Lgs. 82/2005 e succ. modif.);

le "*Linee guida per la dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini – Normativa e prassi*", adottate dal Ministero della Salute nel marzo 2007;

l'art. 39 del D.L. 25 giugno 2008, n. 112 ("*Disposizioni urgenti per lo sviluppo economico, la semplificazione, la competitività, la stabilizzazione della finanza pubblica e la perequazione Tributaria*"), conv. in L. 6 agosto 2008, n. 133, che ha previsto l'istituzione del c.d. "*libro unico del lavoro*" in luogo del "*libro paga*" e del "*libro matricola*"[9];

il D.P.C.M. 30 marzo 2009, "*Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici*";

il D.Lgs. 2 luglio 2010, n. 110, "*Disposizioni in materia di atto pubblico informatico redatto*

---

7 Cui va aggiunto il decreto del Ministero della Giustizia 17 luglio 2008, "***Regole tecnico-operative per l'utilizzo di strumenti informatici e telematici nel processo civile*" e che ha sostituito il decreto del Ministro della giustizia del 14 ottobre 2004 che regolamentava precedentemente la materia, stante anche quanto disposto dall'art. 61 proprio del Decreto del 2004, secondo il quale "*le regole tecnico-operative sono adeguate all'evoluzione scientifica e tecnologica, con cadenza almeno biennale*".**

8 Cui si affianca il D.M. 2 novembre 2005, recante le "***Regole tecniche per la formazione, la trasmissione e la validazione, anche temporale, della posta elettronica certificata*". Senza dimenticare il D.P.C.M. 6 maggio 2009, recante le "*Disposizioni in materia di rilascio e di uso della casella di posta elettronica certificata assegnata ai cittadini*".**

9 V. anche il successivo decreto del Ministero del Lavoro, della Salute e della Previdenza Sociale del 9 luglio 2008 col quale sono state fissate **le modalità ed i tempi di tenuta e conservazione del Libro Unico, nonché la circolare del Ministero del Lavoro n. 20 del 21 settembre 2008.**

dal notaio, a norma dell'articolo 65 della legge 18 giugno 2009, n. 69";
cui si affiancano altri provvedimenti non organici, ma pur sempre significativi per la modernizzazione del Paese[10].
In tale sede interessa affrontare le problematiche relative alla conservazione digitale dei documenti sanitari quali le cartelle cliniche e i referti medici.

2. La natura di atto pubblico della "cartella clinica" e la rilevanza giuridica della documentazione sanitaria

Prima di scendere *in medias res* è opportuno premettere che la cartella clinica è "*un atto pubblico che esplica la funzione di diario dell'intervento medico e dei relativi fatti clinici rilevanti, sicché i fatti devono essere annotati conformemente al loro verificarsi*"[11] ed è "*caratterizzata dalla produttività di atti costitutivi, traslativi, modificativi o estintivi rispetto a situazioni giuridiche soggettive di rilevanza pubblicistica, nonché dalla* ***documentazione di attività compiute dal pubblico ufficiale che redige l'atto***"[12].
Inoltre l'art. 26 del nuovo Codice di deontologia medica (come approvato **dal Consiglio Direttivo dell'Ordine il 23 gennaio 2007) così dispone:**
"*La cartella clinica delle strutture pubbliche e private deve essere redatta chiaramente, con puntualità e diligenza, nel rispetto delle regole della buona pratica clinica e contenere, oltre ad ogni dato obiettivo relativo alla condizione patologica e al suo decorso, le attività diagnostico-terapeutiche praticate.*
***La cartella clinica deve registrare i modi e i tempi delle informazioni nonché i termini del consenso del paziente, o di chi ne esercita la tutela, alle proposte diagnostiche e terapeutiche; deve inoltre registrare il consenso del paziente al trattamento dei dati sensibili, con particolare riguardo ai casi di arruolamento in un protocollo sperimentale*".**
La cartella clinica costituisce dunque il diario del decorso della malattia e di altri fatti clinici rilevanti e tali fatti debbono essere annotati contestualmente al loro verificarsi in modo intelliggibile. Le annotazioni debbono avvenire nel ragionevole tempo della contestualità ed essere consequenziali. Ciascuna singola annotazione, nel momento stesso in cui viene trascritta, esce dalla disponibilità dell'autore e acquisisce autonomo valore

10 Meritano menzione:
- **il trasferimento "telematico" di quote di S.R.L. ex art. 36, comma 1-bis, del D.L. 112/2008 cit.; il nuovo art. 2215-bis c.c., come introdotto dall'art. 16, comma 12-bis, del D.L. 9 novembre 2008, n. 185 ("*Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale*"), conv. in L. 28 gennaio 2009, n. 2, in forza del quale i libri, i repertori, le scritture e la documentazione la cui tenuta è obbligatoria per disposizione di legge o di regolamento o che sono richiesti dalla natura o dalle dimensioni dell'impresa possono essere formati e tenuti con strumenti informatici.**

11 V. Cass., Sez. V Pen., sent. **16 giugno 2005, n. 22694, in "*Rivista Penale*", 2006, 7/8, pag. 850. V. anche Cass. Pen., sent. 12.11.2008, n. 42166, in "*Rassegna di Diritto Farmaceutico*", 2009, 5, pag. 1065: "*La natura di atto pubblico della cartella clinica è stata più volte affermata da questa Corte (…), anche nel caso di c.c. redatta da medico dipendente di una clinica convenzionata con il Servizio sanitario nazionale (Cass. sez. 5, 23 marzo 2004 n. 22324, Magli; sez. 5, 21 agosto 1981 n. 2032, Nanni), il quale esplica un potere certificativo e partecipa della natura pubblica dell'attività sanitaria cui si riferisce, in virtù della delega di pubbliche funzioni conferita al soggetto privato dal servizio sanitario nazionale (Sez. Un. 27.03.1992, n. 07958, Delogu ed altro) (…) e agisce così per la pubblica amministrazione, concorrendo a formare ed a manifestarne la volontà in materia di pubblica assistenza sanitaria, nonché esercitando in sua vece poteri autoritativi*".**
12 Cass., Sez. V Pen., 17 dicembre 1992.

documentale definitivo. Se ciò è vero, "*le modifiche e le aggiunte integrano un falso punibile, anche se il soggetto abbia agito per ristabilire la verità, perché violano le garanzie di certezza accordate agli atti pubblici*"[13] *e precisamente* **"***tutte le successive modifiche, aggiunte, alterazioni e cancellazioni integrano falsità in atto pubblico, salvo che si risolvano in mere correzioni di errori materiali*"[14]. Ovviamente le falsità potranno essere tanto materiali (art. 476 c.p.), quanto ideologiche (art. 479 c.p.) e da un punto di vista strettamente civilistico l'efficacia probatoria non potrà che essere quella di cui all'art. 2700 c.c. Pertanto la cartella clinica costituisce "*piena prova, fino a querela di falso, della provenienza del documento dal pubblico ufficiale che lo ha formato, nonché delle dichiarazioni delle parti e degli altri fatti che il pubblico ufficiale attesta avvenuti in sua presenza o da lui compiuti*". La cartella clinica **è quindi atto pubblico certificativo e munito di fede privilegiata** per quello che il sanitario, pubblico ufficiale, attesta di aver compiuto o di essere avvenuto in sua presenza[15] e "***la funzione certificatoria*** *deve essere assicurata attraverso la veridicità, la completezza, la correttezza formale e la chiarezza*"[16].

Ma v'è di più. Se è vero quanto affermato sul valore probatorio, sulla rilevanza giuridica in tema di certezza del diritto, sulla completezza, correttezza formale, immodificabilità e irretrattabilità della cartella clinica, i dati in essa contenuti non possono certamente essere cancellati, ma sono, come già sopra accennato, ammesse correzioni di errori materiali tramite rettifica o integrazione. Ciò a patto che le correzioni siano chiaramente visibili. A tal proposito, prassi vuole che sia necessario circoscrivere l'errore tra due parentesi (o comunque interlinearlo, come anche è uso nei verbali di udienza o negli atti notarili), numerarlo e riportare a piè di pagina il numero con la dicitura "*leggasi*", indi scrivere la correzione apportata e apporre firma, data e timbro[17].

E se ce ne fosse ancora bisogno, a ulteriore conferma della rilevanza e della fondamentale funzione probatoria che rivestono la cartella clinica e gli altri documenti sanitari, basta leggere quanto scritto dal Ministero della Salute nella circolare n. 61 del

---

13 ***V.*** **Cass., Sez. V Pen., 21 aprile-11 novembre 1983, n. 9423.**

14 **V. Cass. Pen. sent. 20 gennaio 1987, n. 3632 (Rv. 175430); conforme Cass. Pen., sent. 17 febbraio 2004, n. 13989 (Rv. 228024).**

15 **D'altro canto, ciò che non attiene ai fatti, come per es. la formulazione di giudizi diagnostici, non rientra nella tutela dell'efficacia probatoria dell'atto pubblico.**

16 **Cfr. Cass. Pen., sent. 27 marzo 1992.**

17 La prassi è del tutto coerente col disposto di cui all'art. 7, comma 2, del T.U.D.A., quanto alla redazione e **stesura di atti pubblici: "***il testo degli atti pubblici comunque redatti non deve contenere lacune, aggiunte, abbreviazioni, correzioni, alterazioni o abrasioni. Sono ammesse abbreviazioni, acronimi, ed espressioni in lingua straniera di uso comune. Qualora risulti necessario apportare variazioni al testo, si provvede in modo che la precedente stesura resti leggibile***". In sintesi, dunque, le correzioni possono essere apportate lasciando immodificate e leggibili le precedenti annotazioni errate. Fa eco alla disposizione normativa il Garante per la protezione dei dati personali che, con Comunicato stampa del 12 ottobre 1999 (in Bollettino del n. 10/ottobre 1999, pag. 8), ha confermato che la cartella clinica non deve contenere lacune, abbreviazioni, abrasioni, cancellature, correzioni, aggiunte, che non siano individuabili, pur ammettendosi la rettifica e l'integrazione. Il principio è stato stabilito in un provvedimento con il quale è stato dichiarato infondato il ricorso presentato da un cittadino che aveva chiesto ad una A.S.L. la cancellazione di tutte le informazioni personali che lo riguardavano. Il Garante ha però precisato che è sempre consentito all'interessato di ottenere l'eventuale aggiornamento, rettifica, oppure, per motivi legittimi ed oggettivi, l'integrazione dei dati contenuti nella cartella sanitaria, per es. attraverso l'inserimento di annotazioni sulle risultanze di accertamenti successivamente effettuati presso altri organismi sanitari accreditati.**

19/12/1986: "*Le cartelle cliniche, unitamente ai referti vanno conservate illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire certezza del diritto, oltre a costituire preziosa fonte documentale per le ricerche di carattere storico sanitario. Le radiografie e altra documentazione diagnostica vanno conservate per 20 anni*".
In ragione di ciò diventa assolutamente indispensabile ragionare di conservazione "a norma" delle cartelle cliniche elettroniche, dei referti di laboratorio o di diagnostica per immagini, ben riflettendo sulle caratteristiche di siffatti documenti e sulle *best practices* adottate quando redatti su supporto cartaceo, onde valutare l'impatto della "digitalizzazione" sui medesimi e adeguare strumenti e modalità informatici alle esigenze di certezza del diritto.

3. La conservazione sostitutiva della documentazione sanitaria

3.1 Cartella clinica elettronica

Si è in precedenza accennato ai concetti di digitalizzazione e soprattutto di dematerializzazione, intendendosi per essa la progressiva sostituzione della documentazione cartacea con i documenti informatici, ottenibile nei seguenti modi:

- o attraverso la promozione dell'uso del computer quale strumento privilegiato di redazione degli atti giuridicamente rilevanti, in altre parole attraverso la redazione di documenti informatici originali e originari[18];

o attraverso la "digitalizzazione" dei documenti analogici[19] già esistenti (ossia tramite trasformazione del documento da analogico in informatico), onde eliminare problematiche di gestione e di conservazione dei supporti cartacei, con consistente abbattimento dei relativi costi.

Nel corso degli anni diversi provvedimenti di tipo legislativo o regolamentare hanno consentito la piena sostituibilità della documentazione cartacea tramite l'uso di nuovi strumenti tecnologici. A tal proposito merita menzione l'art. 25 della L. 4 gennaio 1968, n. 15, recante "*Norme sulla documentazione amministrativa e sulla legalizzazione e autenticazione di firme*" (oggi abrogata e sostituita dal T.U.D.A.), che così recitava: *"le pubbliche amministrazioni e i privati hanno facoltà di sostituire, a tutti gli effetti, ai documenti dei propri archivi, alle scritture contabili, alla corrispondenza ed agli altri atti di cui per legge o regola-*

18 Per la definizione di "***documento informatico*", cfr. l'art. 1, comma 1, lett. b), del T.U.D.A., cui si è accennato in precedenza, nonché l'art. 1, lett. p) del CAD.**

19 L'art. 1, lett. p-bis), del CAD definisce il documento analogico come "***la rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti*". Altra definizione è presente nell'art. 1 del D.M.E.F. 23 gennaio 2004 cit., quale documento "*formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta, le immagini su film, le magnetizzazioni su nastro*". *Similiter* l'art. 1, lett. b), della deliberazione n. 11/2004 cit.: "*documento formato utilizzando una grandezza fisica che assume valori continui, come le tracce su carta (esempio: documenti cartacei), come le immagini su film (esempio: pellicole mediche, microfiche, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video)*".**

mento è prescritta la conservazione, la corrispondente riproduzione fotografica, anche se costituita da fotogramma negativo"[20].

Per quel che qui interessa, occorre anzitutto evidenziare che i processi di dematerializzazione trovano oggi i principali riferimenti normativi nel CAD e nella deliberazione CNIPA (oggi "*DigitPA*"[21]) n. 11/2004 cit. (che ha sostituito la precedente deliberazione del 13 dicembre 2001, n. 42, quando ancora era denominata AIPA). Poi, con riferimento specifico alla dematerializzazione della documentazione sanitaria, vanno menzionate le "*Linee guida per la dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini*", adottate dal Ministero della Salute nel marzo 2007, cui si è accennato in precedenza.

Occorre però, prima di tutto, soffermarsi sulla terminologia propria dei processi di dematerializzazione, in particolare sui concetti di "*memorizzazione*", "*archiviazione*", "*conservazione*", "*riversamento diretto*" e "*riversamento sostitutivo*".

Con il termine "*memorizzazione*" ci si riferisce al processo di trasposizione di documenti analogici o informatici su un qualsiasi supporto idoneo che ne garantisca la leggibilità. E' dunque sinonimo di generica registrazione.

Con il termine "*archiviazione*" ci si riferisce al processo di memorizzazione su qualsiasi supporto idoneo di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente e prodromico all'eventuale processo di conservazione. In poche parole archiviazione è sinonimo di organizzazione, etichettatura e classificazione documentale e non a caso è necessario un codice di riferimento, che agevoli le funzioni di ricerca, di consultazione, di leggibilità, di esibizione e di estraibilità di copia del documento archiviato[22].

Infine, con il termine "*conservazione*", che si riferisce all'esigenza di mantenere integre, inalterate e immodificabili nel tempo le informazioni contenute in un determinato documento[23], si intende quel processo che presuppone la memorizzazione su supporti ot-

---

20 V. anche il D.P.C.M. 11 settembre 1974, "***Norme per la fotoriproduzione sostitutiva dei documenti di archivio e di altri atti delle pubbliche amministrazioni*". L'art. 6 di siffatto provvedimento prevede che "*Per la riproduzione di documenti d'archivio ed altri atti seguita da distruzione dell'originale, ai sensi e per gli effetti dell'art. 25 della legge 4 gennaio 1968, n. 15, è ammesso l'uso di procedimenti tecnici, ivi compresa la microfilmatura in duplex, che diano garanzia di fedeltà al documento riprodotto, di duplicabilità, di leggibilità, di resistenza dell'immagine a tentativi di alterazione fraudolenta e di stabilità illimitata nel tempo, in condizioni normali di conservazione*".**

21 Si ricordi che con D.Lgs. 1 dicembre 2009, n. 177, recante la "***Riorganizzazione del Centro nazionale per l'informatica nella pubblica amministrazione*", il nuovo ente "*DigitPA*" subentra al CNIPA anche in tutti i riferimenti normativi.**

22 In tal senso, al fine di agevolare siffatte funzioni, è opportuno l'utilizzo di determinate parole-chiave (***keywords***) **ovvero di marcatori specifici (cc.dd. "*meta-tag*", ossia metadati presenti nel linguaggio *HTML* utilizzati per fornire informazioni sulle pagine Web agli utenti o ai motori di ricerca di Internet, ma adattabili quali strumenti di indicizzazione ai motori interni a banche-dati o ad archivi elettronici), nonché opportuni formati, in particolar modo se standard, come il *.pdf*.**

23 In relazione a ciò, si ricordi che l'art. 44 del CAD (rubricato "***Requisiti per la conservazione dei documenti informatici*") così dispone:**

"***Il sistema di conservazione dei documenti informatici garantisce:***

- ***a) l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445;***

l'integrità del documento;

la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di registrazione e di classificazione originari;

tici o altri idonei supporti, dei documenti e eventualmente anche delle loro impronte, che termina con l'apposizione della firma digitale e del riferimento temporale sull'insieme dei documenti o su un'evidenza informatica contenente l'impronta[24] o le impronte dei documenti o di insieme di essi da parte del c.d. "*responsabile della conservazione*" (figura sulla quale si tornerà in seguito).

Chiariti questi concetti (su quelli di riversamento diretto e sostitutivo si tornerà nel prosieguo della trattazione), si possono ora analizzare più da vicino i processi di conservazione, tenendo distinta, da un lato, la conservazione dei documenti originariamente informatici e, dall'altro, la conservazione sostitutiva *stricto sensu* dei documenti originariamente analogici. E proprio quest'ultima presenta gli aspetti di maggiore interesse, dal momento che essa consente la totale eliminazione o distruzione della documentazione cartacea.

Per quanto riguarda la prima essa deve essere effettuata mediante memorizzazione dei documenti interessati su supporti ottici o, sebbene non ottici, comunque idonei ai sensi dell'art. 8 della deliberazione n. 11/2004[25] e terminare con l'apposizione sull'insieme dei

---

b) ***il rispetto delle misure di sicurezza previste dagli articoli da 31 a 36 del decreto legislativo 30 giugno 2003, n. 196, e dal disciplinare tecnico pubblicato in Allegato B a tale decreto*".**

Sulle problematiche attinenti alla protezione dei dati personali di cui alla lettera d) dell'art. 44 cit., si tornerà nel prosieguo della trattazione, a proposito delle misure di sicurezza suggerite dal Gruppo dei Garanti europei ex art. 29 della direttiva 95/46/Ce (c.d. "*Direttiva privacy*") e dal Garante italiano per la protezione dei dati personali.

24 **Per "*impronta*" si intende una sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione a una prima sequenza originaria di un'opportuna funzione di *hash*. L'hash è a sua volta una funzione matematica che genera, a partire da una generica sequenza di simboli binari, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali. Siffatti concetti risultano di particolare importanza in relazione alle modalità di sottoscrizione del documento informatico tramite "*firma digitale*" (come definita dall'art. 1, lett. s), del CAD, recentemente modificato dal D.Lgs. 235/2010 cit., laddove ormai la firma digitale non è più un particolare tipo di firma elettronica qualificata, bensì di firma elettronica avanzata), in quanto, per esigenze di tempo e di praticità, la funzione di hash consente di cifrare e dunque di "firmare" solo un breve riassunto del testo di un documento (e non un intero documento, la cui lunghezza è arbitraria e sempre variabile), pochi caratteri cioè che costituiscono per l'appunto l'impronta o *digest* del testo. Il digest sarà sempre di lunghezza fissa (indipendentemente dalle dimensioni del documento originario), ma sarà nel contempo univoco e irreversibile, come sopra scritto.**

25 **Di seguito il testo integrale dell'art. 8 cit.: "*1. Tenuto conto dell'evoluzione tecnologica e della disciplina dettata dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è data facoltà alle pubbliche amministrazioni e ai privati, ove non ostino particolari motivazioni, di utilizzare, nei processi di conservazione sostitutiva e di riversamento sostitutivo, un qualsiasi supporto di memorizzazione, anche non ottico, comunque idoneo a garantire la conformità dei documenti agli originali, nel rispetto delle modalità previste dalla presente deliberazione*".**

Sull'irrilevanza della tipologia di supporti, considerando che la conformità ai documenti è data dal processo di archiviazione/conservazione e non certo dal materiale di cui i supporti sono costituiti, v. l'art. 43, commi 1 e 2, del CAD:

"*1. I documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se* ***la riproduzione e la conservazione nel tempo sono effettuate*** *in modo da garantire la conformità dei documenti agli originali nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.*

2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o

documenti ovvero su un'evidenza informatica contenente l'impronta o le impronte dei documenti o insiemi di essi, del riferimento temporale (ossia l'informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici) e della firma digitale da parte del responsabile della conservazione, figura centrale nei processi di conservazione e disciplinata dall'art. 5 della deliberazione n. 11/2004 cit. Egli in particolare definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, ne organizza conseguentemente il contenuto e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato. Per quel che concerne gli aspetti essenziali della sicurezza sia dei dati archiviati e da conservarsi, sia delle procedure adottate, il responsabile della conservazione, salva l'adozione delle misure di sicurezza prescritte dal D.Lgs. 30 giugno 2003 e succ. modif. (recante il "*Codice in materia di protezione dei dati personali*"), svolge i seguenti compiti:

- fornisce le necessarie indicazioni sulla generazione e sulla gestione delle copie di sicurezza o *backup* (numero, frequenza, formato, priorità, test di *restore*, etichettatura, incarichi e responsabilità);
- verifica la corretta funzionalità del sistema e dei programmi in gestione;
- adotta le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione (custodia fisica; policy procedurali per coloro che sono autorizzati a prelevare e usare i backup; protezione logica tramite crittografia);
- definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;
- verifica periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti (su tali concetti si tornerà nel prosieguo della trattazione).

Resta salva, per il responsabile della conservazione, la possibilità di delegare i propri compiti a una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate (sulla c.d. "delega di funzioni", v. di seguito), nonché la possibilità di affidare il procedimento di conservazione sostitutiva, in tutto o in parte, in *outsourcing*, ossia a soggetti esterni, pubblici o privati.
Se dunque un cartella clinica nasce originariamente come documento informatico e le informazioni che contiene sono elaborate elettronicamente, così come le successive annotazioni, al termine del ciclo della cartella stessa, laddove sia necessario cristallizzare i dati in essa contenuti nel tempo, sarà per es. il primario o il direttore di unità operativa complessa il responsabile della conservazione, in quanto responsabile della regolare compilazione della cartella clinica e dei registri nosologici, nonché della

---

***documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali*".**
Anche l'art. 3, comma 2, del D.M.E.F. 23 gennaio 2004 cit. fa esplicito riferimento a una memorizzazione "*su qualsiasi supporto di cui sia garantita la leggibilità nel tempo*".

loro conservazione fino alla consegna all'archivio centrale[26]. Egli quindi firmerà digitalmente il documento, con annesso riferimento temporale. Ma potrà farlo anche un suo delegato, per es. l'aiuto-medico o l'assistente[27]. In tal modo la cartella clinica viene "chiusa", "sigillata" e acquista quelle caratteristiche di certezza nella provenienza (imputabilità o paternità della cartella e non ripudi abilità), nonché di integrità, immodificabilità e inalterabilità del contenuto nel tempo. Tuttavia alcune considerazioni si impongono.

Per quel che riguarda i supporti ovvero i formati sui quali vengono archiviate e successivamente e conservate le informazioni, essi devono garantire le caratteristiche di "staticità" e "immodificabilità": a tal fine il documento informatico non deve contenere macroistruzioni[28] o codici eseguibili[29], tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati. Quanto ai supporti di tipo ottico risul-

---

26 **V. l'art. 7, comma 1, del d.P.R. 27 Marzo 1969, n. 128, "*Ordinamento interno dei servizi ospedalieri*".**

27 Dovrebbe trattarsi di vera e propria "***delega di funzioni***", **per la quale valgono i principi elaborati ormai da tempo dalla giurisprudenza per es. in materia di compiti spettanti al datore di lavoro per quel che concerne la sicurezza e la tutela della salute e dell'incolumità del dipendente sui luoghi di lavoro. Oggi peraltro siffatti principi hanno trovato espresso riconoscimento normativo nell'art. 16, comma 1, del D.Lgs. 9 aprile 2008, n. 81 e succ. modif., recante la "*Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro*", noto anche come Testo unico sulla salute e sicurezza sul lavoro o "*TUSL*". Tale disposizione recita come segue:**

"*La delega di funzioni da parte del datore di lavoro, ove non espressamente esclusa, è ammessa con i seguenti limiti e condizioni:*

- *a) che essa risulti da atto scritto recante data certa;*
- *b) che il delegato possegga tutti i requisiti di professionalità ed esperienza richiesti dalla specifica natura delle funzioni delegate;*

che essa attribuisca al delegato tutti i poteri di organizzazione, gestione e controllo richiesti dalla specifica natura delle funzioni delegate;

che essa attribuisca al delegato l'autonomia di spesa necessaria allo svolgimento delle funzioni delegate;

che la delega sia accettata dal delegato per iscritto".

Al comma 2 dell'art. 16 cit. è prescritto poi l'obbligo di dare alla delega adeguata e tempestiva pubblicità.

Ad ogni buon conto, l'art. 7 del d.P.R. 128/1969 cit. stabilisce altresì che:

- **l'aiuto medico ospedaliero sostituisce il primario in caso di assenza, impedimento o nei casi di urgenza;**

l'assistente collabora con il primario e con l'aiuto nei loro compiti, ha la responsabilità dei malati a lui affidati, risponde del suo operato all'aiuto e al primario e provvede direttamente nei casi di urgenza;

in caso di assenza o di impedimento dell'aiuto, le sue funzioni sono esercitate dall'assistente con maggiori titoli o dall'assistente di turno.

Con ciò volendosi significare che già di per sé un meccanismo automatico (*ope legis*) di delega esiste già all'interno dell'organigramma e dell'impianto di *line* (gerarchico) ospedaliero.

28 Per la definizione di "***macroistruzioni***", **cfr. http://it.wikipedia.org/wiki/Macro. In genere per macroistruzioni o più semplicemente "*macro*" si intende una procedura o funzione in grado di essere richiamata da eventi ed essere parametrizzata. Le macro consentono di ottenere una serie di operazioni con l'invio di un solo comando. Per es. in un foglio di calcolo, alcune operazioni tipiche di una macro sono inserimento/eliminazione di righe/colonne, formattazione del testo/numero e colore, copia-incolla di valori, esecuzione di funzioni come le somme. Microsoft Office consente l'esecuzione di macro all'interno di un singolo file o aprendo file salvati con i programmi *Outlook*, *Word*, *Excel* o *Powerpoint*. Utilizzare siffatti formati espone per es. al rischio di infezione da virus (cc.dd. macrovirus) ovvero a mutamenti inaspettati e imprevisti di informazioni, come la data.**

29 Per la definizione di "***codice eseguibile***", **cfr. http://it.wikipedia.org/wiki/Eseguibile. In genere per "codice eseguibile" o più semplicemente "*eseguibile*" si intende un *file* che contiene un programma eseguibile per un computer, ovvero un programma scritto in linguaggio macchina e quindi pronto per l'esecuzione. In sostanza è un programma in grado di eseguire altri programmi e di operare in modo non trasparente rispetto all'utente, ossia a sua insaputa. L'eseguibile è spesso usato come veicolo di trasmissione di *malware*, magari celando la propria reale estensione (tecnica c.d. "troiana").**

tano molto utili i dispositivi cc.dd. "*W.O.R.M.*", acronimo per "*Write Once, Read Many*" (o, alternativamente, "*Write One, Read Multiple*"), con riferimento a *storage* (archivi di massa, come CD o DVD), non riscrivibili, ma che consentono molteplici letture. Quanto invece ai formati, suggeriti sono quelli aventi seguenti estensioni:

- *.rtf*, *.odt*, *.pdf*[30], per documenti;

.tiff, *.jpg*, *.gif*, per immagini;
.txt, *.xml*[31], per solo testi.

In secondo luogo, considerando che la firma digitale rende assolutamente "certo" il documento con essa sottoscritto, sia sotto il profilo della connessione univoca del medesimo al suo autore ("*entity authentication*"), sia sotto il profilo della immodificabilità e inalterabilità dei dati in essa raccolti ed elaborati ("*data authentication*"), sorge un problema di correzione degli errori materiali e di aggiornamento della cartella clinica stessa, una volta "cristallizzata" e "sigillata" nel contenuto e nel tempo. Apposite soluzioni tecnologiche dovrebbero consentire al medico pubblico ufficiale estensore o ai suoi ausiliari e/o delegati di integrare o correggere materialmente la cartella clinica elettronica, ormai immodificabile, lasciando comunque evidenza delle integrazioni e delle correzioni, tramite un sistema di annotazione digitale realizzabile con *link* o collegamenti ipertestuali. In tal modo ogni modificazione, a sua volta firmata digitalmente e munita di riferimento temporale, verrebbe associata univocamente, tramite richiamo per mezzo di un codice o numero di protocollo, al documento originale e originario. L'annotazione così conterrebbe gli aggiornamenti e le rettifiche necessarie, con i dovuti riferimenti, e non andrebbe a intaccare il contenuto della cartella clinica precedentemente formata (e comunque cristallizzata e immutabile).

Infine, vero è che la cartella quale particolare forma di "atto pubblico", una volta firmata digitalmente e munita del relativo riferimento temporale, dovrebbe essere opponibile comunque a terzi: insomma avrebbe naturalmente, per come strutturata e cristallizzata al termine del processo di conservazione sostitutiva, la c.d. "*data certa*". Tuttavia, considerando che i certificati digitali qualificati rilasciati per l'utilizzo di dispositivi di firma digitale hanno una durata predefinita e limitata nel tempo[32], quantunque le regole tecniche della deliberazione n. 11/2004 cit. non lo specifichino, sarebbe quanto mai opportuno che il riferimento in questione fosse effettivamente opponibile ai terzi. All'uopo l'associazione al documento informatico di una "*marca temporale*" risulterebbe certamente il metodo più semplice e tecnicamente più adatto. Per marca temporale si intende, ai sensi dell'art. 1 del D.M.E.F. 23 gennaio 2004 cit., una "*evidenza informatica*

30 Lo standard ISO 19005-1:2005 definisce un profilo del formato .pdf (definito a sua volta nello standard ISO 32000), detto ***PDF/A-1*, che, per la sua caratteristica di esser privo di elementi esterni e "dinamici" (come appunto le *macro* e gli *.exe*), assicura, anche grazie al fatto che non si tratta di un formato proprietario, ma di uno standard dello ISO (*International Organisation for Standardization*), la continuità nel tempo (fonte: *iged.it online SPECIALE OMAT ROMA 2008*).**
Vedasi inoltre l'accordo tra l'allora CNIPA (oggi DigitPA) e *Adobe* del 3 marzo 2006, "*Protocollo di intesa per la disponibilità del formato di firma digitale definito nelle specifiche PDF (Portable Document Format) proposto dalla società Adobe Systems Inc.*".

31 Cfr. l'Allegato alla deliberazione n. 34/2006, "***Regole Tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML*".**

32 A tal proposito l'art. 28, lett. f), del CAD, prescrive che tra le informazioni, che devono essere inserite nei certificati qualificati, vi debbono essere anche quelle relative all'indicazione del termine iniziale e finale del periodo di validità del certificato.

che consente di rendere opponibile a terzi un riferimento temporale". Fa eco a siffatta definizione l'art. 1 lett. i) del D.P.C.M. 30 marzo 2009 cit.: "*il riferimento temporale che consente la validazione temporale*", ove "*validazione temporale*" significa per l'appunto "*risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi*" (art. 1, lett. aa), del CAD)[33]. Pertanto una evidenza informatica è sottoposta a validazione temporale mediante generazione e applicazione di una marca temporale alla relativa impronta (art. 43 del D.P.C.M. 30 marzo 2009 cit.). L'apposizione di una marca temporale (che tecnicamente altro non è che una firma digitale che si aggiunge a quella già apposta dal responsabile della conservazione) consentirebbe in poche parole di estendere la validità di un documento informatico, i cui effetti si protraggano nel tempo oltre il limite della validità della chiave di sottoscrizione (e la cartella clinica ha proprio tali caratteristiche, visto che deve essere conservata senza limiti di tempo). Si potrebbe pensare all'apposizione di una marca temporale alla conclusione del processo di redazione della cartella clinica ovvero al momento del decesso del paziente interessato.
Discorso a parte va fatto per la conservazione sostitutiva dei documenti originariamente analogici, tant'è che occorre preliminarmente differenziare a seconda che essa coinvolga documenti analogici originali unici o documenti analogici originali non unici[34]. Esclusivamente per i primi la chiusura del processo di conservazione necessita della presenza di un pubblico ufficiale (notaio o altro pubblico ufficiale rogante), chiamato ad apporre la sua firma digitale e il suo riferimento temporale (o marca per le ragioni sopra indicate).

Per i secondi, invece, è sufficiente l'intervento del responsabile della conservazione che, dopo aver proceduto alla memorizzazione dell'immagine dei documenti direttamente sui supporti idonei, eventualmente, anche della relativa impronta, appone, sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi, il riferimento temporale (o la marca; *ut supra*) e la propria firma digitale a garanzia della corretta esecuzione del processo.

Pertanto, nel caso in cui la cartella clinica nasca originariamente su supporto cartaceo, essa, in qualità di documento analogico unico, dovrà essere trasformata in documento

33 A completamento di quanto già scritto va ricordato il disposto di cui all'art. 47 del D.P.C.M. 30 marzo 2009 cit.:
"***1. Il riferimento temporale assegnato ad una marca temporale coincide con il momento della sua generazione, con una differenza non superiore ad un minuto secondo rispetto alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591*".**
***2. Il riferimento temporale contenuto nella marca temporale è specificato con riferimento al Tempo Universale Coordinato (UTC)*".**
Il "*tempo legale italiano*" (ora esatta) è stabilito dall'I.N.RI.M. (acronimo di "*Istituto Nazionale di Ricerca Metrologica*"), ente pubblico di ricerca, afferente al Ministero dell'Istruzione, dell'Università e della Ricerca, con sede a Torino.

34 Ferma restando la definizione di documento analogico, come vista in precedenza, **l'art. 1, lett. v), del CAD contiene la definizione di "*documenti originali non unici*" quali "*documenti per i quali sia possibile risalire al loro contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi*". Si pensi per es. alle fatture, ai documenti di trasporto, alle ricevute fiscali, agli scontrini fiscali, al libro giornale.**
Per esclusione sono "*documenti originali unici*" proprio quelli per i quali non sia possibile risalire al loro contenuto attraverso altre scritture o documenti. Si possono considerare originali unici, a titolo esemplificativo, i titoli all'ordine di cui agli articoli 2009 e segg. c.c., come l'assegno girato o la cambiale, oppure la "*scheda carburante*", i libri sociali e, per l'appunto, le cartelle cliniche e i referti sanitari.

elettronico, su supporti e in formati che garantiscano immutabilità e staticità, firmata digitalmente (con annesso riferimento temporale) dal primario o dal responsabile della struttura complessa ovvero da un delegato, per poi essere definitivamente firmata digitalmente da un notaio o altro pubblico ufficiale rogante. In caso di aziende ospedaliere o aziende sanitarie locali tale pubblico ufficiale potrebbe essere rappresentato dal direttore sanitario, il quale ex art. 5, comma 1, del d.P.R. 128/1969 cit. "*vigila sull'archivio delle cartelle cliniche*". Il condizionale è però d'obbligo, in quanto va rimembrata la disposizione di cui all'art. 5, comma 4, della deliberazione n. 11/2004 cit.: "*Nelle amministrazioni pubbliche il ruolo di pubblico ufficiale è svolto dal dirigente dell'ufficio responsabile della conservazione dei documenti o da altri dallo stesso formalmente designati, fatta eccezione per quanto previsto dall'art. 3, comma 2, e dall'art. 4, commi 2 e 4, casi nei quali si richiede l'intervento di soggetto diverso della stessa amministrazione*". *Ergo* tra le eccezioni previste, per le quali è richiesto l'intervento di un soggetto esterno alla medesima amministrazione, c'è proprio quella relativa alla conservazione sostitutiva di un documento analogico originale unico (ex art. 4, comma 2, della deliberazione n. 11/2004 cit.), quale è la cartella clinica.

Per quel che riguarda la possibilità di distruzione dell'originale analogico, prevista dall'art. 4, comma 3, della deliberazione n. 11/2004 cit. ("*La distruzione di documenti analogici, di cui è obbligatoria la conservazione, è consentita soltanto dopo il completamento della procedura di conservazione sostitutiva*"), si nutrono parecchi dubbi per quel che concerne siffatta possibilità per la cartella clinica. Infatti la disposizione *de qua* va coordinata con quanto previsto dall'art. 22, commi 5 e 6, del CAD, il cui testo di seguito si riporta integralmente:

"*5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico.*

6. Fino alla data di emanazione del decreto di cui al comma 5 per tutti i documenti analogici originali unici permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico".

In attesa dell'entrata in vigore nel decreto di cui al comma 5, si potrebbe però trovare un espediente giuridico proprio nel comma 6, salva poi l'approvazione in via definitiva del disegno di legge (attualmente al Senato) n. 2243 della XVI Legislatura (già atto della Camera n. 3209), recante "*Disposizioni in materia di semplificazione dei rapporti della Pubblica Amministrazione con cittadini e imprese e delega al Governo per l'emanazione della Carta dei doveri delle amministrazioni pubbliche e per la codificazione in materia di pubblica amministrazione*" (a firma dei Ministri Brunetta, Calderoli, Scajola, Sacconi, Tremonti), il cui art. 7 recita come segue:

"*Art. 7 - Conservazione delle cartelle cliniche*

1. La conservazione delle cartelle cliniche, senza nuovi o maggiori oneri a carico della finanza pubblica, è effettuata esclusivamente in forma digitale. Le copie delle cartelle cliniche sono

rilasciate agli interessati, su richiesta, anche in forma cartacea, previo pagamento di un corrispettivo stabilito dall'amministrazione che le detiene.
2. Le disposizioni del comma 1 si applicano anche alle strutture sanitarie private accreditate.
3. Con regolamento da adottare ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, entro centoventi giorni dalla data di entrata in vigore della presente legge, dal Ministro della salute, di concerto con i Ministri per la pubblica amministrazione e l'innovazione, dell'economia e delle finanze, della difesa e per la semplificazione normativa, sentiti la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano e il Garante per la protezione dei dati personali, nel rispetto di quanto previsto dall'articolo 41 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, sono stabilite le modalità uniformi di attuazione del comma 1 del presente articolo nonché la decorrenza degli adempimenti di cui al medesimo comma 1".
Per concludere, vanno menzionate altre due nozioni di estrema importanza e precisamente quelle di "*riversamento diretto*" e di "*riversamento sostitutivo*".

Con il primo termine si intende il trasferimento di uno o più documenti portati in conservazione da un supporto di memorizzazione a un altro, senza che venga alterata la loro rappresentazione informatica (classico è l'esempio dei "*backup*" o copie di sicurezza). Con il secondo, invece, il trasferimento comporta siffatta alterazione (in gergo informatico si usa anche il termine di "*migrazione*"), per es. per la necessità di un aggiornamento tecnologico dell'archivio informatico, laddove non sia possibile o conveniente mantenere il formato di rappresentazione dei documenti originariamente conservati. La differenza non è da poco giacché, mentre per il riversamento diretto la normativa non prevede particolari formalità, per il riversamento sostitutivo essa prevede l'intervento pur sempre del responsabile della conservazione che deve assicurare il corretto svolgimento del processo. Se il riversamento sostitutivo coinvolge poi documenti informatici sottoscritti, allora sarà addirittura necessario l'intervento di un notaio o altro pubblico ufficiale che, apponendo la propria firma digitale, attesterà la conformità di quanto riversato al documento d'origine.
L'art. 4, comma 4, della deliberazione n. 11/2004 cit. prevede poi specifiche formalità per il riversamento sostitutivo di documenti analogici: "*Il processo di riversamento sostitutivo di documenti analogici conservati avviene mediante memorizzazione su altro supporto ottico. Il responsabile della conservazione, al termine del riversamento, ne attesta il corretto svolgimento con l'apposizione del riferimento temporale e della firma digitale sull'insieme dei documenti o su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi. Qualora il processo riguardi documenti originali unici di cui al comma 2, è richiesta l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto riversato al documento d'origine*".
In tema di riversamento sostitutivo, per quel che concerne tutte le problematiche inerenti all'apposizione della marca temporale e alla corretta individuazione del pubblico ufficiale, si rinvia a quanto sopra scritto.
Sull'affidamento in *outsourcing* di compiti e di responsabilità inerenti alle procedure di archiviazione elettronica e conservazione sostitutiva, si tornerà nel prosieguo della

trattazione.

3.2 La dematerializzazione della documentazione clinica in laboratorio e in diagnostica per immagini

Altro aspetto interessante della dematerializzazione della documentazione sanitaria è rappresentato dai processi di creazione in formato digitale *ab origine* ovvero di conservazione sostitutiva dei referti e delle immagini radiologiche. Le Linee-guida del Ministero della Salute del Marzo 2007 cit. hanno come specifico oggetto proprio tali problematiche e di seguito si cercherà di mettere in evidenza i punti salienti del documento *de quo*.

Va premesso che il referto, per avere dignità giuridica e per ottenere valore legale e probatorio, deve essere sottoscritto dal medico refertante. Per le immagini radiologiche (definibili anche come "*rappresentazioni iconografiche*"), le modalità di gestione sono normate dal D. M. 14 febbraio 1997, che tratta delle specifiche fasi di acquisizione, archiviazione e disponibilità delle stesse. In particolare l'art. 4, comma 1, afferma che *"ove la documentazione iconografica di cui al precedente articolo non venga consegnata al paziente, questa deve essere custodita con le modalità di cui ai successivi commi*". Perciò in tal caso la struttura erogante dovrà attenersi a specifiche modalità di gestione in grado di garantirne la disponibilità. Sulle immagini diagnostiche va poi aggiunto che:

- la circ. n. 61/1986 cit. asserisce che le radiografie non rivestono "*il carattere di atti ufficiali*", ma sono i dati su cui si deve basare la refertazione diagnostica del medico specialista;

mancando l'iconografia di un intrinseco atto medico e dell'indispensabile assunzione di responsabilità professionale per esso, gli elementi essenziali che ne possono definire la giuridica esistenza, considerato che per essa non è richiesta forma predeterminata (certamente non scritta *ad substantiam* ex art. 1350, n.13, c.c.), né v'è obbligo di sottoscrizione, sono quelli derivanti dalla definizione di cui all'art. 2712 c.c. modificato dall'art. 23-quater del CAD (riproduzione meccanica nel genere e informatica nella specie).

Operate tali dovute premesse, si può ora affrontare la tematica della digitalizzazione della documentazione sanitaria diversa da quella rappresentata dalla cartella clinica.

Orbene, il referto di medicina di laboratorio consiste in una relazione scritta contenente prevalentemente, ma non esclusivamente, dati numerici, a fronte della richiesta di esami o di specifici quesiti clinici. Il contenuto rappresenta in genere i risultati degli esami di laboratorio, con le opportune informazioni collegate (per es.: valori di riferimento, commenti, note interpretative, indicazioni, suggerimenti e prescrizioni). Esso necessita della convalida per essere presentato in forma cartacea e/o in forma elettronica al medico curante e per essere consegnato al paziente nei casi previsti (per es. per l'accesso ambulatoriale alla struttura del laboratorio).

Un referto può venire composto, tecnicamente, in molti modi: si spazia dalla redazione manuale mediante uno strumento di *word processing*, sino alla composizione completamente automatica da parte di sistemi che elaborano referti, passando anche per strumenti di dettatura vocale in grado di costruire un referto completo partendo da poche espressioni verbali enunciate dinanzi ad un microfono.

Quale che sia la tecnica utilizzata, il referto elettronico deve essere comunque sottoscritto. In particolare dovrà essere apposta la firma digitale del medico refertante, a se-

conda dei casi:

- tramite firma digitale di un referto singolo previa visualizzazione e conferma;

tramite procedura semiautomatica per firmare un lotto di referti selezionati;
tramite procedura totalmente automatica di firma di referti pre-validati (o comunque individuati in qualche modo) a seconda delle necessità organizzative del laboratorio.
Ognuna di codeste modalità merita attenzione.
La prima modalità è la più semplice. In siffatta ipotesi la firma digitale viene dall'utente apposta a uno specifico referto in un contesto interattivo: poiché l'utente costruisce interattivamente il contenuto del documento, dedicando un certo tempo a questa redazione, si può ipotizzare un controllo visivo diretto su tale contenuto.
La seconda modalità prevede la possibilità di una firma "semi-automatica" di lotti di documenti: è il caso di un utente che deve firmare un insieme di referti già preparati in precedenza. L'utente ha pertanto a disposizione un ambiente operativo che gli permette di vedere una "lista" dei documenti che possono essere firmati, con la possibilità di "navigare" lungo la lista e di aprire individualmente qualsiasi documento per esaminarne il contenuto. L'utente potrebbe selezionare un sotto-insieme di questa lista ed avviare una procedura di firma digitale dei documenti così selezionati, che verrebbero quindi firmati automaticamente senza ulteriori interruzioni. Giuridicamente occorre far riferimento all'art. 35, comma 2, del CAD in materia di "*dispositivi sicuri di firma*"[35].
Infine, quanto alle firme apposte con procedura "automatica", la norma di riferimento è certamente rappresentata dall'art. 35, comma 3, del CAD, concernente il caso in cui un sistema di firma sia stato avviato per processare in modo automatico un flusso di documenti – provenienti da altri sottosistemi – che il titolare della chiave privata (e quindi del dispositivo di firma) non ha modo di controllare puntualmente (a differenza dunque dell'ipotesi della firma semi-automatica). La procedura deve essere realizzata in modo che una fase di avvio informi l'utente sui dettagli operativi della procedura automatica e chieda la sua conferma, che verosimilmente dovrà essere accompagnata dall'inserimento delle credenziali per l'attivazione del dispositivo. Difficilmente un sistema di questo tipo utilizzerà una *smart-card*; più probabilmente farà uso di dispositivi di tipo "*HSM*" (acronimo per "*Hardware Security Module*") in grado di assicurare una procedura automatica di sottoscrizione, una sorta di sistema di "*firma massiva*". Si ricordi inoltre che ai sensi dell'art. 4, comma 2, del D.P.C.M. 30 marzo 2009 cit., "*se il soggetto appone la sua firma per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del codice, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso*".
Ad ogni modo, quale che sia la modalità utilizzata, tra quelle sopra indicate, la firma digitale dei referti di laboratorio identifica la responsabilità del Direttore del Servizio e dei dirigenti che possiedono i requisiti previsti per sottoscrivere i referti.
La firma digitale è necessaria anche per validare i referti di diagnostica per immagini.
Ai fini della conservazione sostitutiva le Linee-guida impongono l'uso della marca temporale. Infatti, quanto al ciclo di vita dei referti, la procedura c.d. di "*consolidamen-*

35 Ai sensi di tale disposizione, i documenti informatici devono essere presentati al titolare (del dispositivo di firma), prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma.

to", necessaria per collegare l'esistenza del documento firmato ad un istante di tempo certo e dimostrabile, si ottiene:

a) verificando con la massima accuratezza la validità del certificato digitale

e

b) associando al documento in questione una marca temporale.

Responsabile del mantenimento nel tempo dei referti riguardanti un paziente interno è la Direzione Sanitaria del presidio ospedaliero ove sono stati redatti. Responsabile della gestione dell'iconografia e del suo mantenimento nel tempo è invece il Responsabile dell'Unità Operativa che ha provveduto alla produzione. Con l'introduzione della gestione digitale e dell'obbligatorio mantenimento nel tempo attraverso la conservazione ottica, responsabili della documentazione (anche della sua archiviazione quindi), fino all'invio della stessa alla conservazione, saranno i responsabili delle Unità Operative che l'hanno prodotta. Da quel momento solo il Responsabile della conservazione, all'uopo individuato e nominato, diverrà responsabile del mantenimento del tempo dei referti e delle immagini.

4. Dematerializzazione della documentazione sanitaria e data-protection

Considerando la delicatezza e l'assoluta importanza dei dati e delle informazioni contenute nella documentazione sanitaria e clinica (dati "*supersensibili*", quali quelli idonei a rivelare lo stato di salute, gli orientamenti sessuali e addirittura dati genetici), della dematerializzazione della medesima non poteva non occuparsi anche il Garante per la protezione dei dati personali italiano, oltre al Gruppo dei Garanti Privacy europei costituito ex art. 29 della direttiva 95/46/Ce (c.d. direttiva in materia di data-protection). In tal senso risultano particolarmente interessanti i seguenti documenti e provvedimenti:

- "*Documento di lavoro sul trattamento dei dati personali relativi alla salute contenuti nelle cartelle cliniche elettroniche (CCE)*", Bruxelles, 15 febbraio 2007, 00323/07/EN, WP 131;

Raccomandazione della Commissione UE del 2 luglio 2008 sull'interoperabilità transfrontaliera dei sistemi di cartelle cliniche elettroniche;

Provvedimento a carattere generale del 5 marzo 2009 (in Bollettino del n. 103/marzo 2009, pag. 0) del Garante Privacy italiano, recante le "*Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario*";

Provvedimento del 26 novembre 2009 del Garante Privacy italiano, "*Dematerializzazione della documentazione clinica*" (http://www.privacy.it/garanteprovv200911262.html).

Non è ovviamente possibile in tale sede analizzare specificamente ogni singolo provvedimento, tuttavia di seguito si cercherà di offrire una sintetica ricostruzione delle direttive, dei criteri e degli obblighi gravanti sui Titolari del trattamento dei personali contenuti nella documentazione clinica digitale (o digitalizzata), nonché sui loro ausiliari (responsabili, ove designati, e incaricati del trattamento) per quel che concerne le misure di sicurezza per la protezione dei dati medesimi.

Restano fermi i principi inderogabili stabiliti dalla direttiva 95/46/Ce e, nel nostro ordinamento nazionale, dal già citata D.Lgs. 30 giugno 2003, n. 196, "*Codice in materia di protezione dei dati personali*", in particolare:

- finalità: il trattamento successivo dei dati è vietato se incompatibile con

le finalità per le quali essi sono stati rilevati;

- qualità dei dati: i dati personali devono essere pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati. Ne deriva che i dati non pertinenti non devono essere raccolti e se lo sono stati, devono essere eliminati. Inoltre il principio impone che i dati siano esatti e aggiornati;

conservazione: i dati personali non devono essere conservati per un arco di tempo superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o successivamente trattati;

informazione: i titolari del trattamento dei dati devono fornire alle persone presso le quali raccolgono tali dati determinate informazioni, in modo tale da fornire per l'appunto una completa "*informativa*" (v. in particolare art. 13 del D.Lgs. 196 cit.) al paziente sulle modalità e finalità del trattamento medesimo, garantendogli il potere di controllo sui suoi dati, assicurandogli altresì un trattamento in forma anonima, laddove ciò sia possibile, tramite tecnologie che rendano tali dati temporaneamente inintelligibili anche a chi è autorizzato;

autodeterminazione: il consenso dell'interessato al trattamento dei dati deve essere libero, informato, consapevole, espresso (scritto *ad substantiam*, laddove si tratti di dati sensibili: v. art. 26, comma 1, del D.Lgs. 196 cit.) e specifico (deve cioè riferirsi a una situazione ben definita e concreta in cui si prevede un trattamento dei dati medici); più in generale deve trattarsi di una decisione volontaria, presa da una persona in pieno possesso di tutte le sue facoltà e senza alcuna forma di coercizione, sociale, finanziaria, psicologica o d'altro tipo e si può in seguito ritirare senza correre il rischio di essere danneggiati, per es. con la minaccia di interruzione delle cure[36];

diritto d'accesso dell'interessato: l'interessato (paziente) ha la facoltà di verificare l'esattezza dei dati e di assicurarsi che siano aggiornati[37];

---

36 Esistono comunque deroghe "obbligatorie", peraltro "tassative" al principio di autodeterminazione, nei casi di:

- **trattamento necessario per salvaguardare un interesse vitale della persona interessata o di un terzo nel caso in cui la persona interessata sia nell'incapacità fisica o giuridica di dare il proprio consenso (art. 26, comma 4, lett. b), del D.lgs. 196 cit.);**
- **trattamento necessario (non meramente utile) per la prevenzione o per la diagnostica medica, per la somministrazione di cure o per la gestione di centri di cura" ed effettuato da un professionista in campo sanitario soggetto al segreto professionale sancito dalla legislazione nazionale, comprese le norme stabilite dagli organi nazionali competenti, o da un'altra persona egualmente soggetta a un obbligo di segreto equivalente (art. 8, paragrafo 3, della direttiva 95/46 cit.)**

Quest'ultima deroga riguarda solo il trattamento di dati personali allo scopo specifico di fornire servizi sanitari di natura preventiva, diagnostica, terapeutica o post-terapeutica e di gestire tali servizi (per es. per la fatturazione, la contabilità o le statistiche). Non è dunque consentito un trattamento successivo che non risulti necessario per la prestazione diretta di questi servizi, come la ricerca medica, il rimborso dei costi da parte di un regime di assicurazione malattia, o il recupero di crediti.

Esiste infine una deroga facoltativa "*per motivi di interesse pubblico rilevante*", autorizzata dall'art. 8, paragrafo 4, della direttiva 95/46 cit. Tuttavia la deroga deve essere contenuta in una disposizione giuridica o in una decisione dell'autorità di controllo (base giuridica speciale). Per quel che concerne i casi di interesse pubblico rilevante, certamente ci si può riferire a ragioni di igiene pubblica e pubblica sanità, nonché di sicurezza sociale (in quest'ultimo caso, per assicurare la qualità e la redditività per quanto riguarda le procedure per rispondere alle richieste di prestazioni e servizi nell'ambito del regime di assicurazione sanitaria), fermo restando che siffatti casi devono essere limitati, proporzionati e espressamente previsti dalla legge. Il ricorso all'art. 8, paragrafo 4, cit. deve inoltre essere notificato dallo Stato membro alla Commissione.

37 L'accesso alla documentazione clinica può essere consentito – a parte allo stesso pa-

correttezza nella gestione transfrontaliera dei dati: i dati possono essere trasferiti in Paesi extra UE solo in forma anonima o, come minimo, con una pseudonimizzazione, salvo pur sempre il consenso esplicito dell'interessato al suddetto trasferimento;
prior checking: prima dell'inizio del trattamento, il progetto di dematerializzazione deve essere presentato al Garante Privacy, affinché possa effettuare una verifica preliminare ai sensi dell'art. 17 del D.Lgs. 196 cit., trattandosi di un trattamento che "*presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può determinare*";
obblighi di notificazione: sempre prima dell'inizio del trattamento e una volta che il Garante Privacy abbia espresso parere positivo in sede di *prior checking*, deve essere effettuata la notificazione al Garante medesimo, in base a quanto previsto dagli artt. 37 e 38 del D.Lgs. 196 cit.;
obblighi di sicurezza: i Titolari del trattamento hanno l'obbligo di attuare misure appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita o dalla diffusione non autorizzata. I dati sanitari di un soggetto, oltretutto, sono spesso collegati con dati relativi ad altri soggetti, terzi rispetto all'interessato (come lo stato di salute o le malattie pregresse dei suoi familiari) e per questo l'attenzione alla sicurezza deve essere massima. Le misure di protezione possono essere logiche, fisiche, tecniche, procedurali e organizzative.
Da quest'ultimo punto di vista, occorre anzitutto affermare che non può esistere dematerializzazione e dunque conservazione digitale della documentazione sanitaria senza "sicurezza". Anzitutto lo stesso CAD, all'art. 44, comma 1-bis, dispone come segue:
"*Il sistema di conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196*[38]*, e, ove previsto, con il responsabile del servizio per*

---

ziente – solo agli operatori sanitari e/o al personale autorizzato delle strutture sanitarie che intervengono in quel momento nelle cure. Inoltre il paziente dovrebbe avere la possibilità, se lo desidera, di impedire l'accesso ai dati del suo fascicolo sanitario: egli cioè dovrebbe poter sapere preventivamente chi desidera accedere ai suoi dati, quando e perché, e le eventuali conseguenze di un rifiuto. Devono a tal fine essere elaborate procedure che evitino indebite pressioni psicologiche sul paziente affinché acconsenta ad autorizzare l'accesso ai suoi dati.

Deve invece essere assolutamente inibito, anche con la previsione di opportune sanzioni, l'accesso nei seguenti casi:

- **ai medici che intervengono come periti per parti terze, per es. per compagnie d'assicurazione private, in controversie;**

per la concessione di aiuti al pensionamento;
ai datori di lavoro dell'interessato.

38 Si riporta di seguito per intero il testo dell'art. 29 cit.: ***"1. Il responsabile è designato dal titolare facoltativamente.***
2. Se designato, il responsabile è individuato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.
3. Ove necessario per esigenze organizzative, possono essere designati responsabili più soggetti, anche mediante suddivisione di compiti.
4. I compiti affidati al responsabile sono analiticamente specificati per iscritto dal titolare.
***5. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale, anche tramite verifiche periodiche, vigila sulla puntuale osservanza delle disposizioni di cui al comma 2 e delle proprie istruzioni*".**
Il sistema di designazione è dunque simile a quello (già sopra esaminato) della "delega di funzioni" e

la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi di cui all'articolo 61 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, nella definizione e gestione delle attività di rispettiva competenza".

Inoltre l'art. 51, comma 1, del CAD (rubricato proprio **"*Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni*"**) prevede che le norme di sicurezza definite nelle regole tecniche di cui all'art. 71 del CAD stesso debbano garantire l'esattezza, la disponibilità, l'accessibilità, l'integrità e la riservatezza dei dati[39] e inoltre che i documenti informatici delle P.A. devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta[40].

Siffatte disposizioni stabiliscono dunque una sorta di "cordone ombelicale" tra D.Lgs. 196 cit. e CAD stesso, volendosi con ciò ribadire l'assoluta importanza della sicurezza ICT nel settore della documentazione amministrativa digitale (o digitalizzata), ivi inclusa quella sanitaria.

E' necessario, anzi obbligatorio, poi che siano scrupolosamente rispettati gli obblighi in materia di misure di sicurezza non solo minime (quelle di cui all'Allegato B al D.lgs. 196/2003, c.d. "*Disciplinare in materia di misure minime di sicurezza*"), ma anche "*idonee e preventive*" stabilite dal Garante Privacy tramite propri provvedimenti a carattere generale (cui in precedenza si è accennato), onde evitare responsabilità di tipo penale[41], amministrativo[42] e civile[43].

In particolare devono essere adottati ed efficacemente attuati i seguenti accorgimenti:

- sistema di "*autenticazione*"[44] (*password* sufficientemente lunghe e robuste, di-

---

risulta molto efficace soprattutto nelle realtà organizzative di medie o grandi dimensioni, quali possono essere proprio le aziende ospedaliere o quelle sanitarie locali o i grandi enti di ricerca e di sperimentazione bio-medica.

39 In attesa che vengano adottate le "nuove" regole tecniche, restano in vigore quelle di cui al D.P.C.M. 30 marzo 2009 cit., cui si affiancano quelle previste dal D.Lgs. 196 cit. e dall'Allegato B al medesimo, come meglio si vedrà nel prosieguo della trattazione.

40 Merita a tal proposito menzione l'art. 31 del D.Lgs. 196 cit. in materia di obblighi generale di sicurezza dei dati personali:

"***I dati personali oggetto di trattamento sono 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*".**

41 L'art. 169 del D.Lgs. 196 cit. prevede in caso di mancata od omessa adozione di misure "minime" di sicurezza la pena dell'arresto sino a due anni. Le misure "minime", è bene ricordarlo, costituiscono quel "***complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31*".** **Esse dunque, proprio perché assicurano un livello minimo di protezione, devono essere predisposte nel quadro dei più generali obblighi di sicurezza di cui all'art. 31 cit. o previsti da speciali disposizioni, quali quelle prescritte da provvedimenti del Garante Privacy.**

42 L'art. 162, comma 2-bis, del D.Lgs. 196 cit. prevede che in caso di trattamento di dati personali effettuato in violazione delle prescrizioni in materia di misure minime è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da diecimila euro a centoventimila euro ed è escluso il pagamento in misura ridotta.

43 L'art. 15 del D.Lgs. 196 cit. stabilisce che "***chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile*".** **Il trattamento di dati personali è considerato pertanto attività pericolosa *ex lege*, con notevoli vantaggi per il danneggiato sul piano dell'*onus probandi*. Ma v'è di più: infatti il danno risarcibile non è solo quello patrimoniale, ma anche quello non patrimoniale per le ipotesi di violazione delle regole di correttezza e liceità nel trattamento dei dati. E' indubbio che condizione indispensabile per garantire la liceità del trattamento sia proprio quella di adottare adeguate misure di protezione dei dati medesimi.**

44 Per "***autenticazione informatica*" si intende ex art. 4, comma 3, lett. c), del D.Lgs. 196 cit., "*l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità*".**

spositivi di firma digitale, *token*, *badge*, codici identificativi, sistemi cc.dd. "*IAM*"[45], etc.);

gestione delle credenziali di autenticazione (custodia delle password, *policy* per la gestione e la custodia delle password, parametri di complessità delle password, mutamento periodico delle password, disabilitazione degli *account* non più utilizzati da almeno sei mesi, verifica periodica e validazione/rivalidazione degli *account*, custodia dei dispositivi di firma elettronica, *help-desk* per i casi di perdita o smarrimento dei dispositivi, etc.);

adozione di un sistema di "*autorizzazione*" e stesura delle lettere di incarico per tutti coloro che svolgono, nella realizzazione dei progetti di dematerializzazione, un trattamento di dati personali, con la specifica indicazione dei privilegi e dei profili autorizzatori[46];

designazione individuale degli "*amministratori di sistema*" e redazione delle relative lettere d'incarico, stesura dell'elenco degli amministratori di sistema e sistema di *log-management*[47];

registrazione (*log*) e documentazione di tutte le fasi del trattamento che hanno avuto luogo nel sistema, specialmente delle richieste d'accesso per leggere o compilare le cartelle cliniche elettroniche e *audit* (verifiche interne regolari e controlli dell'autenticità delle autorizzazioni); i log raccolti dovranno essere garantiti nella loro integrità, immodificabilità e inalterabilità nel tempo e conservati per periodi di tempo pertinenti e non eccedenti;

misure contro specifici rischi (*virus* e altri *malware*; accessi abusivi; trattamenti illeciti e non conformi);

sistemi di *patching management* (aggiornamenti dei sistemi operativi, dei software gestionali e degli applicativi, ivi inclusi i *browser* di navigazione e i *client* di posta elettronica);

procedure di *backup* (cc.dd. "*copie di sicurezza*", sia dei dati che dei programmi, in particolare del software operativo o di base, dei registri di sistema e degli applicativi) e di *disaster recovery*, test di *restore*[48];

---

45 Acronimo per "***Identity Access Management*", sistema automatizzato per la validazione degli *account* e per il controllo degli accessi logici e dei privilegi assegnati ad ogni utente di sistemi informatici e telematici.**

46 Per "***sistema di autorizzazione*" si intende ex art. 4, comma 3, lett. g), del D.Lgs. 196 cit., "** ***l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente*". Per "*profilo di autorizzazione*" si intende ex art. 4, comma 3, lett. f), del D.Lgs. 196 cit., "*l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti*", in poche parole i diritti o privilegi che un utente di un sistema informatico ha sui dati che è autorizzato a trattare. L'autorizzazione all'utente (operatore di sistema), che correttamente è da individuarsi nella figura dell'incaricato del trattamento deve essere contenuta in un'apposita lettera di designazione, scritta e dettagliata, che individui puntualmente l'ambito del trattamento consentito (v. art. 30 del D.Lgs. 196 cit.).**

47 Per siffatte particolari figure di operatori di sistema, v. il Provvedimento a carattere generale del 27 novembre 2008 e succ. modif. "***Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*" (in G.U. n. 300 del 24 dicembre 2008).**

48 Siffatto punto merita particolare attenzione. Devono a tal proposito essere considerate talune regole prescritte dall'Allegato B, precisamente i Punti 18, 21 e 23, di cui di seguito si riporta il testo integrale:

- **Punto 18: "*Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale*";**

Punto 21: "*Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non*

protezione fisica, procedurale e tecnologica dei backup (ambienti protetti, autorizzazioni al prelievo e uso, crittografia, etc.);

- continuità nell'erogazione della corrente elettrica (U.P.S., gruppi elettrogeni);
- procedure di *wiping* e/o di *file-shredding* dei supporti dismessi e riutilizzabili ovvero distruzione, demagnetizzazione, punzonatura, deformazione, etc. di quelli non più utilizzabili[49];

redazione e/o revisione del D.P.S.;

uso della cifratura (crittografia, simmetrica o asimmetrica) o separazione/disgiunzione (tramite codici identificativi) dei dati supersensibili, sia in fase di archiviazione, che in fase di trasmissione/inoltro/transito (protocolli *S/MIME*, *PGP*, *SSL* etc.)[50];

***consentiti*";**

Punto 23: "*Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni*".

Inoltre il Punto 19.5 dell'Allegato B prevede che, all'interno del "*Documento Programmatico sulla Sicurezza*" (o D.P.S.), siano descritti criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al punto 23.

Quest'ultimo punto va coordinato con quanto attualmente previsto dall'art. 50-bis del CAD in materia di "*business continuity*" (continuità operativa) delle P.A.:

"1. In relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongono i piani di emergenza in grado di assicurare la continuità delle operazioni indispensabili per il servizio e il ritorno alla normale operatività.

2. Il Ministro per la pubblica amministrazione e l'innovazione assicura l'omogeneità delle soluzioni di continuità operativa definite dalle diverse Amministrazioni e ne informa con cadenza almeno annuale il Parlamento.

3. A tali fini, le pubbliche amministrazioni definiscono :

a) il piano di continuità operativa, che fissa gli obiettivi e i principi da perseguire, descrive le procedure per la gestione della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle potenziali criticità relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale;

il piano di disaster recovery, che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione.

DigitPA, sentito il Garante per la protezione dei dati personali, definisce le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifica annualmente il costante aggiornamento dei piani di disaster recovery delle amministrazioni interessate e ne informa annualmente il Ministro per la pubblica amministrazione e l'innovazione.

4. I piani di cui al comma 3 sono adottati da ciascuna amministrazione sulla base di appositi e dettagliati studi di fattibilità tecnica; su tali studi è obbligatoriamente acquisito il parere di DigitPA".

Altra importantissima norma di raccordo pertanto tra CAD e D.Lgs. 196 cit.

49 V. a tal proposito il Provvedimento a carattere generale del Garante Privacy del 13 ottobre 2008 in materia di "***Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*". V. altresì** il D.Lgs. 25 luglio 2005, n. 151 ("***Attuazione delle direttive 2002/95/Ce, 2002/96/Ce e 2003/108/Ce, relative alla riduzione dell'uso di sostanze pericolose nelle apparecchiature elettriche ed elettroniche, nonché allo smaltimento dei rifiuti***").

50 Il Garante Privacy ha chiarito che, laddove venisse meno **il requisito operativo corrente della fase clinica, e anche al fine di limitare i rischi di una diffusione incontrollata dei dati, può essere indicata una conservazione in forma crittografata per la fase di archiviazione storica o, in alternativa, l'impiego in questa fase di forme di anonimizzazione dei dati identificativi.**

Inoltre l'oscuramento crittografico (o comunque il trattamento disgiunto tramite codici identificativi) dei dati può risultare una soluzione tecnologica adatta laddove la legge imponga l' "anonimato" della

implementazione di dispositivi di "*firma digitale*", dei supporti e dei formati idonei per garantire integrità, autenticità e immodificabilità dei dati, ivi inclusa la "*marca temporale*" (*time-stamp*);
protezione delle aree e dei locali dove viene realizzato il progetto e dove avvengono i trattamenti dei dati sensibili (sistemi anti-incendio; rilevazione e allarme fumi in ambiente; rilevatori di temperatura e di umidità;, allarme anti-intrusione; blindature; registri di controllo degli accessi fisici, badge; guardie particolari giurate; video-sorveglianza; etc.);
istruzioni chiare e documentate per tutto il personale autorizzato su come usare correttamente i sistemi di archiviazione, conservazione e trattamento informatizzati di dati e su come evitare rischi e violazioni della sicurezza (formazione[51]).
In caso di affidamento dell'attività di archiviazione e conservazione digitale in *outsourcing*, il Garante Privacy ha chiarito che debba essere redatta una dettagliata lettera di istruzioni al fornitore esterno. Tale soggetto dovrebbe essere designato sia responsabile della conservazione sostitutiva, sia responsabile del trattamento dei dati, con specificazione analitica, nell'atto di designazione, delle modalità di conservazione dei documenti e delle misure di sicurezza da adottare. Particolare attenzione dovrà essere posta ai servizi di gestione degli incidenti di sicurezza e dunque al servizio di *Help-desk*, con accesso al servizio attraverso vari canali (telefono, applicazioni software per via telematica, e-*mail*, *fax*). La gestione di una chiamata al servizio di Help-desk deve prevedere almeno le seguenti fasi:

a) registrazione dell'evento (apertura del *ticket*);

erogazione del servizio ovvero risoluzione del problema segnalato;
termine (chiusura del *ticket*).
Il servizio dovrà comprendere la rendicontazione periodica delle chiamate registrate, indicando per ciascuna di esse almeno i seguenti dati: data e ora della chiamata, codice dell'operatore ricevente, problema segnalato, attività svolte a seguito della chiamata ed esito, data e ora di chiusura della chiamata. Per quel che concerne le indicazioni dell'orari di apertura e chiusura del ticket, esse debbono essere prese come riferimento per il calcolo del livello di servizio. Dovrà comunque essere garantito un servizio di manutenzione correttiva e adeguativa. La prima riguarda la diagnosi e la rimozione delle cause e degli effetti di funzionamenti non corretti delle applicazioni. La seconda comprende l'attività

persona. Si pensi alle ipotesi di vittime di atti di violenza sessuale o di pedofilia, di HIV e sieropositività, di uso di sostanze stupefacenti e psicotrope, di abuso di alcool, di interventi di interruzione volontaria della gravidanza, di disconoscimento di maternità, di servizi offerti dai consultori familiari.

51 Il Punto 19.6 stabilisce che il D.P.S. deve tra l'altro contenere idonee informazioni riguardo la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. Ne consegue che la formazione è misura di sicurezza minima a carattere organizzativo, deve essere effettuata obbligatoriamente una volta all'anno, presumibilmente in prossimità della scadenza del 31 marzo di ciascun anno, termine entro il quale il D.P.S. deve essere aggiornato, e se ne dare atto nel D.P.S. stesso (possibilmente dovrebbe essere predisposta apposita documentazione che certifichi e documenti l'avvenuta formazione).

volta ad assicurare la costante aderenza delle applicazioni all'evoluzione dell'ambiente tecnologico del sistema informativo del fornitore, nonché l'adeguamento a modifiche normative.
Da ultimo si ricordi che:

- ai sensi del Punto 19.7 dell'Allegato B, il D.P.S. deve contenere anche la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare;

ai sensi del Punto 25 dell'Allegato B, il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

5. Conclusioni

La via della modernizzazione è ormai tracciata. Tanti segnali sono in tal senso (si pensi recentemente all'invio telematico di certificati medici, secondo quanto previsto dall'art. 55-septies del D.Lgs. 30 marzo 2001, n. 165 e succ. modif., "*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*", come aggiunto dall'art. 69, comma 1, del D.lgs. 27 ottobre 2009, n. 150, "*Attuazione della legge 4 marzo 2009, n. 15, in materia di ottimizzazione della produttività del lavoro pubblico e di efficienza e trasparenza delle pubbliche amministrazioni*"[52]).
E' ormai non più solo necessario, ma indispensabile e, per così dire, obbligatorio da una parte abbattere i costi di gestione della "carta", dall'altra garantire efficienza, efficacia, economicità, semplificazione e snellimento dell'azione amministrativa. I processi di dematerializzazione, di implementazione di tecnologie che garantiscano maggior rapidità e risparmi (in termini di risorse, tempo ed energie), ma che nel contempo garantiscano altresì le esigenze imprescindibili di sicurezza e protezione dei dati, dei sistemi e delle infrastrutture tecnologiche, procedono proprio nella direzione che oggi l'uomo contemporaneo si aspetta. E' chiaro che serviranno investimenti, sensibilizzazione, formazione, informazione, abbattimento di barriere culturali e graduale riduzione del "*digital divide*", ma servirà anche il coraggio del cambiamento, servirà costanza nel cambiamento, seppur secondo una politica accorta e portata avanti con calma e prudenza. D'altronde è sempre meglio una riforma lenta, ma graduale e sensibile, che una rivoluzione immediata, ma che talora risulta disastrosa. Non a caso: "*Non la forza, ma la costanza di un alto sentimento fa gli uomini superiori* (Friedrich W. Nietzsche).

**** **** ****

Telesio Perfetti

---

52 Cui vanno aggiunti i segg. provvedimenti:

- **Decreto del Ministero della Salute 26 febbraio 2010, "*Definizione delle modalità tecniche per la predisposizione e l'invio telematico dei dati delle certificazioni di malattia al SAC*";**

Circ. 11 marzo 2010, n. 1 (in G.U. n. 112 del 15 maggio 2010), "*Indicazioni operative per la trasmissione per via telematica dei certificati di malattia, ai sensi dell'articolo 55-septies del decreto legislativo 30 marzo 2001, n. 165, introdotto dall'articolo 69 del decreto legislativo 27 ottobre 2009, n. 150*".

Avvocato in Roma

Docente di "*Diritto dell'informatica e delle comunicazioni*" presso l'Università degli Studi di Perugia - Dipartimento di Matematica e Informatica

www.studiolegalefd.it
http://computerlaw.wordpress.com

E-Mail: perfetti@computerlaw.it
P.E.C.: telesioperfetti@ordineavvocatiroma.org

Profilo pubblico su LinkedIN: http://it.linkedin.com/pub/telesio-perfetti/26/515/881