

BOZZA

LINEE GUIDA PER LA DEMATERIALIZZAZIONE

DELLA DOCUMENTAZIONE CLINICA IN LABORATORIO E IN DIAGNOSTICA PER IMMAGINI NORMATIVA E PRASSI

V19 – MARZO 2007

MINISTERO DELLA SALUTE

SOMMARIO

1	AUTORI	4
2	INTRODUZIONE	5
3	PREMESSE GIURICHE E NORMATIVE	7
3.1	VALORI GIURIDICO, MEDICO-LEGALE E PROBATORIO DEL REFERTO E DELL'ICONOGRAFIA	7
3.2	TIPOLOGIE DI SOTTOSCRIZIONE INFORMATICA	8
3.3	VALENZA PROBATORIA DEL DOCUMENTO INFORMATICO SOTTOSCRITTO	9
3.4	VALENZA PROBATORIA DEL DOCUMENTO INFORMATICO NON SOTTOSCRITTO (RIPRODUZIONI INFORMATICHE EX ART. 2712 COD. CIV.)	10
3.5	UTILIZZO PROBATORIO IN GIUDIZIO	11
4	DOCUMENTI DA DEMATERIALIZZARE	12
4.1	DOCUMENTAZIONE DI DIAGNOSTICA PER IMMAGINI	12
4.1.1	REFERTO	12
4.1.2	IMMAGINI	13
4.1.3	TEMPI DI CONSERVAZIONE	14
4.1.4	CONTESTO DI UTILIZZO	19
4.2	DOCUMENTAZIONE DI LABORATORIO DI ANALISI	19
4.2.1	REFERTO DI MEDICINA DI LABORATORIO	19
4.2.2	TEMPI DI CONSERVAZIONE	20
5	CLASSIFICAZIONE FASCICOLAZIONE SCARTO	22
5.1	CLASSIFICAZIONE E FASCICOLAZIONE	22
5.2	SCARTO DEI DOCUMENTI	24
6	AUTENTICAZIONE DOCUMENTI	26
6.1	PREMESSA – MODALITA' DI SOTTOSCRIZIONE DIGITALE	26
6.1.1	FIRMA SINGOLA APPOSTA IN CONTESTO INTERATTIVO	26
6.1.2	FIRMA SEMIAUTOMATICA DI LOTTI DI DOCUMENTI	27
6.1.3	FIRME APPOSTE CON PROCEDURA AUTOMATICA	27
6.2	PREMESSA – CICLO DI VITA DEI REFERTI	28
6.2.1	SIGN-ON DEL SOTTOSCRITTORE	28
6.2.2	SOTTOSCRIZIONE	28
6.2.3	CONSOLIDAMENTO	29
6.2.4	CONSERVAZIONE SOSTITUTIVA	30
6.2.5	CONSIDERAZIONI	30
6.3	FIRMA DIGITALE DEL REFERTO DI MEDICINA DI LABORATORIO	31
6.4	FIRMA DIGITALE DEI REFERTI DI DIAGNOSTICA PER IMMAGINI	31
6.5	AUTENTICAZIONE DELLE IMMAGINI	32
7	CONSOLIDAMENTO DEI DOCUMENTI	33
7.1	VERIFICA DELLA VALIDITÀ DEL CERTIFICATO	34
7.1.1	CRL – LISTE DI SOSPENSIONE E REVOCA	34
7.1.2	SERVIZIO PUNTUALE DI INFORMAZIONE SULLO STATO DI VALIDITÀ DI UN CERTIFICATO, EROGATO DAL CERTIFICATORE	35
7.1.3	APPROCCIO ORGANIZZATIVO	35
7.1.4	CONSIDERAZIONI	36
7.2	VERIFICA DELLA VALIDITÀ DEL CERTIFICATO	36
8	CONSERVAZIONE SOSTITUTIVA DEI DOCUMENTI	38
8.1	DOCUMENTI DEMATERIALIZZATI DA CONSERVARE	38
8.2	RESPONSABILE DEL PROCEDIMENTO DI CONSERVAZIONE SOSTITUTIVA	38
8.3	NOMINA DEL RESPONSABILE, DELEGHE E INCARICHI	41
8.4	SUPPORTI PER LA CONSERVAZIONE SOSTITUTIVA	42

8.4.1	LA PRASSI	45
8.5	PROCEDURE DI CONSERVAZIONE SOSTITUTIVA.....	46
8.5.1	FORMATO DEL FILE DELLE IMPRONTE.....	46
8.5.2	MODALITA' DI MEMORIZZAZIONE	47
8.5.3	DIMENSIONI DEI VOLUMI.....	48
8.5.4	AGGREGAZIONE DEI DOCUMENTI NEI VOLUMI	48
8.5.5	PROCEDURE DI ACCUMULO E CHIUSURA DEI VOLUMI.....	49
8.5.6	INTERVALLI TRA DUE ESECUZIONI DEL PROCESSO DI CONSERVAZIONE	49
9	ESIBIZIONE DEI DOCUMENTI	50
9.1.1	REFERTI E IMMAGINI DIGITALI	50
10	APPLICAZIONE DELLA DEMATERIALIZZAZIONE NEI SISTEMI CLINICI.....	52
10.1	DEMATERIALIZZAZIONE DEI REFERTI.....	54
10.2	DEMATERIALIZZAZIONE DELLE IMMAGINI RADIOLOGICHE	59
10.3	DEMATERIALIZZAZIONE DEL REFERTO RADIOLOGICO STRUTTURATO.....	61
11	NORMATIVA E LINEE GUIDA DI RIFERIMENTO.....	64
11.1	NORMATIVA DI RIFERIMENTO DI CARATTERE GENERALE.....	64
11.2	NORMATIVA DI RIFERIMENTO PER DOCUMENTAZIONE DI DIAGNOSTICA PER IMMAGINI... 64	64
11.3	NORMATIVA DI RIFERIMENTO PER REFERTI DI LABORATORIO DI ANALISI	64
11.4	NORMATIVA DI RIFERIMENTO PER FIRMA DEI DOCUMENTI.....	65
11.5	NORMATIVA DI RIFERIMENTO PER CONSOLIDAMENTO	65
11.6	NORMATIVA DI RIFERIMENTO PER CONSERVAZIONE SOSTITUTIVA	65
11.7	NORMATIVA DI RIFERIMENTO PER L'ESIBIZIONE	65
12	GLOSSARIO.....	66

1 AUTORI

Il presente documento è stato diretto e curato da:

MINISTERO DELLA SALUTE

- Walter Bergamaschi - Direzione Informatica
- Lidia di Minco – Direzione Informatica

con la collaborazione di:

MINISTERO DEI BENI CULTURALI

- Micaela Procaccia - Archivi

DIT - DIPARTIMENTO INNOVAZIONE TECNOLOGICA

- Katia Colantonio – Innovazione Italia
- Stefano Lotti – Innovazione Italia
- Orsola Venute – Innovazione Italia
- Daniela Berardi – Innovazione Italia

CNIPA

- Maurizio Gentilini

SIRM – SOCIETÀ ITALIANA RADIOLOGIA MEDICA

- Roberto Grassi
- Franco Vimercati

AIFM – ASSOCIAZIONE ITALIANA DI FISICA MEDICA

- Alberto Del Corona – Azienda ASL n. 6 di Livorno

SIMEL – SOCIETÀ ITALIANA MEDICI DI LABORATORIO

- Piero Cappelletti, AO Pordenone
- Davide Giavarina – ULSS Vicenza

AMCLI – ASSOCIAZIONE DEI MICROBIOLOGI CLINICI ITALIANI

- Giacomo Fortina, AO Novara
- Roberto Rigoli – ULSS Treviso

SiBioC – SOCIETÀ ITALIANA DI BIOCHIMICA CLINICA E BIOLOGIA MOLECOLARE

- Mario Plebani, AOU Padova
- Michele Mussap, AOU San Martino Genova

AITECH - ASSINFORM

- Vincenzo Gambetta

IHE – INTEGRATING THE HEALTHCARE ENTERPRISE

- Claudio Saccavini – Project Manager IHE Italia
- Roberto Silverio – Project Manager Radiologia IHE Italia
- Andrea Giovagnoni – Co-chair IHE Italia
- Palmino Sacco – Co-chair IHE Italia
- Roberto Baudizzone – CompEd s.r.l.
- Umberto Ferri – Medas s.r.l.
- Roberto Ponte – LeDoc s.r.l.
- Alessandra Ramelli – LeDoc s.r.l.
- Stefano Floris – Metafora s.r.l.
- Antonio Redaelli – Metafora s.r.l.
- Cristina Zonta – Insiel s.p.a.

2 INTRODUZIONE

Il presente documento ha l'obiettivo di fornire ai Direttori Generali, Direttori Sanitari, Direttori/Responsabili dei Sistemi Informativi e dei Dipartimenti e U.O. di Diagnostica per Immagini, Radiologia, Medicina Nucleare e Servizi di Medicina di Laboratorio, le linee guida per poter gestire la documentazione clinica testuale e iconografica in formato digitale, nel rispetto delle attuali normative.

Quanto riportato vale per le strutture sanitarie pubbliche e private, come asserisce il D. Lgs n. 82/05 che, pur rivolgendosi precipuamente alla Pubblica Amministrazione, prevede espressamente all'art. 2 co. 3 i destinatari delle proprie disposizioni concernenti "i documenti informatici, le firme elettroniche, ...", relative alla formazione, gestione, alla conservazione, nonché le disposizioni... relative alla trasmissione dei documenti informatici si applicano anche ai privati ai sensi dell'articolo 3 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445" ancora parzialmente in vigore.

Già oggi, le U.O. di Laboratorio di Analisi e di Diagnostica per Immagini sono i reparti maggiormente informatizzati delle strutture sanitarie italiane. Questi reparti rappresentano i servizi che, insieme, producono il maggior numero di documentazione clinica, sia per Pazienti interni che per Pazienti esterni.

In considerazione di questi argomenti, si sottolinea che il presente documento vuole unicamente dare direttive pratiche e raggiungibili per la completa dematerializzazione degli archivi di referti di Laboratorio e di referti e immagini di Diagnostica per Immagini, da analogici (cartacei e pellicole) a digitali.

In questo ambito non viene trattata la dematerializzazione di:

- documenti di archivi analogici e digitali pre-esistenti sia testuali che iconografici;
- consenso informato dei Pazienti relativamente ad atti medici.

Non rientra inoltre nei compiti degli autori definire o indirizzare atteggiamenti deontologici quali:

- trasferimento dei documenti clinici (teleconsulti, telerefertazione, ...);
- quantità (e.g.: numero di immagini), tipologia o qualità (e.g.: immagini grezze, filtrate, elaborate) di documentazione clinica da archiviare o da esibire;
- supporto sul quale esibire i risultati.

In considerazione delle evoluzioni tecnologiche e normative, è prevedibile che il presente documento venga aggiornato periodicamente.

Per maggiore completezza è sin d'ora indispensabile evidenziare che tutte le attività che si vanno a trattare nelle presenti linee guida (firma, consolidamento, archiviazione e conservazione del documento informatico, esibizione) rientrano a pieno titolo nelle attività previste dall'art. 4, co. 1, lett. a) del D.lgs n. 196/03 – Codice in materia di protezione dei dati personali, secondo il quale il trattamento va inteso come "qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati".

Inoltre, è da sottolineare che tutti i procedimenti di dematerializzazione qui affrontati riguardano dati personali idonei a rivelare lo stato di salute del paziente, per il trattamento dei quali è

assolutamente necessario prestare la massima cura, ottemperando con precisione alle imposizioni del D.Lgs. n. 196/03 e dei suoi allegati. In particolare, al Titolo V del Codice e nello specifico Allegato B, il Legislatore si è dimostrato estremamente attento a questi dati di forte interesse pubblico e alle attività ad essi correlate: ciò pretendendo che minime e idonee misure vengano messe in atto per poter procedere al trattamento e garantire la riservatezza delle informazioni e la sicurezza dei sistemi che le gestiscono.

3 PREMESSE GIURICHE E NORMATIVE

3.1 VALORI GIURIDICO, MEDICO-LEGALE E PROBATORIO DEL REFERTO E DELL'ICONOGRAFIA

Il referto è l'atto obbligatoriamente redatto in forma scritta col quale lo specialista dichiara conformi a verità i risultati degli esami diagnostici ottenuti, unitamente all'interpretazione clinica dei risultati stessi, in relazione al quadro clinico e all'anamnesi del paziente¹.

L'analisi giuridica deve essere ulteriormente approfondita: premesso l'obbligo perché si abbia la giuridica esistenza (art. 1350, n.13 cod. civ. forma scritta ad substantiam), vi è la necessità di inquadrare il referto nella categoria dell'atto pubblico o in quella della scrittura privata.

Si ritiene di poter fermamente sostenere che il referto medico di nostro interesse debba rientrare nella tipologia della scrittura privata².

Per quanto concerne invece la forma scritta "digitale" del referto, premesso che l'art. 2702 del Codice Civile asserisce che "la scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta", se ne evince che il codice si sofferma ad individuare gli elementi essenziali per l'esistenza giuridica della scrittura privata: il documento deve essere composto da una dichiarazione scritta, proveniente dal soggetto interessato e sottoscritta da quest'ultimo.

Nulla il Codice Civile dice sulle modalità di redazione della scrittura privata né si sofferma sui supporti o sui mezzi di scrittura, sulla firma e sulla conservazione dei documenti.

Esso può quindi avere qualsiasi forma tecnologica, purché idonea a raggiungere lo scopo desiderato.

Pertanto, proprio in base all'art. 2702 del Codice Civile sopra riportato, il referto, per avere dignità giuridica e per ottenere valore legale e probatorio, deve essere sottoscritto dal medico refertante.

Del contenuto del referto vi deve essere un'assunzione di responsabilità da parte di colui che lo ha redatto; è proprio la sottoscrizione che attribuisce la paternità dell'atto e permette, anche in un momento successivo, di risalire all'autore di questo.

Infine, secondo la definizione di risultato³, si è certi di poter affermare che l'immagine radiologica è un suo tipico esempio, come lo possono essere i preparati istologici e citologici. La stessa Circolare

¹ E' necessario prevedere e inquadrare giuridicamente il referto medico, attribuendo al termine "referto" significati diversi a seconda del soggetto che lo stende e del contesto in cui esso viene redatto, per fargli ottenere anche valenze legali e probatorie differenti.

Il risultato è il puro esito degli esami diagnostici eseguiti mediante strumentazioni cliniche in un Servizio (Laboratorio, Radiologia, ...); un prodotto privo di interpretazione o valutazione clinica da parte dello specialista, ovvero una lettura pura e semplice di un dato analitico.

Il certificato è il documento a cui il medico è obbligato (in base anche all'art.22 del Codice di deontologia medica 1998) e nel quale deve limitarsi ad attestare i dati obiettivi di competenza tecnica che abbia direttamente constatato in totale aderenza alla realtà.

² Secondo il diritto, gli atti pubblici devono possedere requisiti ben individuati e devono essere redatti da un pubblico ufficiale. Per il referto diagnostico, le norme vigenti non prevedono alcuno dei rigidi requisiti dell'atto pubblico codificato.

Ministero della Sanità n. 61 del 19 dicembre 1986, N. 900.2/ AG. 464/260, concernente il "Periodo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura", 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, Cod. Civ.) né obbligo di sottoscrizione, sono quelli derivanti dalla definizione di cui all'art. 2712 Cod. Civ. modificato dall'art. 23 del D. Lgs. 82/2005: riproduzione meccanica nel genere e informatica nella specie.

Grazie alle odierne caratteristiche dell'iconografia, possono essere inoltre sfruttate le facilitazioni tecnologiche per garantire la sicurezza, la riservatezza e l'immodificabilità del dato, che peraltro altra parte della normativa in vigore impone, individuando, tracciando ed evidenziando ogni attività e tutti i soggetti agenti.

3.2 TIPOLOGIE DI SOTTOSCRIZIONE INFORMATICA⁴

In estrema sintesi e per restare ancorati alle definizioni di legge, si possono indicare le seguenti tipologie di sottoscrizione (latamente definibile) informatica:

- **La "firma elettronica non qualificata o c.d. leggera"** (D. Lgs. 82/05, art. 1, comma 1, lett. q, modif. dal D. Lgs. 4 aprile 2006 n. 159 in G.U. n. 99 del 29 aprile 2006)⁵.
- **La "firma elettronica qualificata"** (D. Lgs. 82/05, art. 1, comma 1, lett. r, modif. dal D. Lgs. 4 aprile 2006 n. 159 in G.U. n. 99 del 29 aprile 2006)⁶.

Da inquadrare nel genere "firma elettronica qualificata" è la "firma digitale" (D. Lgs. 82/05, art. 1, comma 1, lett. s)⁷.

³ Si veda la nota 1.

⁴ Giova, preliminarmente sottolineare che la sottoscrizione informatica differisce – in essenza – dalla sottoscrizione autografa e che proprio l'utilizzo del termine "firma" (utilizzato invece nell'accezione comune e soprattutto nel codice civile, per indicare la sottoscrizione autografa), allo scopo di definire quella tecnologia informatica cui essa è legata (soprattutto, come vedremo, se digitale), non deve generare nell'operatore un timore maggiore di quello che esso tranquillamente gestisce durante la propria giornata lavorativa utilizzando gli altri strumenti tecnologici.

⁵ "L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica"

⁶ "La firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma"

⁷ È "un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici".

3.3 VALENZA PROBATORIA DEL DOCUMENTO INFORMATICO SOTTOSCRITTO

Il documento informatico sottoscritto con :

- **“firma elettronica non qualificata o c.d. leggera”** (d.lgs. 82/05, art. 1, comma 1, lett. q, modif. dal D. Lgs. 4 aprile 2006 n. 159 in G.U. n. 99 del 29 aprile 2006)⁸ è **liberamente valutabile in giudizio**⁹ (art. 21, comma 1 D.Lgs. 82/05)
- **“firma elettronica qualificata”** (d.lgs. 82/05, art. 1, comma 1, lett. r, modif. dal D. Lgs. 4 aprile 2006 n. 159 in G.U. n. 99 del 29 aprile 2006) ha **l'efficacia di scrittura privata**¹⁰ prevista dall'art. 2702 del Codice Civile (art. 21, comma 2 D.Lgs. 82/05) e risponde al requisito della **forma scritta**¹¹ (art. 20, comma 3 D.Lgs. 82/05).

La forza innovativa del citato art. 21, 2. comma, è evidente laddove, di fatto, equipara, quale prova da utilizzare in un giudizio, il documento informatico, digitalmente sottoscritto, al documento analogico (ad es. cartaceo) cui sia apposta una sottoscrizione autografa.

La natura giuridica di “scrittura privata” non è senza conseguenze (tranquillizzanti) sul piano pratico per chi opera con la firma digitale (ad es. colui che referta e di conseguenza la Struttura).

Infatti, come per il documento cartaceo autografo, anche per il documento informatico digitalmente sottoscritto, il valore probatorio (essendo di natura presuntiva) potrà essere neutralizzato esclusivamente da colui (l'operatore) contro il quale esso verrà prodotto in giudizio e ne disconoscerà la sottoscrizione (digitale), negando, di conseguenza, la paternità delle dichiarazioni in esso contenute¹².

PRECISAZIONE TERMINOLOGICA: chiunque operi con la firma digitale dovrà tenere conto della distinzione tra l'efficacia probatoria della **“scrittura privata”** (di cui si è trattato finora) ed efficacia probatoria della **“scrittura privata riconosciuta”**¹³.

⁸ “L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica”.

⁹ Tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità. In altri termini sarà affidata alla discrezionalità (motivata) del Giudicante stabilire se esso soddisfi il requisito della forma scritta e quindi il valore probatorio.

¹⁰ Che consente di attribuire (in base ad un presunzione semplice) la paternità delle dichiarazioni contenute nel documento, al suo sottoscrittore con firma digitale o elettronica qualificata.

¹¹ Forma scritta “ad substantiam” ex art. 1350 cod. civ. numeri da 1 a 12.

¹² Si ricorda inoltre che, non trattandosi di “sottoscrizione autografa” ma di sottoscrizione generata dall'utilizzo di dispositivi basati su tecnologie (semplici, ma) particolari, il titolare sarà ammesso a provare – in sede di disconoscimento della firma digitale - che il predetto utilizzo di dispositivi e tecnologie non sia a lui riconducibile (ad es. per l'abuso compiuto da un terzo che si sia appropriato dei dispositivi di firma).

Naturalmente, il disconoscimento (giudiziale) della sottoscrizione (digitale) del documento informatico, darà luogo alla sua assoluta inutilizzabilità probatoria nel processo (il giudice non potrà dunque decidere alcunché sulla base di esso) se, ex art. 216, 2° comma, c.p.c. la parte che intende giovare (contro il presunto operatore e sottoscrittore) non ne avrà richiesta la verifica o questa non sortisca esito positivo.

¹³ Nella categoria della “scritture private riconosciute” rientrano essenzialmente tre categorie: 1. scritture private con sottoscrizione autenticata da notaio o altro pubblico ufficiale a ciò autorizzato (art. 2703 Cod. Civ.); 2. scritture private non disconosciute da colui contro il quale esse sono prodotte (art. 2702 Cod. Civ.); 3. scritture private disconosciute da colui contro il quale esse sono prodotte che siano state positivamente verificate (in genere tramite una consulenza tecnica che ne accerti la appartenenza al sottoscrittore).

Tali documenti non possono essere disconosciuti, ma fanno piena prova della provenienza delle dichiarazioni di chi li ha sottoscritti.

3.4 VALENZA PROBATORIA DEL DOCUMENTO INFORMATICO NON SOTTOSCRITTO (Riproduzioni informatiche ex art. 2712 Cod. Civ.)

Si ritiene di dovere distinguere due fattispecie di documento "non firmato"¹⁴:

- il **documento informatico che non sia mai stato sottoscritto** (perché ad es. non ne è richiesta la forma scritta quale requisito di esistenza o validità);
- il **documento informatico** che, in virtù dell'art. 21, comma 3, D.Lgs. 82/05, viene dalla legge considerato **privo di firma** in quanto sia stato sottoscritto con firma digitale o altro tipo di firma elettronica **qualificata basata su certificato elettronico scaduto, revocato o sospeso**.

A tali documenti deve essere attribuita l'**efficacia probatoria delle riproduzioni meccaniche** ex art. 2712 Cod. Civ. (riproduzione meccanica e/o riproduzione informatica, giusta modifica di cui all'art. 23, comma 1, cod. amm. Dig it.)¹⁵.

IMPORTANTE: Resta comunque affidato alla libera valutazione del Giudice il riconoscimento della rispondenza di detti documenti al requisito della forma scritta (art. 20, comma 1 bis, D. Lgs. 82/05).

In tali tre casi, l'unico rimedio previsto dal nostro ordinamento sarà la Querela di Falso (c.p.c. art. 221)

¹⁴ Individuabili per legge e che devono essere trattate con i medesimi criteri in relazione al loro valore probatorio ed alla possibilità che ne venga riconosciuta giudizialmente la forma scritta.

¹⁵ Sarà, pertanto, possibile utilizzarli a scopi probatori in giudizio e formeranno piena prova (ancorché, si ripete, non sottoscritti digitalmente) dei fatti e delle cose in essi rappresentate.

Sarà onere della parte contro cui siano prodotti (che potrà, contrariamente a quanto avviene per il disconoscimento di sottoscrizione della scrittura privata, essere anche un soggetto diverso da colui che li ha generati) di ripudiarne in giudizio la conformità ai fatti o alle cose medesime.

La "piena prova" verrà esclusa con il disconoscimento del documento "non firmato" e tuttavia, diversamente a quanto avviene, come si è appena detto, in caso di disconoscimento del documento informatico digitalmente sottoscritto, tale rifiuto (da parte di colui contro il quale esso viene prodotto) non precluderà (per giurisprudenza della Suprema Corte) al giudice la possibilità di accertarne la conformità ai fatti ed alle cose rappresentate, anche attraverso altri mezzi di prova, ivi comprese le presunzioni (cfr. sentenza n. 11445/01 della Suprema Corte).

L'operatore ha dunque in questo caso una tutela piena che è identica a quella che gli competeva nell'era del solo analogico (si pensi ad es. a chi opera nel settore dell'iconografia che, si ritiene, non richieda – per la sua giuridica esistenza - la forma scritta : 'atto pubblico o scrittura privata).

Identico uso probatorio potrà essere fatto per i documenti informatici che richiedano la forma scritta per essere considerati giuridicamente esistenti (c.d. forma scritta ad substantiam).

A tal uopo occorre precisare che, in forza dell'art. 20, comma 2, D. Lgs. 82/05, il documento informatico privo di firma digitale o di firma elettronica qualificata non soddisfa il requisito della forma scritta (questa norma, peraltro, combinata a quanto previsto dall'art. 21, 3 comma, della medesima legge, ha sgombrato il campo dai dubbi interpretativi indotti dall'abrogato art. 10, 2 comma, DRR 445/2000, secondo il quale il documento informatico con firma elettronica soddisfa il requisito legale della forma scritta).

3.5 UTILIZZO PROBATORIO IN GIUDIZIO

Al solo scopo di dare completezza alla trattazione di cui sopra, trattando delle modalità pratiche di utilizzo processuale dei documenti informatici (sottoscritti e non), è stata individuata una chiara distinzione tra documenti informatici riproducibili o non riproducibili in analogico (su carta).

Nel primo caso il Giudice istruttore, se lo riterrà utile e/o necessario per costituire un documento "cartaceo" opponibile ad ogni effetto a tutte le parti del giudizio, potrà procedere personalmente ex art. 261 c.p.c. alle operazioni di stampa su carta fissando a tal uopo un'udienza alla presenza di tutte le parti e verbalizzando (atto pubblico ex art. 2699 c.c.) la piena conformità tra documento cartaceo e informatico.

Se invece il documento informatico non potrà essere riprodotto su carta, il giudice ne effettuerà l'esame in apposita udienza, alla presenza di tutte le parti in contraddittorio tra loro, utilizzando lo strumento di cui all'art. 259 c.p.c. ossia l'ispezione intesa nel suo significato più ampio, con l'assistenza, quando occorre, di un Consulente Tecnico d'Ufficio che consenta di visualizzare e interpretare il suono e le immagini.

4 DOCUMENTI DA DEMATERIALIZZARE

Ai fini della conservazione legale di referti e immagini, con l'avvio di una gestione digitale, è importante evidenziare come non vi sia più senso alcuno nel differenziare fra paziente interno e paziente esterno. Come verrà meglio sottolineato in seguito nel presente documento, da un punto di vista organizzativo, procedurale e medico legale, si deve propendere oggi per la conservazione legale della documentazione radiologica prodotta per tutti i pazienti afferenti alla Struttura. Archiviare e conservare tutta la documentazione sta divenendo sempre più necessario: da un punto di vista clinico, con il rapido accesso a tutti gli approfondimenti diagnostici precedenti, da un punto di vista organizzativo, con la razionalizzazione e l'ottimizzazione di risorse umane e tecnologiche, da un punto di vista medico-legale, con la totale disponibilità nella Struttura della documentazione originale immutabile.

4.1 DOCUMENTAZIONE DI DIAGNOSTICA PER IMMAGINI

4.1.1 REFERTO

L'art. 3 del D. M. 14.2.97, quale norma di attuazione prevista dall'art. 111, comma 10 del D. L.gs n. 230 del 17.3.95, definisce chiaramente la documentazione radiologica, diversificando l'iconografia dai resoconti¹⁶.

"1. La documentazione disciplinata dal presente decreto ... è così stabilita: a) documenti radiologici e di medicina nucleare: consistono nella documentazione iconografica prodotta a seguito dell'indagine diagnostica utilizzata dal medico specialista nonché in quella prodotta nell'ambito delle attività radiodiagnostiche complementari all'esercizio clinico; b) resoconti radiologici e di medicina nucleare: referti stilati dal medico specialista radiologo o medico nucleare".

Si può pertanto asserire che il resoconto radiologico è proprio il referto medico, che va inteso come l'atto scritto col quale il Medico Radiologo o Medico nucleare formula l'interpretazione dell'immagine ottenuta dagli esami diagnostici, tenendo conto del quadro clinico e dell'anamnesi del paziente. I documenti radiologici sono invece le immagini, quali risultato dell'esecuzione dell'indagine diagnostica, ovvero il puro esito degli esami eseguiti mediante strumentazioni; esso è

¹⁶ Il D. L.gs n. 187/2000 è la norma italiana con cui è stata recepita la direttiva 97/43/ EURATOM in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche. Con l'art. 15 del decreto legislativo sono stati espressamente abrogati gli articoli da 109 a 114 compresi del D. L.gs n. 230/95, portando il panorama radiologico e giuridico a domandarsi se l'abrogazione dell'art. 111 del D.L.gs n. 230/95 abbia trascinato con sé anche le norme d'attuazione ivi previste. Un'automatica abrogazione del D. M. 14.2.97 porterebbe invero al venir meno dei concetti giuridici di base ed anche di alcuni di carattere organizzativo e medico-legale concernenti la documentazione radiologica tutta.

Così l'Ufficio Legislativo del Ministero della Salute italiano risponde (Prot.N.100.1.QUF/5.222-992) ad una nota del Dipartimento della Prevenzione (DPV: UO 7/LD 31.187/00/62 del 15.2.2001), asserendo, con riferimento al D. L.gs n. 230, che "... La ratio della disposizione normativa ... è di evitare la ripetizione di esami superflui, consentendo l'utilizzo di documenti radiologici già eseguiti. Ne discende, pertanto, che il decreto ministeriale 14/2/97 che ha stabilito le disposizioni idonee a consentire l'utilizzo di documenti radiologici già eseguiti, sia da considerarsi ancora valido, ancorché l'art. 111 del D.L.gs 230/95, che ha previsto l'adozione del citato decreto ministeriale, sia stato abrogato dall'art. 15 del Decreto Legislativo 187/2000."

pertanto un prodotto privo di interpretazione o valutazione clinica da parte dello specialista, trattandosi di una pura lettura di un dato analitico.

Referto strutturato

In un prossimo futuro, la netta e rigida differenziazione normativa fra referto e immagine radiologica potrebbe essere presto sgretolata dall'avvento del cosiddetto "referto strutturato" (Structured Report, SR): nel mondo radiologico internazionale e nazionale si sta approfondendo l'implementazione di una commistione fra testo referto e immagini correlate e ritenute clinicamente rilevanti per la diagnosi. Sino ad oggi l'analisi si è limitata alla fattibilità tecnologica, ma importanti analisi in ambito clinico, organizzativo e medico-legale si stanno avviando in merito.

Le ragioni per estendere al referto strutturato il tradizionale referto radiologico, inteso come un documento testuale contenente i risultati dell'atto medico radiologico, sono legate alle nuove metodologie di refertazione, in cui la gestione elettronica dei dati (sistemi RIS/PACS) fa perdere senso alla accoppiata testo/immagini (carta/pellicole), fondendole in oggetti della stessa natura (bit), in cui il testo tradizionale viene sostituito da un "ipertesto". Le nuove apparecchiature di diagnostica per immagini tendono inoltre a produrre sempre di più dati "volumetrici" difficilmente sintetizzabili in immagini tradizionali.

Quindi si può definire un "referto strutturato", inteso o come vero e proprio "oggetto" secondo lo standard DICOM, o secondo le indicazioni del CDA HL7, come un ipertesto in cui siano presenti:

- dati anagrafici del paziente;
- specifiche note anamnestiche;
- quesito clinico;
- descrizione della tecnica dell'indagine radiologica;
- descrizione dei reperti radiologici;
- diagnosi conclusiva;
- immagini direttamente prodotte dalla modalità e ritenute di particolare interesse da parte dello specialista radiologo o medico nucleare (a titolo esemplificativo si faccia riferimento al profilo di integrazione Key Images Note, IHE), in base alle quali lo specialista ha formulato la sua diagnosi;
- ogni tipo di elaborazione, ricostruzione, riformattazione operato dallo specialista radiologo o medico nucleare al fine di ottenere la diagnosi, ivi comprese le varie modificazioni di valori di finestra e livello abitualmente utilizzate per la definizione di strutture anatomiche differenti; di queste modifiche si deve tenere traccia nell'archivio digitale con rappresentazione dei differenti "stati di presentazione" (Presentation state; al proposito si veda il profilo di integrazione Consistent Presentation of Images, IHE).

Il referto strutturato dovrà seguire la stessa normativa cui sono sottoposti gli attuali referti testuali.

4.1.2 IMMAGINI

Come precedentemente descritto, ed analogamente a quanto accade per i referti, la modalità di gestione delle immagini diagnostiche (rappresentazioni iconografiche) è normata dal D. M. 14.2.97, 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." In tal caso la struttura erogante dovrà attenersi a specifiche modalità di gestione in grado di garantirne la disponibilità.

All'art. 4 comma 2. viene chiarito come la normativa si applichi in generale a qualsiasi immagine diagnostica, indipendentemente dalle modalità di acquisizione, prendendo così atto dell'evoluzione

tecnologica del settore che sta vivendo il passaggio da immagini acquisite con modalità analogiche ad immagini acquisite e gestite con formato digitale (diagnostica filmless): "La documentazione iconografica di cui al precedente comma può essere acquisita mediante pellicole radiografiche, supporti cartacei, supporti elettronici. Può essere detenuta in apposito locale predisposto, può essere microfilmata oppure può essere memorizzata in archivio elettronico, in conformità alla direttive dell'Agenzia per l'informatizzazione della pubblica amministrazione".

In questo documento saranno trattate esclusivamente le modalità di conservazione tramite archivi elettronici.

Una particolarità della diagnostica per immagini (digitali) è l'impiego del protocollo DICOM, ormai universalmente utilizzato per la gestione delle immagini diagnostiche. Secondo tale protocollo, le immagini prodotte sono associate ad informazioni quali dati anagrafici del paziente, modalità di acquisizione, modalità di visualizzazione dell'esame, etc.

Si è sentito il bisogno di specificare quando i dati acquisiti dalle varie apparecchiature per Diagnostica per immagini si aggregano per formare quella che comunemente in diagnostica per immagini si definisce immagine, in quanto i moderni sistemi producono dei "metadati", quali ad esempio le immagini "grezze". Si può tranquillamente affermare che, in diagnostica per immagini, l'immagine digitale è un insieme di dati iconografici, anagrafici e numerici rappresentati informaticamente secondo lo standard DICOM. Definiamo inoltre rappresentazione digitale di immagine diagnostica qualsiasi trasformazione dal formato DICOM ad altri formati quali ad esempio jpeg, gif, avi, etc.

Vanno quindi archiviate, e sottoposte successivamente al processo di conservazione a termini di legislazione vigente, tutte le immagini digitali in formato DICOM prodotte dalle apparecchiature di diagnostica per immagini della Struttura. Qualora alcune immagini fossero non in formato DICOM, si potrà procedere alla loro conservazione, prestando particolare attenzione al fatto che dovrà essere garantita almeno per un arco temporale di dieci anni la loro visualizzabilità dal responsabile della conservazione. Si ricorda che il Comitato DICOM sconsiglia vivamente archiviazioni di immagini in formati proprietari, sottolineando in particolare la scarsa stabilità e portabilità dei formati video.

4.1.3 TEMPI DI CONSERVAZIONE

La normativa di riferimento (D. Lgs n.230/95, D.M. 14.2.97, Circolare Ministero della Sanità n. 61/86 e DPR 14/02/1997) non differenzia in modo alcuno fra la documentazione analogica e quella digitale, ai fini della conservazione nel tempo. Alla luce di quanto sino ad ora esposto, vengono qui di seguito semplificati e riassunti i contenuti normativi riguardanti i previsti obblighi di mantenimento dei referti e delle immagini nel tempo, con indicazione dei soggetti responsabili dell'adempimento.

Referto¹⁷

REFERTO ANALOGICO		
	TEMPO	RESPONSABILE
PAZIENTE INTERNO	Illimitato	Direzione Sanitaria
PAZIENTE ESTERNO	Non previsto dalle norme nazionali Possibilità di previsione da parte di norme regionali	Paziente o UO di Diagnostica per Immagini

REFERTO INFORMATICO		
	TEMPO	RESPONSABILE
PAZIENTE INTERNO	Illimitato	Responsabile Conservazione Sostitutiva
PAZIENTE ESTERNO	Non previsto dalle norme nazionali Previsto da norme regionali Auspicabile illimitato	Paziente o Responsabile Conservazione Sostitutiva

Per motivi di completezza, qui sopra vengono illustrati lo scenario analogico e quello digitale, sia per il paziente esterno che per l'interno, per giungere poi a dimostrare che nella pratica dell'ambito digitale quest'ultima differenziazione normativa non ha più ragione di esistere.

Il testo del documento viene composto nel sistema informatico e validato digitalmente dal medico refertante. Nel caso del paziente interno il documento deve essere inserito nella cartella clinica di ricovero elettronica, qualora essa esista nella Struttura in tale formato; ove invece ci si trovi in regime di cartella clinica di ricovero analogica, il referto, nato e firmato digitalmente, deve essere rappresentato in copia su supporto analogico e così inserito in cartella. L'originale digitale del documento viene poi sottoposto a conservazione ottica secondo la normativa vigente.

L'art. 4 del D.M. 14.2.97 (Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230) prevede che "4.3. Qualunque sia la forma di archivio prescelta, la documentazione deve poter essere disponibile a richiesta per successive esigenze mediche. Tale disponibilità deve essere mantenuta per un periodo non inferiore a dieci anni per i documenti di cui al punto a) del precedente articolo [immagini] ed a tempo indeterminato per i documenti di cui al punto b) dello

¹⁷ Nell'odierna realtà sanitaria il referto analogico concernente un paziente interno prende vita su supporto cartaceo e viene sottoscritto autografamente in calce dal Medico Radiologo o Medico nucleare; in originale circola all'interno della Struttura, fisicamente accluso alle cartelle dei reparti di degenza; sempre in forma originale viene inserito in cartella clinica di ricovero al momento della sua chiusura e lì mantenuto a tempo indeterminato. Ciò viene espressamente previsto dalle vigenti norme e soprattutto dalla Circolare del Ministero della Sanità del 19 dicembre 1986, n. 61, la quale impone alle Strutture sanitarie pubbliche e private di conservare le medesime cartelle a cura della Direzione Sanitaria di presidio ospedaliero, unitamente ai referti, "illimitatamente poiché rappresentano un atto ufficiale indispensabile a garantire la certezza del diritto, oltre a costituire preziosa fonte documentaria per le ricerche di carattere storico sanitario". Inoltre secondo l'art.7 del D.P.R. n. 128/1969 "Il primario è responsabile della regolare compilazione delle cartelle cliniche, dei registri nosologici e della loro conservazione, fino alla consegna all'archivio centrale". L'art.5 del medesimo decreto asserisce che il Direttore Sanitario "vigila sull'archivio delle cartelle cliniche, ... rilascia agli aventi diritto, in base ai criteri stabiliti dall'amministrazione, copia delle cartelle cliniche".

Assai spesso copia di tale referto analogico viene mantenuta presso il Servizio di Diagnostica per immagini al mero scopo di consultazione clinica, senza che vi sia imposizione normativa alcuna in merito.

stesso articolo [referti], salvo termini diversi stabiliti con direttive del Ministro della sanità su conforme parere del Consiglio superiore di sanità”.

Quando quest'articolo parla di documentazione che “non venga consegnata al paziente” fa quindi pensare automaticamente a quella che riguarda il paziente ricoverato, o della quale si sceglie di trattenere nella Struttura un esemplare (originale o copia).

Immagini¹⁸

IMMAGINI ANALOGICHE		
	TEMPO	RESPONSABILE
PAZIENTE INTERNO	10 anni	UO di Diagnostica per Immagini o Paziente
PAZIENTE ESTERNO	Non previsto	Paziente

IMMAGINI DIGITALI		
	TEMPO	RESPONSABILE
PAZIENTE INTERNO	10 anni	Responsabile Conservazione Sostitutiva
PAZIENTE ESTERNO	Non previsto dalle norme nazionali Auspicabile 10 anni	Paziente o Responsabile Conservazione Sostitutiva

Anche qui valgono le considerazioni fatte più sopra per i referti, con l'aggiunta di una precisazione per quanto concerne l'iconografia analogica. Da una asettica lettura del DM 14.2.07, la documentazione iconografica analogica potrebbe essere consegnata al paziente anche nel caso in cui questi fosse un interno, poiché non vi è contenuto normativo alcuno che imponga il suo mantenimento nel tempo all'interno della Struttura che la ha prodotta. Una tale conclusione poteva per l'analogico convenire da un punto di vista economico e organizzativo, mancando anche particolari pericoli di modificazione dei dati delle pellicole con ripercussioni cliniche e medico-legali. Invece con il digitale tali motivazioni vengono automaticamente a cadere.

Qualora la Struttura scelga di mantenere nel tempo presso di sé l'iconografia prodotta da una propria U.O. di Diagnostica per Immagini anche per un paziente in regime di ricovero deve farlo a cura della U.O. e sotto la responsabilità del dirigente responsabile dell'U.O. stessa, del direttore di Struttura complessa o del Capo Dipartimento per almeno dieci anni.

La responsabilità dell'iconografia prodotta da una U.O. esterna alla Diagnostica per immagini è auspicabile che venga conservata con le medesime modalità previste per la Diagnostica per Immagini ma sotto la responsabilità del responsabile della U.O. che l'ha generata. Con la conservazione ottica, la responsabilità del mantenimento nel tempo va a ricadere invece sul Responsabile della Conservazione esplicitamente identificato. Sia per le immagini radiologiche analogiche sia per quelle digitali, il mantenimento nel tempo deve avvenire per un periodo non inferiore a dieci anni, così come imposto dal D.M. 14.2.97. Non vi è norma che imponga di consegnare al momento della dimissione alcunché al paziente interno, il quale, su espressa richiesta formale, può ottenere una copia della documentazione. Qualora l'iconografia sia stata prodotta per un paziente in regime ambulatoriale, il D.M. 14.2.87 non impone che la

¹⁸ Anche per la trattazione della documentazione iconografica aiuta mantenere la distinzione sul materiale prodotto per pazienti interni ed esterni e sulla natura analogica e digitale della stessa.

In merito alla conservazione delle immagini radiologiche, la Circolare Ministero della Sanità n. 61/86 afferma che “non rivestendo esse il carattere di atti ufficiali, si ritiene che sotto il profilo medico, medico-legale, amministrativo e scientifico possa essere sufficiente un periodo di venti anni”, oggi peraltro tramutato in dieci anni dalla normativa radiologica specifica.

documentazione venga mantenuta da parte della Struttura erogante la prestazione, bensì permette espressamente che essa possa essere interamente consegnata al paziente.

Referto strutturato

Sono state già definite le immagini radiologiche digitali come rappresentazioni informatiche di dati ottenuti da apparecchiature diagnostiche espresse in formato DICOM. E' fuori dallo scopo di questo documento entrare nel merito delle procedure di controllo della qualità dei sistemi in oggetto, affinché producano dei dati corretti e certificati. Tuttavia si sottolinea l'importanza di predisporre le necessarie misure minime affinché questi risultati siano garantiti.

Alla fine dell'acquisizione dei dati e dopo successive elaborazioni e trattamenti da parte del Medico specialista radiologo o medico nucleare o del Tecnico Sanitario di Radiologia Medica, il quale ultimo agisce comunque su delega dello specialista stesso, si ottiene una serie di file DICOM contenenti i risultati. Questi possono essere delle semplici immagini (Instances), dei risultati numerici (Evidence Documents) o dei filmati (Multiframe Instances). In ogni caso non si tratta di dati ottenuti da interpretazione diagnostica/clinica. Queste evidenze informatiche vengono trasferite sul sistema PACS (Picture Archiving and Communication System) ove vengono sottoposte a procedimento di archiviazione con l'apposizione di un riferimento univoco (normalmente generato dall'apparecchiatura stessa). Successivamente i dati archiviati vengono sottoposti a procedimento di conservazione sostitutiva, che può essere effettuato anche in un sistema informatico diverso dal PACS, secondo le modalità previste dalla legge e secondo le linee operative stilate dal Responsabile della Conservazione. Risulta evidente che dal momento dell'archiviazione (inserimento delle immagini nel sistema PACS) non è più possibile modificare i dati delle immagini, vista anche la non obbligatorietà alla sottoscrizione delle stesse. Il lasso di tempo che intercorre tra l'archiviazione e la conservazione è particolarmente delicato, in quanto alterazioni dei file risulterebbero difficilmente rilevabili, soprattutto in mancanza di predisposizione di misure idonee.

Si consiglia quindi di abbreviare al minimo questo intervallo temporale, al fine di garantire l'integrità dei dati immagine specie in riferimento alle immagini generate in urgenza. È consigliabile l'adozione di una procedura scritta e certificata in cui vengano descritti i passaggi in termini di modalità e tempi per rendere corretta la conservazione.

E' necessario apporre la marca temporale al referto in urgenza o se il referto viene consegnato subito al paziente o al medico richiedente quale garanzia assoluta per il radiologo ed il paziente.

In presenza di un referto strutturato contenente le immagini diagnostiche, viene definita una relazione indissolubile fra referto e immagini. Il referto strutturato deve essere conservato a tempo illimitato e le immagini digitali originarie, ovvero tutti i dati che hanno portato alla selezione delle immagini immesse nel referto strutturato, devono essere comunque conservate per un periodo di almeno 5 anni.

REFERTO STRUTTURATO		
	TEMPO	RESPONSABILE
PAZIENTE INTERNO	Illimitato	Responsabile Conservazione Sostitutiva
PAZIENTE ESTERNO	Auspicabile illimitato	paziente e Responsabile Conservazione Sostitutiva

Considerazioni

Il DM 14.2.97 dà, o meglio non nega, la possibilità di consegnare al paziente interno le immagini per lui prodotte e al paziente esterno sia le immagini sia il referto. Dalle Strutture pubbliche e private una tale libertà è stata comprensibilmente ben accolta e quasi ovunque concretizzata, poiché vista come una soluzione alle difficoltà organizzative di gestione anche logistica degli archivi analogici. Peraltro il D. Lgs n.187/00, all'art.3 co. 5 asserisce che "Il prescrittore e lo specialista, per evitare esposizioni non necessarie, si avvalgono delle informazioni acquisite o si assicurano di non essere in grado di procurarsi precedenti informazioni diagnostiche o documentazione medica pertinenti alla prevista esposizione", andando a ribadire ciò che veniva già asserito anche dall'art.1, co.1 del DM 14.2.97: "Il presente decreto stabilisce le disposizioni atte a permettere che i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche".

Talvolta, a livello regionale – come è accaduto nella Regione Lombardia – sono state emanate norme o diffuse raccomandazioni con cui veniva rivolto l'invito alle Strutture pubbliche e private di mantenere comunque nel tempo la documentazione presso di sé, per il timore di poter perdere troppo facilmente le importanti informazioni cliniche precedentemente generate.

Si ritiene di poter asserire che la differenziazione fra paziente esterno e paziente interno aveva ragioni di esistere nel mondo analogico riguardo alle diverse tipologie di documenti prodotti, con i loro diversi tempi e luoghi di mantenimento e con i differenti soggetti responsabili.

Gli aspetti clinici (rapidi reperimento e scambio delle informazioni), organizzativi (omogeneizzazione e standardizzazione dei workflow), medico-legali (i dati vengono conservati all'interno della Struttura, senza possibilità di manipolazione e modifica) e tecnologici (sicurezza e riservatezza nella gestione, garanzia di corretta riproducibilità dei dati anche dopo parecchi anni) fanno propendere per la scelta di una conservazione ottica di tutta la documentazione (iconografia, referti e referti strutturati) all'interno della Struttura produttrice della stessa, con i tempi che la normativa impone e riportati nelle tabelle. Ciò è ritenuto fondamentale ai fini del recupero delle informazioni, per garantire quindi migliori diagnosi, cura e assistenza.

E' noto a tutti come nella pratica sanitaria la documentazione analogica consegnata al paziente sia spesso malamente custodita e aleatoriamente recuperabile nel momento del bisogno. Appare quindi ancor più irrealizzabile lo scenario in cui sia il singolo cittadino a provvedere alla conservazione ottica secondo la normativa vigente. Ma ancor più, se dovessimo propendere per la totale consegna della documentazione digitale al paziente esterno, la Struttura erogante si potrebbe trovare in una vulnerabile posizione sotto gli aspetti medico-legali e probatori, poiché sprovvista delle informazioni cliniche adeguate, oggetto di un possibile contraddittorio.

Con la gestione digitale della documentazione radiologica, si riesce a rispondere pienamente a ciò che la normativa imponeva da un punto di vista clinico. Non solo, oggi per motivi di sicurezza, di garanzia di autenticità e immodificabilità dei dati, giuridici, medico-legali e probatori è indispensabile che il documento sia sottoposto a conservazione ottica, ottemperando pedissequamente ai contenuti normativi.

Si ritiene pertanto di poter raccomandare le Strutture produttrici della documentazione di provvedere esse alla gestione e anche alla conservazione della stessa (facendo eventualmente uso del diritto di delegare le attività e di affidare alcuni procedimenti ad altri soggetti, così come meglio chiarito nelle presenti linee guida). Poiché da un punto di vista organizzativo sembra essere assai più complicato e dispersivo gestire il doppio filone per documentazione consegnabile al paziente e documentazione da doversi mantenere nella Struttura, si consiglia di conservare informaticamente all'interno di quest'ultima tutta la documentazione radiologica in essa prodotta. Così si riuscirà anche rispondere in modo corretto a tutta la normativa vigente, sia di impronta clinica che tecnica.

4.1.4 CONTESTO DI UTILIZZO

Prima di procedere alla dematerializzazione dei documenti sanitari radiologici, è auspicabile l'implementazione di una serie di misure tecniche atte ad assicurare la correttezza delle procedure e il controllo dei processi, misure che sono già oggetto di norme (vedi legge sulla privacy) e che devono quindi essere predisposte per la tutela sia dei pazienti che degli operatori.

Si ritiene molto importante che la prima di queste misure sia l'adozione di una gestione sicura della sincronizzazione degli orologi di tutti i sistemi informativi coinvolti nella gestione dell'attività diagnostica. Ciò allo scopo di poter risalire con precisione, in caso di contenzioso, alla sequenza temporale degli eventi. Si rimanda al paragrafo della marcatura temporale l'analisi tecnologica di tali soluzioni, sottolineando però che i documenti radiologici oggetto di questa linea guida (referto ed immagini) contengono informazioni temporali che non ricadono nella problematica della marcatura temporale. Tali informazioni sono inserite nei vari documenti da firmare e/o conservare (ad esempio l'ora di esecuzione dell'esame radiologico viene inserita sia nel referto sia nelle immagini).

A tal proposito si consiglia di risolvere questo problema utilizzando le soluzioni proposte nel profilo IHE ITI Consistent Time (CT), rimarcando che questa soluzione non può essere invece adottata per la marcatura temporale dei referti e dei "supporti" di conservazione sostitutiva.

Si auspica inoltre che ogni aspetto della gestione venga monitorato da appositi meccanismi informatici, tali da poter definire con precisione, per ogni operazione effettuata sui sistemi, orario, tipo e autore di detta operazione. Ciò permette di risalire con precisione alla responsabilità individuale di comportamenti ed azioni di rilevanza non solo amministrativa, ma anche clinica e financo penale. Per la realizzazione tecnica di tali procedure, comunemente definite sistemi di audit, si confronti il profilo di integrazione Audit Trail and Node Authentication, IHE ITI.

Ultimo ma primo in ordine di importanza è l'aspetto relativo all'Identity Management del soggetto che utilizza a vario titolo il sistema informativo di Radiologia: con questo termine si intende la capacità del sistema di identificare un soggetto e di assegnare a questo un ruolo nel sistema informativo. Risulta evidente che questo dovrebbe essere un elemento non proprio del singolo sistema di radiologia, ma del sistema informativo ospedaliero, tuttavia per poter dematerializzare i documenti di radiodiagnostica, si deve tassativamente essere dotati di un tale accorgimento tecnologico. Si ricorda che questo è parte integrante delle norme di sicurezza minime ed idonee indicate nella normativa sulla privacy, e che tutti i trattamenti inerenti la dematerializzazione devono obbligatoriamente essere descritti nel Documento Programmatico della Sicurezza (DPS) come previsto dalla norma.

4.2 DOCUMENTAZIONE DI LABORATORIO DI ANALISI

4.2.1 REFERTO DI MEDICINA DI LABORATORIO

In medicina i risultati degli esami di laboratorio, con le opportune informazioni collegate (es. valori di riferimento, i commenti e le note interpretative, le indicazioni, i suggerimenti e le prescrizioni), costituiscono la risposta del laboratorio alla richiesta di esami o allo specifico quesito clinico.

La risposta del laboratorio è il messaggio con cui ordinariamente vengono trasmesse le informazioni prodotte nella fase analitica.

La Risposta del laboratorio può assumere diverse forme, dalle più semplici alle più complesse: Il risultato, ossia l'informazione prodotta in laboratorio e inserita in un archivio elettronico o riportata su supporto cartaceo; il foglio di risposta, un documento che riporta del tutto o in parte i risultati e gli altri elementi informativi che compongono la risposta; il Certificato, un foglio di risposta che viene autenticato in modo formale, per gli usi previsti dalle norme e dai regolamenti; il Referto.

Il risultato non può essere registrato o trasmesso senza le informazioni collegate che ne consentano la tracciabilità e l'individuazione di tutti gli operatori che hanno contribuito alla produzione e/o alla validazione e/o alla trasmissione del risultato stesso.

La validazione del risultato può avvenire in più fasi, ciascuna delle quali collegata nella registrazione con il risultato stesso.

La messa in circolazione di risultati è di per sé attestazione individuale di validità. La "firma" sul foglio di risposta può pertanto essere dilazionata nel tempo, se condizioni di urgenza o di immediata necessità del risultato determinano la necessità del rilascio dello stesso, a condizione che le procedure ed il flusso delle operazioni siano di per sé sufficienti a garantirne ragionevolmente l'autenticità e la tracciabilità.

Il referto di laboratorio è autenticato in modo formale attraverso la firma del Direttore o dei Dirigenti. La firma non attesta la validità del contenuto clinico del referto, che deriva invece dal controllo di tutti i processi di laboratorio che esitano nel risultato, nella sua consegna/trasmissione e nell'utilizzo dei dati per la gestione del Paziente. L'implementazione e il miglioramento continuo del controllo dell'intero processo rimangono comunque responsabilità del Direttore del laboratorio clinico.

La firma digitale può essere apposta con una, o più, delle tre modalità descritte nei capitoli 6.1.1, 6.1.2 e 6.1.3. (firma di un referto singolo previa visualizzazione e conferma, procedura semiautomatica per firmare un lotto di referti selezionati, procedura totalmente automatica di firma di referti pre-validati o comunque individuati in qualche modo) a seconda delle necessità organizzative del laboratorio.

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.

Il Referto di Medicina di Laboratorio è quindi una relazione scritta contenente prevalentemente, ma non esclusivamente, dati numerici; 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 (accesso ambulatoriale alla struttura del laboratorio, ecc.). Scopo del referto di Medicina di Laboratorio è quello di presentare i risultati in forma strutturata per facilitarne la corretta interpretazione, attraverso l'indicazione di informazioni quali gli intervalli di riferimento e i livelli decisionali, le specifiche di qualità, il calcolo di eventuali indici derivati, i commenti interpretativi, eventuali comunicazioni al Medico Curante e rapporti di consulenza.

Il referto di Medicina di Laboratorio contiene dati personali, riferiti al Paziente che ha effettuato gli esami di laboratorio richiesti dal Medico Curante, e dati sensibili, riferiti alla tipologia di esami richiesti con l'eventuale diagnosi presuntiva e ai relativi risultati convalidati ed espressi sotto forma numerica, letterale, grafica ecc., inclusi eventuali ulteriori informazioni e comunicazioni a completamento. Per la struttura e i contenuti del referto è consigliata la conformità allo Standard ISO 15189:2003.

4.2.2 TEMPI DI CONSERVAZIONE

Il referto di diagnostica di Laboratorio, totalmente rispondente ai requisiti illustrati nel paragrafo 4.1 del presente documento, deve soggiacere a quanto previsto da tutta la normativa più volte citata, che prevede il suo inserimento in cartella clinica di ricovero e la sua conservazione a tempo indeterminato, qualora riguardi un paziente interno (D.P.R. n. 128/1969, Circolare Ministero della Sanità n. 61/86).

In mancanza di puntuali previsioni normative in ambito laboratoristico, si ritiene invece di poter agire, utilizzando l'analogia legis e richiamando, per la trattazione del referto del paziente esterno,

la norma in ambito radiologico. Ciò con tutte le osservazioni riportate a corollario concernenti la differenziazione fra analogico e digitale.

Contrariamente, appare assai esplicito il D.P.C.M. 10.2.84, che al suo art. 9 prevede che il Direttore di Laboratorio sia responsabile "della conservazione per almeno un anno dei risultati diagnostici; delle relazioni diagnostiche e dei risultati di controllo di qualità; della buona conservazione dei preparati citologici ed istologici e delle occlusioni in paraffina per almeno cinque anni".

5 CLASSIFICAZIONE FASCICOLAZIONE SCARTO

5.1 CLASSIFICAZIONE E FASCICOLAZIONE

La Guida elaborata dal Comitato sugli archivi elettronici del Consiglio internazionale degli archivi, come pure il Codice dell'amministrazione digitale, entrato in vigore il 1 gennaio 2006, indicano come requisito fondamentale per lo svolgimento della funzione conservativa il mantenimento dell'autenticità, della leggibilità e intelligibilità nel tempo della produzione documentaria digitale.

L'integrità e l'identificazione univoca e certa dei documenti e delle relazioni tra di essi costituiscono gli elementi fondanti, indispensabili per garantire la reperibilità del documento ricercato e la certezza della sua validità giuridica e rispondenza al criterio di ricerca.

In altri termini, devono dunque essere conservati i dati che esprimono l'appartenenza del singolo documento al complesso archivistico (fascicolo, serie, fondo, ecc.) nel quale esso è organicamente e gerarchicamente inserito.

Esperienze in diversi settori (compreso quello della documentazione sanitaria) hanno posto in evidenza il fatto che l'informazione corretta deve necessariamente essere inserita in un corpus strutturato di documenti, pena l'incertezza sulla sua autenticità e validità, oltre che la perdita di elementi di informazione dati proprio dall'appartenenza ad una struttura.

Non a caso, nell'ambito delle indicazioni prodotte in sede di discussione sulla documentazione sanitaria, sono stati indicati – fra gli elementi fondamentali per l'archiviazione dei referti di laboratorio – dati come: identificazione del paziente, indirizzo, destinazione del referto; nome del medico richiedente, che di fatto rimandano a documentazione di tipo diverso, ma parte del medesimo fascicolo virtuale, come la richiesta di prestazione redatta dal medico curante.

“Occorre che i documenti restino identificabili in maniera univoca attraverso elementi e attributi ad essi relativi, quali:

- i dati di provenienza (organizzazione responsabile/autore);
- le componenti logiche interne;
- la registrazione univoca e con data certa che testimoni in modo incontrovertibile l'avvenuta acquisizione all'archivio;
- le relazioni documentarie che identificano le modalità di accumulazione, formazione e organizzazione stabile dell'archivio (classificazione e fascicolazione, accessibilità, tempi di conservazione, procedure di riversamento e di validazione e relative responsabilità). Si parla di **self sufficiency** del documento, il cui profilo dovrà contenere tutte le informazioni necessarie a garantire la sua conservazione in forma autentica e contestualizzata, mediante anche l'aggiunta di informazioni relative ai livelli superiori, cioè alla struttura archivistica alla quale lo stesso documento è destinato ad appartenere in maniera definitiva (nel passaggio all'archivio storico).”

Si tratta, dunque, di utilizzare strumenti e pratiche tradizionalmente adibite alla costruzione corretta degli archivi, quali i titolari, i massimari di scarto, i repertori dei fascicoli, i regolamenti: strumenti e pratiche che sono state, specialmente negli anni fra il 1978 e il 1999 (gli anni delle riforme della sanità) in gran parte trascurate, con danni in alcuni casi gravissimi per la conservazione permanente degli archivi. Il Decreto Legislativo 445/2000, Testo unico sulla documentazione amministrativa che raccoglie e sistematizza la normativa degli anni Novanta, ed i

provvedimenti attuativi richiamano l'obbligo delle pubbliche amministrazioni di dotarsi di questi strumenti, come pure del Manuale di gestione, nella costituzione e gestione di un archivio su supporto non convenzionale.

Conseguentemente, è indispensabile progettare la conservazione in ambiente digitale di un documento dal momento della sua acquisizione all'archivio che coincide con la sua assunzione al protocollo, o, per i documenti non soggetti a protocollazione con l'attribuzione di una classifica che identifica a quale segmento di procedura dell'Ente il documento stesso viene attribuito.

Per quanto riguarda le strutture sanitarie, va comunque ricordato che la loro attività, anche quando è una attività di cura, sanitaria o socio sanitaria, poggia su una complessa attività amministrativa che opera attraverso una molteplicità di procedure (di reclutamento del personale, di ispezione e autorizzazione, di acquisto, di appalto) che investono un settore cruciale, quale è quello della salute del cittadino. La gestione della documentazione, sia essa di carattere sanitario o amministrativo, va affrontata con strumenti omogenei. La corretta classificazione di un referto, di una documentazione iconografica, dell'esito di una analisi di laboratorio, all'interno di un fascicolo sulla cui conservazione esistono tempi certi, in un archivio, è uno degli elementi di garanzia che concorrono a dare certezza sull'autenticità di un documento, rispondendo allo stesso tempo, ad una esigenza emersa anch' essa nel corso del lavoro sulla documentazione sanitaria.

In particolare per i referti di laboratorio e per le immagini radiodiagnostiche, l'attento controllo sull'intero processo (**Total Testing Process**) di generazione e autenticazione, e la presenza di sistemi e di griglie di allarme che permettano di identificare, correggere e prevenire, in tempo reale, le anomalie, possono incidere sulla sicurezza e sulla precisione del risultato finale. Quindi la responsabilità vera non sta tanto nella validazione del risultato finale, ma anche, e principalmente, nella predisposizione, attivazione e continuo miglioramento di un Sistema Qualità nel quale le procedure ed i processi vengono pensati ed attuati per assicurare il migliore esito possibile in tutte le fasi operative ed, in ultimo, per permettere un appropriato utilizzo clinico delle informazioni.

In ognuno dei passaggi successivi, cioè nelle successive operazioni di inserimento del documento nel contesto di appartenenza (**fascicolo/dossier**), premessa per la formazione dell'unità archivistica che dovrà essere consegnata all'archivio di deposito e poi all'archivio storico, il documento deve essere accompagnato dalle informazioni di contesto (**profilo**) che si arricchiscono di nuovi elementi, fino al passaggio nel luogo (virtuale o fisico) di conservazione permanente.

Si ottiene in tal modo una perfetta realizzazione del principio dell'ininterrotta custodia, documentato dalla continuità dei passaggi, delle operazioni che i documenti hanno subito in ciascuno, delle responsabilità collegate, in una parola da quella che gli archivisti definiscono "traditio" della fonte o anche storia archivistica: che è poi documentazione della validità legale della fonte documentale e, per altro aspetto, della sua affidabilità per la storia.

Per scendere su un terreno pratico, sarà indispensabile, ad esempio, in ambito radiologico, che, quando le "evidenze informatiche vengono trasferite sul sistema PACS (Picture Archiving and Communication System) - ove vengono sottoposte a procedimento di archiviazione con l'apposizione di un riferimento univoco (normalmente generato dall'apparecchiatura stessa)" (cfr. in questo documento il punto 4.1.3.) - la formulazione di tale riferimento univoco sia strutturata in maniera tale da ricondurre in modo esclusivo a quel paziente, a quel contesto clinico, ovvero a quella specifica richiesta nella storia del paziente, e ad un solo ed unico referto al quale l'immagine radiologica, in attesa del referto strutturato, sarà connessa da una corretta classificazione. Altrettanto vale per il momento dell'archiviazione del referto di laboratorio (cfr.6.4.).

Qualora ciò non sia già avvenuto, è indispensabile, dunque, per ciascun Ente, compiere gli atti preliminari all'applicazione del D.P.R. 445/2000 e, in particolare, l'individuazione delle Aree Organizzative Omogenee, l'istituzione di un Protocollo generale, l'istituzione del Servizio archivistico e l'individuazione formale del suo responsabile. E' necessario riorganizzare i flussi documentali, legandoli al censimento dei procedimenti amministrativi, e individuare i responsabili dei singoli procedimenti, predisporre e introdurre l'uso di un **Titolario** di classificazione dei documenti, che

consenta di garantirne l'univoca identificazione nel tempo, attraverso una corretta protocollazione, classificazione e fascicolazione.

L'Amministrazione archivistica del Ministero per i beni e le attività culturali, alla quale sono conferiti – ai sensi del D.Lgs.42/2004, art. 10 e del regolamento di organizzazione del Ministero per i beni e le attività culturali (DPR 173/04) – poteri di vigilanza e controllo sugli archivi pubblici, e funzioni di sostegno alle pubbliche amministrazioni nella fase di progettazione e creazione del proprio sistema archivistico, allo scopo di assicurarne la conservazione nel tempo, ha predisposto modelli di Titolario di classificazione, Prontuario di scarto, Regolamento d'archivio e Manuale di gestione, specificamente destinati alle Aziende sanitarie locali, già utilizzati in diverse strutture. Si tratta – nel caso del Titolario – di uno strumento articolato per funzioni, attribuite dalla normativa vigente alle Aziende e, quindi, applicabile indipendentemente dalla struttura organizzativa che svolge quelle funzioni, la quale, come è noto, è autonomamente stabilita da ciascuna Azienda e, dunque, diversa da Regione a Regione. Questi documenti possono essere scaricati dall'indirizzo: http://www.archivi.beniculturali.it/divisione_III/schola_salernitana.html.

5.2 SCARTO DEI DOCUMENTI

Si ritiene utile rammentare la procedura prevista dalla vigente normativa per lo scarto della documentazione appartenente agli archivi degli Enti pubblici (Codice dei beni culturali e del paesaggio, Decreto legislativo 22 gennaio 2004, n.42, art.21). Tale operazione è soggetta all'autorizzazione della Soprintendenza archivistica competente per territorio.

Lo scarto di documenti d'archivio può essere proposto quando si verificano due condizioni: l'esaurimento dell'utilità giuridico-amministrativa dei documenti e la mancanza di apprezzabile interesse come fonte storica.

Allo scopo di favorire tale selezione, per ognuno dei settori della pubblica amministrazione vengono predisposti (in accordo con l'Amministrazione archivistica) degli elenchi di tipologie documentarie "tipiche", altrimenti detti "massimari" di conservazione e scarto. Il **Prontuario di scarto per le Aziende sanitarie** locali elaborato nell'ambito del progetto "Schola salernitana" è disponibile all'indirizzo http://www.archivi.beniculturali.it/divisione_III/schola_salernitana.html.

Ogni proposta di scarto deve essere adeguatamente motivata indicando per ogni serie perché si ritiene sia venuto meno l'interesse giuridico-amministrativo e perché non si ravvisi la necessità di una conservazione per scopi storici. Tale motivazione deve essere espressa con la massima chiarezza in particolare nei casi di documenti che non compaiono nei massimari di scarto. Una motivazione adeguata può essere quella che si conservano illimitatamente altri documenti (da indicare espressamente) comprensivi dei medesimi dati contenuti nei documenti che si propongono per lo scarto.

Poiché oggetto di scarto non sono i singoli documenti ma le loro aggregazioni (serie tipologicamente omogenee oppure fascicoli disomogenei al loro interno ma uniformi quanto alla modalità della loro formazione come gli acquisti di beni mobili), è opportuno che l'organizzazione dell'archivio corrente tenga conto della futura necessità di conservare solo parte della documentazione prodotta, e quindi preveda, ad esempio, la creazione di sottofascicoli facilmente individuabili ed estraibili in occasione dello scarto, mentre si conserva la parte fondamentale del fascicolo medesimo.

Procedura di scarto: la procedura di scarto, per l'archivio di un ente pubblico, si svolge in quattro fasi:

- 1 Il dirigente dell'Ente trasmette alla Soprintendenza archivistica, con lettera protocollata, l'elenco in due copie, entrambe da lui firmate, delle tipologie archivistiche che si ritiene non abbiano più utilità amministrativa.

- 2 La Soprintendenza archivistica restituisce una copia dell'elenco, vistato con approvazione totale o parziale.
- 3 Nel caso di documentazione cartacea, l'Ente provvede a cedere i documenti da scartare alla Croce Rossa Italiana, o, in caso di indisponibilità della medesima, a organizzazioni, anche di volontariato (ex DPR 8/1/2001 n.37, art. 8), che ne garantiscano la distruzione (tramite triturazione, incenerimento, macerazione a fine di riciclare il materiale).
- 4 Infine l'Ente trasmette alla Soprintendenza archivistica copia del verbale attestante le modalità dell'avvenuta distruzione.

6 AUTENTICAZIONE DOCUMENTI

6.1 PREMessa – MODALITA' DI SOTTOSCRIZIONE DIGITALE

Le diverse tipologie di documenti oggetto della trattazione di queste linee guida corrispondono a diverse esigenze procedurali a tutti i livelli, incluso il contesto in cui la firma digitale viene apposta. In questa sezione si propone un'analisi dei contesti più tipici, giustificandone la conformità alla normativa in vigore.

A questo riguardo il riferimento è fornito dal Dlgs 82/2005, in particolare l'art. 35 "Dispositivi sicuri e procedure per la generazione delle firme". In particolare i commi 2 e 3 di tale articolo riuniscono l'insieme procedure-dispositivi (riconoscibili come hardware e software coinvolti nelle operazioni) prescrivendo alcuni vincoli piuttosto precisi, diversi per il caso generale e per le firme "apposte con procedura automatica".

A fini di chiarezza si ritiene utile analizzare, in questo contesto, tre diversi casi riconducibili ai due commi citati. Si vedano le successive sezioni.

6.1.1 FIRMA SINGOLA APPOSTA IN CONTESTO INTERATTIVO

La firma singola apposta in contesto interattivo è il caso della firma digitale che l'utente appone ad uno specifico referto, per esempio in radiologia, redatto in modo manuale o quasi manuale. 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.

Il comma 2 del citato art. 35 recita "... I documenti informatici devono essere presentati al titolare, prima dell'apposizione della firma, chiaramente e senza ambiguità, e si deve richiedere conferma della volontà di generare la firma ...".

Il soggetto di questa presentazione è sempre l'insieme di dispositivi e procedure, quindi in definitiva il sistema di refertazione + il componente software che presiede alla generazione della firma digitale + il dispositivo di firma vero e proprio (smartcard o simile) + il software di interfaccia (driver, PKCS#11) che consente l'interazione tra questi componenti.

Le modalità con cui avviene la presentazione non sono prescritte in modo rigido. È tuttavia importante che dal momento in cui l'utente avvia la procedura di firma (agendo, per esempio, sul bottone [Firma referto]) e il momento in cui il sistema presenta la prescritta richiesta di conferma, l'utente abbia la possibilità di visualizzare il contenuto del documento in modo immediato ed intuitivo, oppure che il sistema apra spontaneamente una finestra di visualizzazione.

La presentazione chiara e senza ambiguità ha delle implicazioni sulla scelta del formato di rappresentazione dei referti (argomento che nel complesso esula dagli scopi del presente documento), inducendo ad evitare formati in cui il contenuto informativo del documento siano separati dal modello di presentazione, ove quest'ultimo non sia a sua volta coperto dalla firma.

La richiesta di conferma in se stessa è una finestra contenente una chiara dicitura del significato dell'operazione con almeno un bottone di conferma ed uno di annullamento dell'operazione.

6.1.2 FIRMA SEMIAUTOMATICA DI LOTTI DI DOCUMENTI

La firma semiautomatica di lotti di documenti è il caso di un utente che deve firmare un insieme di referti già preparati in precedenza. Si pensi all'ordine di grandezza, tipicamente, delle decine o centinaia di documenti.

L'utente ha 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 esaminarlo nel contenuto; nei contesti ove ciò sia applicabile si può anche pensare che l'utente possa editare/modificare i documenti, il tutto dovrà essere eseguito rispettando tutte le fasi previste dal flusso operativo, compresa l'attività di validazione preliminare alla firma del referto, sia essa manuale o assistita.

L'utente potrebbe selezionare un sottoinsieme di questa lista ed avviare una procedura di firma digitale dei documenti così selezionati, che verrebbero quindi firmati automaticamente senza ulteriori interruzioni (salvo la richiesta di conferma per l'avvio della procedura di firma effettiva) usando il suo dispositivo di firma.

Poiché l'utente, prima di confermare l'effettivo avvio della sessione di firma, ha la piena possibilità di visionare i contenuti dei documenti si ricade nel caso del comma 2: il sistema di fatto presenta chiaramente i documenti e consente un esame approfondito sotto il pieno controllo dell'utente.

6.1.3 FIRME APPOSTE CON PROCEDURA AUTOMATICA

Questa modalità, corrispondente al comma 3 dell'art. 35, descrive il caso in cui un sistema di firma automatica venga avviato per processare in modo automatico un flusso di documenti – provenienti da altri sottosistemi – che il titolare della chiave privata (quindi del dispositivo di firma) non ha modo di controllare puntualmente.

Si tratta di una situazione pienamente legittima (un server di marcatura temporale, per esempio, opera in questo modo), ma che va gestita in modo corretto.

Il primo requisito dettato dalla normativa, è che l'attivazione della procedura sia chiaramente riconducibile alla volontà del sottoscrittore, ossia il titolare del dispositivo. La procedura deve quindi 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 smartcard, più probabilmente farà uso di dispositivi di tipo HSM).

Il secondo requisito è che l'adozione della procedura automatica sia resa palese in relazione al singolo documento sottoscritto; questo può essere realizzato in molti modi, tra cui un'esplicita dicitura all'interno di ogni documento firmato. Tuttavia è sufficiente che venga prodotto, a priori, un documento del sistema di qualità o una delibera che attesti l'esistenza della procedura automatica, indicando quali tipologie di documenti verranno processati in tal modo, specificando i dettagli del certificato che viene impiegato dalla procedura.

Un ulteriore vincolo si trova nelle regole tecniche (DPCM 13/01/2004), art. 4 comma 2: "Se il titolare appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso".

Questa prescrizione ha lo scopo di rendere identificabili i documenti firmati con tale procedura e spiega la raccomandazione di indicare – nella documentazione della procedura – gli estremi del certificato.

6.2 PREMESSA – CICLO DI VITA DEI REFERTI

Tra le diverse tipologie di documenti oggetto della dematerializzazione i referti – sia quelli radiologici che quelli di laboratorio – devono certamente essere corredati di sottoscrizione digitale. Questa natura di documenti informatici sottoscritti implica in generale la necessità di una gestione completa, dal punto di vista tecnico-giuridico, del relativo “ciclo di vita”: gli adempimenti non possono infatti esaurirsi, a norma di legge, con la mera apposizione di una firma digitale seguita da una qualche forma di archiviazione.

In questa sezione ci si propone di illustrare, a titolo di introduzione, le fasi salienti di questo ciclo di vita. Esulano da questo contesto considerazioni di carattere approfonditamente tecnico come pure di carattere clinico-procedurale.

Vale una premessa importante: la redazione o composizione del referto dovrebbe essere considerata come “esterna” al ciclo di vita del documento informatico, che per le nostre esigenze deve essere “sottoscritto con firma elettronica qualificata” o con “firma digitale” (Dlgs 82/2005, art. 20 comma 2) e quindi inizia ad esistere all'atto della sottoscrizione.

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 reperti, passando anche per strumenti di dettatura vocale in grado di costruire un referto completo partendo da poche espressioni verbali enunciate dinanzi ad un microfono.

Quali che siano le fasi che conducono alla costruzione del contenuto di un referto, quale che sia la distribuzione temporale di queste fasi, quale che sia la forma informatica finale del referto stesso dobbiamo considerare l'apposizione della firma digitale come l'evento che trasforma una mera sequenza di bit in un vero e proprio “documento informatico”.

Poiché l'atto della sottoscrizione è comunque compiuto da una persona fisica, sia pure nel quadro di una procedura automatica o semiautomatica, l'identificazione di questa persona da parte del sistema e la conseguente autorizzazione ad apporre la propria firma ad una certa tipologia di referti è a sua volta un evento preliminare di grande importanza.

La sequenza di passi significativi può dunque essere riassunta come segue nei prossimi paragrafi.

6.2.1 SIGN-ON DEL SOTTOSCRITTORE

Tramite questa operazione, che per l'utente consiste nel fornire al sistema le proprie credenziali di accesso, il soggetto che dovrà firmare il referto ottiene tale accesso.

L'operazione di sign-on deve ovviamente essere annotata in modo automatico nel registro del sistema, corredata da una accurata informazione su data ed ora dell'evento e dai riferimenti della stazione di lavoro su cui avviene l'accesso.

Particolarmente interessante, per un sistema di gestione di documenti informatici sottoscritti, appare l'adozione di procedure di strong-authentication basate su smartcard – piuttosto che su semplici username/password – contenenti sia la chiave di firma digitale che quella di autenticazione, i cui certificati siano emessi dallo stesso Certificatore. In tal caso il sistema potrebbe contare su un obiettivo maggior livello di certezza sull'effettiva identità dell'utente della stazione di lavoro; ma, soprattutto, lo stesso sistema potrebbe verificare in questa fase lo stato di validità dei certificati, rifiutando l'accesso all'utente il cui certificato venga trovato non valido.

6.2.2 SOTTOSCRIZIONE

L'utente, nel quadro del normale utilizzo del sistema a sua disposizione, attiva la funzione di apposizione della propria firma digitale ad uno o più referti.

Le modalità operative con cui questo può avvenire (firma di un referto singolo previa visualizzazione e conferma, procedura semiautomatica per firmare un lotto di referti selezionati, procedura totalmente automatica di firma di referti pre-validati o comunque individuati in qualche modo) sono approfondite nella sez. 6.1, ma in ogni caso il singolo referto riceve lo status di documento informatico sottoscritto al momento in cui gli viene apposta una firma digitale.

I componenti del sistema che gestiscono questa fase dovrebbero verificare lo stato di validità del certificato del sottoscrittore prima di consentire la generazione della firma, indipendentemente dal fatto che le misure attuate in fase di sign-on possano escludere, con buona approssimazione, che un certificato non valido venga utilizzato per la sottoscrizione.

Come vedremo la successiva fase di consolidamento avrà lo scopo di collegare l'esistenza del documento firmato ad un istante di tempo certo e dimostrabile; tuttavia è opportuno che il sistema utilizzi anche altri due strumenti di registrazione temporale, che pur non avendo la caratteristica di opponibilità ai terzi possono costituire elementi a sostegno del corretto svolgimento delle procedure.

Gli strumenti utilizzabili a questo scopo sono:

- annotazione nel registro degli eventi, meglio se corredata di informazioni univoche come l'impronta del documento, della firma, del certificato utilizzato;
- attivazione dell'attributo signing-time a livello della firma digitale;

Il signing-time rappresenta semplicemente il riferimento temporale dell'istante una in cui viene calcolata la firma. E peraltro un attributo coperto dalla firma digitale, quindi protetto da successive alterazioni al pari del contenuto del documento.

A patto che l'istante codificato nel signing-time venga derivato dall'orologio globale del sistema esso coinciderà con il tempo della registrazione dell'evento, ma ha il vantaggio di essere ricavabile direttamente dal documento.

6.2.3 CONSOLIDAMENTO

È quanto mai evidente l'importanza che il referto sottoscritto abbia un pieno e duraturo valore probatorio. Come si approfondirà nella sez. 7 questo risultato si raggiunge comprovando che il referto, al momento della firma (o comunque al momento in cui il referto viene accettato dal sistema), era stato sottoscritto con un certificato in pieno corso di validità.

Il consolidamento si ottiene verificando con la massima accuratezza la validità del certificato ed associando al documento in questione una marca temporale (che è, secondo la normativa attualmente in vigore, il riferimento temporale opponibile ai terzi più adatto all'associazione con un singolo documento o, addirittura, ad una singola firma) ottenuta da un fornitore accreditato del servizio di marcatura temporale.

Si può osservare, rivedendo le fasi descritte in precedenza, che la verifica del certificato era verosimilmente già stata effettuata sia in fase di sign-on che nelle fasi immediatamente precedenti la sottoscrizione. Senza entrare in eccessivi dettagli tecnici e senza avanzare ipotesi sulle possibilità, per un malintenzionato, di aggirare i controlli preliminari, si ritiene di sottolineare la validità generale del principio della ridondanza delle misure di sicurezza, soprattutto in ambienti ad elevata criticità come quello sanitario ed in contesti applicativi eterogenei, ove sono integrate soluzioni di diversi produttori.

NOTA: la situazione ottimale è quella in cui l'istante della sottoscrizione (testimoniato dal signing-time e dalla registrazione dell'evento) e l'istante del consolidamento (testimoniato dalla marca temporale) sono estremamente ravvicinati, al limite della coincidenza.

Qualora l'architettura dei sistemi (code, bilanciamento del carico, capacità del servizio di marcatura temporale, ...) renda inevitabile un ritardo tra questi due eventi, sussisterebbe un problema di ambiguità solo nel caso di una revoca o sospensione di certificato che si verificasse proprio entro tale intervallo. Per questa ragione è opportuno contenere tale ritardo tecnico a livelli accettabili.

6.2.4 CONSERVAZIONE SOSTITUTIVA

In base al Dlgs 82/2005, art. 23, comma 7 " ... gli obblighi di conservazione e di esibizione di documenti previsti dalla legislazione vigente si intendono soddisfatti ... a mezzo di documenti informatici se le procedure utilizzate sono conformi alle regole tecniche dettate ai sensi dell'art. 71 ..." dello stesso Dlgs. Cioè, ad oggi delle Deliberazione CNIPA 11/2004.

Oltre agli adempimenti di tipo formale (a partire dalla nomina del Responsabile della Conservazione) e gestionale previsti da tale Deliberazione, sul piano pratico le regole tecniche prescrivono che i referti vengano raggruppati in insiemi – possiamo definirli "volumi" – e che, più o meno periodicamente, a tali insiemi venga applicata una procedura operativa specifica. Tale procedura – il processo di conservazione, appunto – consiste nella costruzione di un "file di impronte" che contiene i valori hash di tutti i documenti appartenenti al volume, quindi nella sottoscrizione digitale di questo file da parte del Responsabile della Conservazione e la contestuale associazione di un riferimento temporale opponibile ai terzi.

La normativa prescrive inoltre significative responsabilità in ordine alla gestione di questi volumi conservati (copie di sicurezza, garanzie di reperibilità e leggibilità, tracciabilità, ecc.).

È degno di nota che le regole tecniche non prescrivono alcun intervallo massimo predefinito tra la generazione di un documento informatico e il completamento del relativo processo di conservazione. Poiché i referti, per effetto del consolidamento, sono già coperti da marche temporali individuali, non sussiste alcuna particolare criticità, salvo il fatto che nell'intervallo tra la marcatura temporale del documento ed il perfezionamento del processo in questione non si può dire che il documento sia "conservato".

6.2.5 CONSIDERAZIONI

Possiamo fare alcune considerazioni qualitative sull'andamento del tempo tra le diverse fasi:

- Il tempo T1, che trascorre tra l'istante del sign-on e quello di generazione di una firma, è altamente variabile e può essere dell'ordine delle ore. L'effetto negativo dell'allungarsi di questo tempo può essere il verificarsi di una sospensione o revoca di un certificato durante questa fase, il che potrebbe significare che un utente sta realmente usando una falsa identità. Oltre agli accorgimenti possibili per ovviare a questo problema (sign-off forzato in caso di inattività, tempo massimo di lgon, ciclica verifica dello stato dei certificati ed eventuale forzata disconnessione) si evidenzia quanto sia opportuno rieseguire la verifica dello stato al momento della firma e poi di nuovo al momento del consolidamento.
- Il tempo T2, che trascorre tra l'istante di generazione della firma e quello della marca temporale apposta in fase di consolidamento, dovrebbe essere breve (secondi o minuti), dipendendo solo dal tempo tecnico impiegato dal sistema per memorizzare il referto firmato e poi per interagire con il servizio di marcatura temporale, considerati anche i vincoli del carico delle code lavori. L'effetto negativo dell'allungarsi di questo tempo può essere il verificarsi di una sospensione o revoca di un certificato durante questa fase, che implicherebbe uno stato di "ambiguità probatoria": il documento era stato firmato quando il certificato era valido, ma la marca temporale non ci permette di provarlo in modo immediato, pur esistendo elementi valutabili (registro degli eventi, signing-time) a supporto della validità. Ne discende l'opportunità di ottimizzare le prestazioni del sistema in modo da minimizzare il ritardo T2.
- Il tempo T3, che trascorre tra l'istante corrispondente alla marca temporale e quello della finalizzazione del processo di conservazione non è critico, perché la marca temporale mette al

sicuro la valenza probatoria del referto anche in caso di sospensioni o revoche (ma anche scadenza naturale) del certificato che avvenissero durante T3. La ragione di osservare comunque tempi ragionevolmente brevi (dell'ordine di alcuni giorni o alcune settimane) consiste nell'opportunità di evitare lunghi periodi di latenza dei documenti informatici in uno stato di "non conservato".

6.3 FIRMA DIGITALE DEL REFERTO DI MEDICINA DI LABORATORIO

La firma digitale dei referti di laboratorio è un atto di autenticazione di dati di laboratorio in formato elettronico, strutturati in un referto completo elettronico legalmente valido e riconosciuto, conforme allo standard ISO 15189:2003.

Il referto di laboratorio firmato elettronicamente permette l'abolizione di qualsiasi formato cartaceo firmato a penna, garantisce la provenienza delle dichiarazioni di chi l'ha sottoscritto e permette l'invio telematico in sicurezza del referto ai destinatari, sostituendo i mezzi tradizionali di invio e consegna (fax, buste chiuse, raccoglitori di carta, ecc.).

La firma digitale non modifica né condiziona le varie fasi del processo di generazione del referto di laboratorio finale.

La firma digitale non deve ritardare o impedire la tempestiva comunicazione di dati di laboratorio di rilievo clinico per la cura e la salute del Paziente in formato elettronico o cartaceo non autenticati. A tale scopo le diverse modalità di firma espresse nel capitolo 6.1 possono essere applicate alternativamente o contemporaneamente.

La firma digitale dei referti di laboratorio identifica la responsabilità del Direttore del Servizio e/o di coloro che possiedono i requisiti previsti per legge per ottenere la delega.

Tutti i processi susseguenti alla firma digitale del referto di laboratorio (digitalizzazione, criptazione, decriptazione, trasformazione in formati standard, ecc.) finalizzati alla comunicazione, trasmissione e riproduzione in sicurezza e riservatezza, devono garantire l'assoluta immutabilità non solo dei dati contenuti, ma anche dei formati e degli eventuali testi o immagini o riproduzioni grafiche, incluse nel referto.

La firma digitale dei referti di laboratorio garantisce l'autenticità del documento e deve pertanto poter essere rintracciabile nel formato elettronico, fatti salvi i dispositivi che ne tutelano la sicurezza di accesso e la confidenzialità dei contenuti.

Il referto di laboratorio firmato elettronicamente con firma digitale deve rientrare nel novero della documentazione clinica che concorre a costituire la cartella clinica elettronica del Paziente.

6.4 FIRMA DIGITALE DEI REFERTI DI DIAGNOSTICA PER IMMAGINI

Abbiamo già definito in un precedente paragrafo il referto radiologico, in particolare introducendo il concetto di referto strutturato. Come già discusso, il referto radiologico va sottoscritto mediante firma elettronica qualificata. Nel caso il referto sia privo dei riferimenti alle immagini, si provvederà a firmare un file che dovrà essere in formato pdf, odt (Open Document format) oppure CDA (Clinical Document Architecture HL7), in quanto questi tre formati sono considerati efficacemente scambiabili dai vari organismi standardizzatori (HI7, DICOM, OASIS, IHE nel profilo XDS). Nel caso invece di referto strutturato si provvederà a firmare un file in formato DICOM SR o HL7 CDA

versione 2. Dal momento della firma inizierà il suo ciclo di vita di documento informatico e quindi dovrà essere istantaneamente archiviato con l'apposizione di un identificativo univoco e successivamente sottoposto al procedimento di conservazione sostitutiva. Sarà compito del Responsabile della Conservazione definire sia i tempi che intercorreranno fra l'archiviazione e la conservazione sostitutiva sia le misure minime e idonee a garantire l'integrità e la sicurezza del documento firmato.

6.5 AUTENTICAZIONE DELLE IMMAGINI

Come descritto al paragrafo 5.1.2. le immagini, intese come oggetti DICOM, sono associate ad altre informazioni che il medico specialista radiologo o medico nucleare refertante utilizza nell'ambito della propria attività e che possono essere modificate prima o dopo la fase di refertazione.

Il problema dell'autenticazione delle immagini, che riguarda quindi tutto il processo di produzione, refertazione, archiviazione, può essere suddiviso in due macro argomenti:

1. Qualità del dato
2. Corretta assegnazione

Qualità del dato

Per qualità del dato, in questo contesto, si intende la verifica della correttezza e completezza delle informazioni associate all'immagine (metadati), indispensabile prima della conservazione legale. Questa verifica, fatta esaminando il contenuto dei relativi tag DICOM, dovrebbe riguardare le principali informazioni quali: accession number, patient name, modality, study description, ecc. Il controllo dovrebbe essere previsto, oltre che sulle informazioni indirizzate all'archivio legale, anche sulle immagini da refertare, al fine di garantirne la coerenza. Questa attività può essere considerata parte di un più vasto sistema di certificazione complessiva della qualità erogata, in analogia, ad esempio, a quanto richiesto per le apparecchiature diagnostiche, per i rivelatori e per i sistemi di visualizzazione, dal D. Lgs n. 187/2000.

Corretta assegnazione

Può accadere che le immagini vengano erroneamente assegnate a persone diverse rispetto a quelle che si sono sottoposte all'indagine diagnostica. In tali casi debbono essere messe in atto procedure di riassegnazione la cui correttezza deve essere verificata sia in termini di efficacia che di impatto sull'archivio legale. La politica della riassegnazione dovrebbe essere definita dal responsabile della gestione del RIS e PACS ed accettata dal responsabile clinico.

Dopo l'eventuale modifica dei metadati e la corretta assegnazione dell'indagine, le immagini possono essere considerate archiviate (vedi Delibera CNIPA 19/02/04) ossia in fase di pre-conservazione sostitutiva e quindi immodificabili.

7 CONSOLIDAMENTO DEI DOCUMENTI

In questo contesto ci si riferisce unicamente a documenti corredati da una o più firme digitali o firme elettroniche qualificate.

Il valore probatorio di un documento informatico sottoscritto è dunque condizionato al fatto che al momento della sottoscrizione si utilizzi un certificato qualificato in corso di validità, ovvero non revocato o sospeso (D. Lgs. 82/2005, art. 24).

È appena il caso di rilevare che l'importanza di disporre di documenti informatici sottoscritti sulla cui validità vi sia certezza è particolarmente critica in ambito sanitario, in considerazione del fatto che sugli atti medici rappresentati dai documenti in questione si basano, in generale, attività da cui dipendono letteralmente la vita e la salute dei pazienti.

La semplicità del concetto di certificato in corso di validità sottende l'importanza del tempo: un certificato ha per definizione una scadenza naturale (impostata dal Certificatore al momento dell'emissione) dopo la quale nessuna firma deve essere generata con la chiave privata associata ad un certificato scaduto.

Ma il problema più insidioso consiste nella possibilità, in generale, che un certificato perda la propria validità in anticipo rispetto alla sua scadenza naturale, per effetto di un provvedimento di sospensione o revoca. Nelle attuali infrastrutture questi sono eventi imprevedibili ed asincroni (nel senso che possono capitare in un istante di tempo qualunque, non allineato ad alcuna operazione programmata, né da parte dell'utilizzatore dei sistemi, né da parte dei Certificatori) che corrispondono a strumenti (le procedure di Sospensione o Revoca, appunto) peraltro indispensabili per gestire tipiche situazioni di smarrimento, furto, danneggiamento del dispositivo di firma.

La possibilità, assolutamente verosimile, che un certificato venga sospeso/revocato poco prima della generazione di una firma (invalidando la firma stessa) o poco dopo tale generazione (in linea di principio senza influire sulla validità della firma) obbliga a porre in atto adeguate misure per accertare – nell'immediato ed a posteriori – se una specifica firma sia valida oppure no.

Due gli ordini di problemi:

- accertare, a distanza di tempo (per esempio in sede di contenzioso), se la firma fosse valida al momento della sottoscrizione; questo appare relativamente semplice se è possibile collocare con precisione ed attendibilità la "nascita" del documento firmato: sarà certamente possibile ottenere dal Certificatore informazioni precise ed attendibili sulla storia del certificato in relazione ad eventuali provvedimenti di sospensione o revoca;
- accertare, nell'immediatezza della sottoscrizione, se effettivamente il certificato è in corso di validità, al fine di poter utilizzare il documento (si pensi ad un referto) per le attività cliniche; questo risultato appare meno scontato, dipendendo dalla possibilità di disporre in modo immediato e puntuale delle informazioni sullo stato di validità di un certificato.

In ogni caso si parla di "consolidamento" della valenza probatoria se un documento firmato viene arricchito di elementi di prova atti a dimostrarne la validità: una prova dell'esistenza del documento in un certo istante di tempo e la prova del fatto che il certificato del sottoscrittore in quell'istante fosse valido.

È forse il caso di osservare che queste considerazioni costituiscono l'oggetto di una proposta di standard europeo sviluppata dal CEN (Comité Européenn de Normalisation) nell'ambito EESSI (European Electronic Signature Standardization Initiative), su mandato della Commissione Europea a seguito della Direttiva 1999/93/CE relativa ad "un quadro comunitario per le firme elettroniche". Questo documento (CWA 14171 – "General guidelines for electronic signature verification") è un riferimento estremamente autorevole sulle corrette modalità per la verifica delle firme digitali e sugli strumenti da impiegare per mettere al sicuro la validità di un documento rispetto agli eventi che possono occorrere con il fluire del tempo.

Nelle successive sezioni ci si sofferma sulla descrizione delle attività fondamentali di un sistema che provveda al consolidamento, ossia la marcatura temporale e la verifica dello stato di validità dei certificati.

Esula dagli scopi di questo documento entrare nel merito dell'opportunità di implementare queste funzioni sotto forma di un ben definito sistema centrale dedicato al consolidamento piuttosto che in forma più distribuita, integrata in componenti ed applicazioni più o meno specializzate.

7.1 VERIFICA DELLA VALIDITÀ DEL CERTIFICATO

Il consolidamento della valenza probatoria di un documento è completo se all'informazione temporale che fissa un istante di riferimento si associa la prova della validità del certificato associato ad una firma digitale in quell'istante.

È vero che a distanza di tempo (in sede di contenzioso, per esempio) questa informazione può essere richiesta, per via amministrativa, al Certificatore che aveva emesso il certificato in questione, ma è necessario (per evidenti esigenze di convalida dei documenti) assicurarsi, all'atto del consolidamento, che il certificato è effettivamente valido.

A parte lo stato di "non scaduto" che si accerta in modo ovvio confrontando la data attuale (o quella che corrisponde alla marca temporale) con quella di scadenza nominale del certificato, il compito più delicato è determinare se per un dato certificato non siano in corso provvedimenti di sospensione o revoca.

L'argomento è particolarmente delicato e di non facile soluzione. Le successive sottosezioni indicano diversi approcci per la soluzione di questo problema.

7.1.1 CRL – LISTE DI SOSPENSIONE E REVOCA

La pubblicazione delle CRL (Certificate Revocation List) è attualmente obbligatoria per i Certificatori accreditati (Delib. CNIPA 4/2005, art. 9). Il sistema che intende verificare lo stato di revoca di un certificato può leggere, dall'indirizzo (URL) contenuto nel certificato stesso (CRL Distribution Point), la lista che eventualmente potrebbe contenere l'informazione riguardo allo stato di sospensione e revoca del certificato.

Il Certificatore pubblica le CRL aggiornate con una certa periodicità (ricavabile dall'intestazione di ogni CRL), senza che peraltro le regole tecniche indichino un intervallo massimo per tale periodicità.

Tali regole tecniche (DPCM 13/01/2004, art. 22) prescrivono che in caso di possibile compromissione della chiave privata il certificatore debba procedere tempestivamente alla pubblicazione della sospensione, ma sussistono differenti interpretazioni sul significato del termine "tempestivamente" ed, allo stato, non sembra di poter contare su una pronta ed anticipata – rispetto all'intervallo programmato – disponibilità di una CRL aggiornata.

Sul piano tecnico la gestione delle CRL da parte dei certificatori è molto onerosa, per cui non v'è da aspettarsi un significativo miglioramento della frequenza di aggiornamento delle stesse rispetto agli intervalli variabili tra 6 e 24 ore che si osservano oggi.

Questo scenario evidenzia la difficoltà di determinare lo stato di validità di un certificato senza dover attendere, nel peggiore dei casi, molte ore.

D'altronde "La revoca o la sospensione di un certificato qualificato, comunque motivate, hanno effetto dal momento della pubblicazione..." (Dlgs 82/2005, art. 21, comma 3).

Sul piano formale, quindi, la lettura puntuale di una CRL, eventualmente ripetuta alcune volte in un intervallo ragionevole (alcuni minuti) allo scopo di non perdere eventuali nuove pubblicazioni

quasi coincidenti con l'interrogazione, è sufficiente per poter concludere che un certificato non è sottoposto a provvedimenti di sospensione e revoca.

Al di là del piano formale può restare il dubbio che la CRL a disposizione, essendo in generale "vecchia" di alcune ore, manchi nel segnalare una sospensione già avvenuta dopo la sua pubblicazione. Ma a questo dubbio non v'è modo di rispondere se non attendendo una prossima pubblicazione. Che, in generale, può avvenire a distanza di ore.

NOTA: Il citato Dlgs 82/2005, art. 21, comma 3 prosegue "..., salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate". Questa importante precisazione riconduce ad una gestione del problema a livello organizzativo, si veda la sez. 7.1.3.

7.1.2 SERVIZIO PUNTUALE DI INFORMAZIONE SULLO STATO DI VALIDITÀ DI UN CERTIFICATO, EROGATO DAL CERTIFICATORE

Un servizio di questo genere potrebbe essere erogato per mezzo del protocollo standard OCSP (Online Certificate Status Protocol); L'erogazione di un servizio OCSP è attualmente facoltativa per i Certificatori (Delib. CNIPA 4/2005, art. 10) e non risulta che alcuno di essi lo abbia attualmente in funzione a livello di produzione.

Tuttavia i maggiori Certificatori hanno in corso sperimentazioni, anche avanzate, per cui è lecito aspettarsi che una pressione da parte del mercato possa indurli a renderlo operativo in tempi brevi.

L'aspetto importante di un servizio di questo genere è che se venisse erogato direttamente dal certificatore, il quale dispone in tempo reale delle informazioni di sospensione e revoca, esso potrebbe essere veramente puntuale. Si noti che una response OCSP reca la firma dell'emittente, nonché l'indicazione della data ed ora di aggiornamento dell'informazione e la data in cui la stessa response è stata prodotta (che dovrebbe coincidere, a meno di qualche secondo con la marca temporale).

Rispetto alle CRL questo servizio si annuncia evidentemente più confacente alle necessità del consolidamento, non solo sul piano formale.

7.1.3 APPROCCIO ORGANIZZATIVO

Una soluzione organizzativa al problema della disponibilità puntuale dell'informazione sullo stato di sospensione o revoca di un certificato è la gestione centralizzata di tali informazioni all'interno dell'organizzazione che ospita i sistemi ed a cui appartengono i soggetti firmatari dei referti.

Si tratta di:

- 1 istituire nell'organizzazione un "ufficio di gestione del servizio di certificazione". Verosimilmente a tale funzione faranno riferimento i servizi tipici di Registration Authority, ma in particolare dovrà occuparsi delle richieste di sospensioni e revoche;
- 2 imporre, a livello di regolamento interno, che tutti i titolari di certificato qualificato rilasciato per tramite della funzione descritta (e che dovranno essere gli unici abilitati a firmare i documenti nell'ambito delle attività dell'organizzazione) comunichino innanzitutto (od esclusivamente) a tale ufficio di gestione le richieste di sospensione e revoca; evidentemente questo implica l'esistenza di un punto di ascolto disponibile con continuità;
- 3 l'ufficio di gestione dovrà inoltrare, con l'appropriata tempestività, le richieste di sospensione e revoca al Certificatore; nel contempo dovrà aggiornare un database interno per la gestione

dello stato dei certificati, indicando lo stato di non utilizzabilità del certificato a partire da quel momento;

- 4 un apposito server collegato a tale database dovrebbe erogare un servizio di tipo OCSP – ma è possibile prevedere modalità tecniche differenti – che il sistema di consolidamento (ma anche quello di sign-on ed in generale qualunque sottosistema abbia necessità di verificare lo stato di validità di un certificato) possa consultare per avere informazioni tempestive; naturalmente il servizio dovrebbe combinare le informazioni locali con quelle disponibili nelle CRL dei certificatori.

7.1.4 CONSIDERAZIONI

I tre approcci descritti nelle precedenti sezioni richiedono la disponibilità di diversi elementi infrastrutturali. Le CRL sono l'unica infrastruttura disponibile nell'immediato, mentre gli altri due servizi richiedono uno sforzo ulteriore, rispettivamente da parte dei Certificatori o dell'organizzazione ospite.

La scelta di un approccio rispetto agli altri, nell'implementazione, non può che derivare dalla valutazione dei diversi fattori in gioco: aspetto formale della validità di un certificato, criticità del tempo di consolidamento, costi di gestione, evoluzione dei Certificatori.

Da ultimo vale la pena di ribadire che la verifica della validità di un certificato, anche avuto riguardo allo stato di sospensione o revoca, dovrebbe essere svolta dai sistemi di gestione PRIMA di consentirne l'uso per apporre una firma digitale.

Questo accorgimento – peraltro di non sempre facile attuazione, almeno ai massimi livelli di accuratezza – non elimina la necessità di ripetere tale verifica in fase di consolidamento, se non altro a titolo di controprova finale centralizzata.

7.2 VERIFICA DELLA VALIDITA' DEL CERTIFICATO

Il consolidamento della valenza probatoria di un documento è completo se all'informazione temporale che fissa un istante di riferimento si associa la prova della validità del certificato associato ad una firma digitale in quell'istante.

È vero che a distanza di tempo (in sede di contenzioso, per esempio) questa informazione può essere richiesta, per via amministrativa, al Certificatore che aveva emesso il certificato in questione, ma è necessario (per evidenti esigenze di convalida dei documenti) assicurarsi, all'atto del consolidamento, che il certificato sia effettivamente valido.

A parte lo stato di "non scaduto" che si accerta in modo ovvio confrontando la data attuale (o quella che corrisponde alla marca temporale) con quella di scadenza nominale del certificato, il compito più delicato è determinare se per un dato certificato non siano in corso provvedimenti di sospensione o revoca.

Esistono almeno due diversi approcci possibili per ottenere questa informazione:

- Consultazione delle liste di sospensione e revoca (CRL – Certificate Revocation List)
La pubblicazione delle CRL è attualmente obbligatoria per i Certificatori accreditati (Delib. CNIPA 4/2005, art. 9). Il sistema che intende verificare lo stato di revoca di un certificato può leggere, dall'indirizzo (URL) contenuto nel certificato stesso (CRLDistributionPoint), la lista che

eventualmente potrebbe contenere l'informazione riguardo allo stato di sospensione e revoca del certificato; il Certificatore pubblica le CRL aggiornate con una certa periodicità (ricavabile dall'intestazione di ogni CRL), ma esistono casi di particolare urgenza (DPCM 13/01/2004, art. 22) in cui deve avvenire una pubblicazione anticipata di una nuova CRL, contenente i dettagli della sospensione urgente. Poiché la revoca o la sospensione di un certificato qualificato, qualunque ne sia la causa, ha effetto dal momento della pubblicazione della lista che lo contiene (Dlgs 82/2005, art. 36, comma 3) se in un dato istante si legge la CRL dal server del Certificatore e tale CRL non contiene alcun riferimento al certificato sottoposto a verifica si potrebbe concludere che il certificato è valido. La successiva pubblicazione di una CRL diversa da quella già osservata (al più tardi alla scadenza dell'intervallo programmato di aggiornamento) sarà poi la prova finale – assumendo che nemmeno in tale versione della CRL compaia un riferimento al certificato in esame – della validità del certificato.

- Richiesta esplicita sullo stato di validità del certificato (OCSP – Online Certificate Status Protocol)

L'erogazione di un servizio OCSP è attualmente facoltativa per i Certificatori (Delib. CNIPA 4/2005, art. 10) e non risulta che alcuno di essi lo abbia in funzione. Tuttavia i maggiori Certificatori hanno in corso sperimentazioni, anche avanzate, per cui è lecito aspettarsi che una pressione da parte del mercato possa indurli a renderlo operativo in tempi brevi.

Rispetto alle CRL questo servizio si annuncia come più soddisfacente alle necessità del consolidamento: il sistema che intende verificare lo stato di un certificato trasmette una esplicita interrogazione al server del Certificatore, il quale fornisce una risposta – firmata – con l'informazione richiesta (valido, sospeso, revocato), unita all'informazione oraria di generazione della response (producedAt).

Un ulteriore approccio, particolarmente interessante nel medio e lungo termine, è quello di poter disporre all'origine delle informazioni relative allo stato dei certificati intestati agli appartenenti dell'organizzazione. Se un'azienda o una P.A. può gestire in totale autonomia – rispetto al Certificatore – le richieste di sospensione e revoca, evidentemente non è soggetto all'onere di interagire con informazioni provenienti direttamente dal Certificatore, magari estratte laboriosamente dalle CRL. L'organizzazione stessa potrebbe impiantare un proprio sistema OCSP che eroghi il servizio basato su informazioni di prima mano.

Ancora più appetibile, in uno scenario prossimo venturo, è che la sottoscrizione digitale di un documento sia possibile – in un determinato contesto applicativo – solo dopo l'avvenuta autenticazione (sign-on) presso il sistema mediante un apposito certificato (di autenticazione, appunto) strettamente legato a quello di firma (per esempio residente sulla stessa smartcard).

In altre parole, una richiesta di sospensione di certificato da parte di un utente provocherebbe l'immediato fuori servizio del suo dispositivo, negando l'accesso al sistema e – per conseguenza – l'impossibilità di immettere documenti firmati.

È importante sottolineare che la realizzazione di uno scenario di questo tipo non richiede solo la disponibilità di dispositivi di firma con integrate credenziali di autenticazione (questi sono infatti già disponibili, per esempio, con le CNS – Carta Nazionale dei Servizi), ma soprattutto una infrastruttura applicativa che renda veramente impossibile l'introduzione in circolo di documenti firmati al di fuori del sistema controllato.

Da ultimo vale la pena osservare che la verifica della validità di un certificato, anche avuto riguardo allo stato di sospensione o revoca, dovrebbe essere svolta dai sistemi di gestione PRIMA di consentirne l'uso per apporre una firma digitale.

Questo accorgimento – peraltro di non sempre facile attuazione, almeno ai massimi livelli di accuratezza – non elimina la necessità di ripetere tale verifica in fase di consolidamento, se non altro a titolo di controprova finale centralizzata.

8 CONSERVAZIONE SOSTITUTIVA DEI DOCUMENTI

8.1 DOCUMENTI DEMATERIALIZZATI DA CONSERVARE

In qualsiasi Struttura sanitaria, la banca dati clinica viene predisposta ed organizzata esclusivamente per scopi clinici, al fine di poter consultare la documentazione precedente e quindi ricostruire il quadro clinico del paziente per una migliore diagnosi, cura ed assistenza. Le regole per la tenuta di una tale banca dati non vengono individuate da norma alcuna; può pertanto essere attuata su libera iniziativa e con modalità scelte dai singoli utilizzatori.

L'archivio legale è invece espressamente previsto da disposizioni normative che ne individuano i contenuti, così come più sopra visto per la documentazione di Radiodiagnostica per Immagini e di Laboratorio, e ne dettano le specifiche modalità per la formazione e la gestione: gli scopi della sua esistenza sono quindi quelli prettamente medico-legali e probatori.

E' stata ormai pienamente raggiunta e decretata l'equiparazione giuridica fra archivio legale analogico e digitale, purché siano soddisfatte per entrambi le regole di tenuta prescritte dalle norme: Deliberazione CNIPA n. 11/04 all'art. 2, co. 1 dichiara infatti che "Gli obblighi di conservazione sostitutiva dei documenti previsti dalla legislazione vigente sia per le pubbliche amministrazioni sia per i privati, sono soddisfatti a tutti gli effetti ... qualora il processo di conservazione venga effettuato con le modalità di cui agli articoli 3 e 4".

Il vigente decreto legislativo 82/2005 (Codice dell'Amministrazione Digitale), co. 1, Dematerializzazione dei documenti delle pubbliche amministrazioni, sostiene addirittura che "Le pubbliche amministrazioni valutano in termini di rapporto tra costi e benefici il recupero su supporto informatico dei documenti e degli atti cartacei dei quali sia obbligatoria o opportuna la conservazione e provvedono alla predisposizione dei conseguenti piani di sostituzione degli archivi cartacei con archivi informatici". Ed aggiunge all'art. 43, Riproduzione e conservazione dei documenti. 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 sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo. ... 2. Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali. 3. I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali".

8.2 RESPONSABILE DEL PROCEDIMENTO DI CONSERVAZIONE SOSTITUTIVA

Dalle indicazioni normative più volte ripetute, nella gestione analogica responsabile del mantenimento nel tempo dei referti riguardanti un paziente interno è la Direzione Sanitaria del presidio ospedaliero ove sono stati re dati. Responsabile della gestione dell'iconografia e del suo

mantenimento nel tempo è invece il Responsabile dell'Unità Operativa che ha provveduto alla produzione¹⁹. 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.

Ciò premesso, la documentazione sanitaria oggetto di questo documento può essere conservata seguendo le disposizioni di cui all'art. 5 della Deliberazione CNIPA n.11/04.

Questa specifica norma individua e definisce analiticamente le attività di competenza del Responsabile della conservazione, circoscrivendo di conseguenza le responsabilità derivanti a suo carico.

L'elencazione normativa dei compiti afferenti al Responsabile della conservazione, così come di seguito definita, deve essere integrata con la normativa che regola le modalità esecutive di volta in volta individuate dal Legislatore nel testo del codice dell'amministrazione digitale in combinato disposto con le regole tecniche contenute nella Deliberazione²⁰.

L'art. 5 della Deliberazione CNIPA n.11/04, al comma 1 recita che

"Il responsabile del procedimento di conservazione sostitutiva:

- a. definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare, della quale tiene evidenza. Organizza conseguentemente il contenuto dei supporti ottici e gestisce le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche per consentire l'esibizione di ciascun documento conservato;*
- b. archivia e rende disponibili, con l'impiego di procedure elaborative, relativamente ad ogni supporto di memorizzazione utilizzato, le seguenti informazioni:
 - 1) descrizione del contenuto dell'insieme dei documenti;*
 - 2) estremi identificativi del responsabile della conservazione;*
 - 3) estremi identificativi delle persone eventualmente delegate dal responsabile della conservazione, con l'indicazione dei compiti alle stesse assegnati;*
 - 4) indicazione delle copie di sicurezza;**
- c. mantiene e rende accessibile un archivio del software dei programmi in gestione nelle eventuali diverse versioni;*
- d. verifica la corretta funzionalità del sistema e dei programmi in gestione;*
- e. 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;*
- f. richiede la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;*
- g. definisce e documenta le procedure di sicurezza da rispettare per l'apposizione del riferimento temporale;*
- h. 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".*

¹⁹ Tuttavia, come è già stato sottolineato, oggi, con l'avvento della gestione digitale, non ha più senso alcuno differenziare fra conservazione della documentazione sanitaria per paziente interno e per paziente esterno.

²⁰ In particolare giova richiamare l'art. 44 del Dlgs 82/2005 sui requisiti del sistema di conservazione come richiamati dall'art 5, lett. a) del. N. 11/2004 CNIPA, nonché l'art. 4 della medesima delibera.

È da subito utile evidenziare come le attività qui sopra elencate richiedano un alto livello di competenze specialistiche²¹, tali da scongiurare che le figure del Direttore Sanitario, del Responsabile dell'U.O. di Diagnostica per Immagini e del Responsabile dell'U.O. di Laboratorio diano personalmente esecuzione²² ai compiti più prettamente tecnici del Responsabile della conservazione sostitutiva.

In tal senso è provvidenziale il disposto di cui al successivo comma 2²³ dell'articolo in commento, che rende possibile organizzare il servizio di conservazione evitando che, a causa delle fondamentali competenze ed esperienze tecniche richieste per il corretto svolgimento pratico del compito del Responsabile della conservazione, siano quei ruoli dirigenziali e clinici a dover essere incaricati in concreto di tali attività.

Tenendo conto di quanto sopra evidenziato, la figura del Responsabile della conservazione, oltre ad essere obbligatoria per legge, risulta essere assolutamente indispensabile da un punto di vista operativo.

Il Responsabile della conservazione infatti, pur essendo (almeno quanto alla funzione) un soggetto terzo rispetto alla mera formazione della documentazione digitale, riveste un fondamentale ruolo con lo svolgimento sia delle proprie mansioni pratiche ed esecutive, sia di quelle di verifica e controllo dei processi legati alla conservazione tutta.

Alla luce delle attività e competenze che la Deliberazione CNIPA individua in capo al Responsabile della conservazione, oltre che dell'eterogeneità delle realtà sanitarie più o meno complesse, appare indispensabile avviare l'analisi del tema, con l'individuazione delle conseguenti possibili linee di condotta, facendo riferimento a due scenari aziendali diversi²⁴: ovvero ad un'Azienda Sanitaria al proprio interno fortemente articolata sul piano tecnico-organizzativo e ad un'Azienda invece mancante di una consistente struttura in questo senso.

Nel primo caso (Azienda fortemente strutturata ed organizzata), una volta nominato il Responsabile della conservazione, sarà opportuno e raccomandabile che questi deleghi, in tutto o in parte, l'esecuzione delle attività di sua competenza, delegando con nomina formale quei

²¹ Peraltro richiamate al successivo comma 2 del medesimo art. 5 con riferimento alle persone cui è delegabile l'attività di conservazione sostitutiva.

²² La norma di cui al secondo comma, finalizzata a rendere possibile la conservazione sul piano pratico, evitando che il RCS venga "sovraccaricato" sul versante operativo, non può che essere letta in combinato disposto con l'art. 2232 cod. civ.

Infatti, in base a tale articolo, considerata la natura professionale dell'attività di conservazione sostitutiva (rientrante nella previsione del codice civile, al libro v, capo II relativo alle Professioni intellettuali), il RCS sarebbe obbligato a svolgere personalmente l'incarico, con tutte le evidenti difficoltà e ricadute sul piano pratico logistico e tecnico.

Il RCS potrà dunque avvalersi, sotto la propria direzione e responsabilità, di delegati (sostituti ed ausiliari) pubblici o privati per l'esecuzione materiale del processo.

²³ L'art. 5 della Deliberazione CNIPA n. 11/04, al comma 2 prevede che "2. Il responsabile del procedimento di conservazione sostitutiva può delegare, in tutto o in parte, lo svolgimento delle proprie attività ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni ad esse delegate".

²⁴ Entrambi gli scenari sono accomunati dal fatto che il soggetto da nominarsi quale Responsabile della conservazione non può che essere unico per la conservazione ottica di tutta la documentazione aziendale. Inoltre, per i compiti sino ad ora evidenziati, il Responsabile va individuato all'interno dell'Azienda sanitaria e si consiglia venga individuato fra i funzionari o i dirigenti apicali. Appare fondamentale anche che l'identificazione del soggetto sia esplicitata attraverso una nomina ufficiale e formale, con individuazione di tutti gli elementi caratterizzanti; per realizzare questo nella Pubblica Amministrazione sanitaria non si può che ricorrere alla forma del provvedimento o dell'atto deliberativo aziendale.

soggetti interni all'Azienda che dimostrino adeguate esperienze e competenze, in base a quanto previsto dall'art. 5, co. 2 della Deliberazione CNIPA n. 11/04²⁵.

Nel secondo caso invece (Azienda poco strutturata e organizzata che ritenga di non voler investire per diventarlo), si potrà legittimamente ed opportunamente decidere di affidare il procedimento di conservazione, in tutto o in parte, ad altri soggetti, pubblici o privati", così come prevede l'art. 5, comma 3 della Deliberazione²⁶, senza per questo essere manlevati da responsabilità.

In relazione a tale ultima previsione normativa, si ritiene che, essendovi statuita la possibilità di affidare in outsourcing l'intero processo, non venga esclusa l'ipotesi che anche la nomina del RCS possa ricadere su Enti esterni alla struttura.

Resta, tuttavia, raccomandabile che tale funzione venga affidata a Soggetto interno.

8.3 NOMINA DEL RESPONSABILE, DELEGHE E INCARICHI

Alla luce di quanto qui sopra riportato, la figura del Responsabile della conservazione risulta essere assolutamente indispensabile, sia da un punto di vista operativo, sia da un punto di vista normativo e legale.

Se appare fondamentale individuare, all'interno o all'esterno della Struttura, un Responsabile della conservazione sostitutiva, si ritiene altrettanto necessario formalizzare ed ufficializzare la nomina

²⁵ In virtù dell'art. 5 secondo comma il RCS può totalmente (o parzialmente) delegare lo svolgimento delle attività meglio definite alle lettere da a) ad h) del primo comma del medesimo articolo.

Tale delega non può che concretarsi tramite un contratto di mandato (art. 1703 e segg C.C.) in virtù del quale il mandatario si obbligherà a svolgere le attività elencate nell'art. 5 per conto del mandante.

Non è necessaria la forma scritta a pena di nullità, ma è misura minima di prudenza, considerata la complessità delle statuizioni che esso deve contenere ed in relazione alle eventuali responsabilità civili e penali coinvolte, provvedere a formalizzarlo con estrema precisione e dettaglio.

È facoltà delle parti decidere che il contratto venga espressamente considerato gratuito, superando la presunzione di onerosità prevista dall'art. 1709 cod. civ. in forza del quale la misura del compenso, se non pattuita tra le parti, è determinata dalle tariffe professionali, dagli usi o dal Giudice.

Qualora il contratto venga stipulato a titolo gratuito, la responsabilità civile per colpa sembrerebbe doversi valutare con minor rigore (art. 1710, 1° comma, Cod. Civ.), in relazione alla diligenza richiesta (del buon padre di famiglia, art. 1768 Cod. Civ.). La scelta del mandato gratuito sarà pertanto affidata alle politiche gestionali interne all'Azienda Ospedaliera.

Invero, l'attività in questione, in considerazione dell'uso della firma digitale ad esso funzionale ed imprescindibile, sembra rientrare (così si è sempre espresso il legislatore) tra quelle di cui all'art. 2050 cod. civ. definibili pericolose "per sua natura o per la natura dei mezzi adoperati" ed inoltre, i requisiti di competenza ed esperienza richiesti ai mandatari in base all'art. 5, secondo comma, richiamano le responsabilità del prestatore d'opera che implichi "la soluzione di problemi tecnici di speciale difficoltà" (art. 2236 Cod. Civ.).

È dunque evidente che i soggetti delegati dal RCS dovranno svolgere il loro incarico, nei limiti del mandato, applicando la diligenza professionale (art. 1176, secondo comma, Cod. Civ.) richiesta dalla natura (pericolosa ex art. 2050 Cod. Civ.) dell'attività esercitata in base alla norma CNIPA e rispondendo pertanto dei danni per responsabilità contrattuale soltanto nei casi di dolo (coscienza e volontà di provocare il danno) o colpa grave (art. 2236 Cod. Civ.).

Quanto sopra, richiama l'inderogabile obbligo del RCS di adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

L'adozione di tali misure consentirà al RCS di assolvere correttamente all'onere di provare la propria diligenza professionale in caso di danno. Prova che, com'è noto, viene posta a suo carico (e non del danneggiato) in virtù del principio dell'inversione dell'onere della prova previsto dalla legge (art. 2050 Cod. Civ.).

È evidente che il RCS (e la struttura) saranno solidalmente responsabili (ex art. 2055 Cod. Civ.) per eventuali danni prodotti da i loro incaricati (delegati) (art. 1228 e 2049 Cod. Civ.).

²⁶ "Il procedimento di conservazione sostitutiva può essere affidato, in tutto o in parte, ad altri soggetti, pubblici o privati, i quali sono tenuti ad osservare quanto previsto dalla presente deliberazione".

del soggetto che dovrà ricoprire tale ruolo, esplicitandone gli elementi caratterizzanti. Nella Pubblica Amministrazione sanitaria non possiamo che pensare ad una formalizzazione attraverso un provvedimento o un atto deliberativo aziendale.

Come già accennato, la Deliberazione CNIPA n.11/04 all'art. 5, co. 3, prevede che il Responsabile della conservazione sostitutiva possa delegare alcune, o anche tutte, le attività a lui affidate.

Si ritiene importante che, al fine di individuare le singole responsabilità in capo ad ogni attore coinvolto, pure la delega venga prevista e formalizzata, attraverso un contratto di mandato²⁷. Con questo ultimo, avviene il conferimento dell'incarico dello svolgimento di specifiche attività pratiche da parte del Responsabile della conservazione a soggetti altrettanto ben individuati e l'accettazione da parte di questi.

8.4 SUPPORTI PER LA CONSERVAZIONE SOSTITUTIVA

Quando si parla di conservazione nel tempo di documenti (o informazioni) in formato digitale è utile ricordare che sono almeno quattro gli aspetti da tenere in considerazione:

- 1) Si vuole/si deve ottenere la garanzia che i documenti conservati corrispondano agli originali e non subiscano alterazioni nel tempo; nel caso dovessero subirne – vuoi per motivi accidentali o fraudolenti – è bene che chi li consulta ne abbia notizia;
- 2) Bisogna essere certi che quanto registrato su di un supporto al momento della conservazione sia leggibile, indipendentemente dal suo valore o dalle sue caratteristiche, per tutto il periodo per cui deve essere conservato;
- 3) Bisognerebbe mettere in atto tutte le misure idonee a fare sì che in fase di conservazione non venga sovrascritta per errore una registrazione, da conservare, effettuata precedentemente;
- 4) I documenti conservati devono essere (facilmente) reperibili all'interno dell'archivio di conservazione.

Come si vede sono esigenze che solo apparentemente sono simili e si ottengono, in genere, con processi/strumenti differenti.

Nel caso della Conservazione Sostitutiva la prima esigenza è soddisfatta tramite il processo di conservazione, garantito dal responsabile e nel quale ha un ruolo primario la tecnologia della Firma Digitale del responsabile e la Marca Temporale (certificazione della data e ora e prolungamento dell'efficacia delle firme di cui sopra prima della scadenza del loro certificato) dell'evidenza del volume dei dati da conservare.

Uno dei modi per soddisfare la terza esigenza può essere l'impiego di supporti ottici di registrazione WORM, Write Once Read Many [si noti che questa tipologia di supporto non è più richiesta dalle Regole Tecniche AIPA/CNIPA]; in alternativa il compito potrebbe esser affidato a procedure di elaborazione che assicurino la non distruzione accidentale dei dati.

La quarta è il risultato di una opportuna classificazione dei documenti conservati e di una procedura che, in caso di perdita, consenta di ricostruirlo.

Concentriamo l'attenzione sulla seconda.

²⁷ Regolamentato dagli artt. 1703 e segg. Cod. Civ.

Essa, nella normativa vigente, sembrerebbe soddisfatta dall'impiego di supporti a Tecnologia Laser, dall'obbligo di produrre delle copie di sicurezza e dall'obbligo di verifica periodica (almeno ogni cinque anni) dell'effettiva leggibilità dei documenti conservati.

Per quanto concerne i supporti a tecnologia laser, questi non sono influenzati da campi magnetici e hanno una vita molto elevata; si ricorda che gli attuali Dischi Ottici UDO (Ultra Density Optical) da 5,25 pollici sono dati con una vita di 50 anni, mentre per quelli da 12 pollici si arriva a 100.

I meno "resistenti" sono i CD, così come lo sono i più moderni e capienti DVD; a ciò si deve, molto probabilmente, la richiesta di provvedere alla leggibilità dei documenti almeno ogni 5 anni.

Sembrerebbe tutto a posto, ma

La Deliberazione CNIPA 11/2004, infatti, dal Titolo, alle Definizioni, agli Articoli 3 e 4 (definizione del processo di conservazione e dei differenti tipi di riversamento) fa esplicito riferimento a "Supporti Ottici", l'articolo 8, però, recita *"Tenuto conto dell'evoluzione tecnologica e della disciplina dettata dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, è data facoltà ..., ove non ostino particolari motivazioni, di utilizzare, ..., 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"*.

Ferma restando la superfluità evidente insita nell'affermazione che un "supporto (ottico o non ottico) sia in grado di garantire la conformità dei documenti agli originali" (si è appena visto che **la conformità ai documenti è data dal processo di archiviazione e non dal supporto**)

occorre verificare se si volesse in qualche modo autorizzare anche gli altri tipi di supporti.

Anche il decreto del Ministro dell'Economia e delle Finanze del 23 gennaio 2004 fa esplicito riferimento a una memorizzazione *"su qualsiasi supporto di cui sia garantita la leggibilità nel tempo"*. Ciò farebbe pensare che, almeno per i documenti rilevanti ai fini tributari, il tipo di supporto utilizzato per il processo di Conservazione non sia importante per il Ministro dell'economia e delle finanze, che si preoccupa solo di far rilevare la necessità di poter esibire nel tempo il documento (leggibilità garantita nel tempo), in caso contrario ... il documento è come se non fosse disponibile presso il contribuente.

Vista l'interessante possibilità che si prospetta, ossia la libertà di svincolarsi dai supporti ottici in favore della più convenzionale e diffusa tecnologia magnetica, è bene approfondire l'argomento.

Nelle Note Esplicative che accompagnano la Deliberazione il punto 4 (Supporto di memorizzazione), oltre a ribadire che *"la deliberazione autorizza l'utilizzazione di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante la tecnologia laser"*, facendo riferimento a *"quanto previsto ... dal testo unico (Articolo 6²⁸ del DPR, 28/12/2000, n. 445) circa la*

²⁸ DECRETO DEL PRESIDENTE DELLA REPUBBLICA 28/12/2000, N. 445, RECANTE IL TESTO UNICO DELLE DISPOSIZIONI LEGISLATIVE E REGOLAMENTARI IN MATERIA DI DOCUMENTAZIONE AMMINISTRATIVA

Articolo 6 (L-R)

Riproduzione e conservazione di documenti

1. Le pubbliche amministrazioni ed i privati hanno facoltà di sostituire, a tutti gli effetti, i documenti dei propri archivi, le scritture contabili, la corrispondenza e gli altri atti di cui per legge o regolamento è prescritta la conservazione, con la loro riproduzione su supporto fotografico, su supporto ottico o con altro mezzo idoneo a garantire la conformità dei documenti agli originali.
2. Gli obblighi di conservazione ed esibizione dei documenti di cui al comma 1 si intendono soddisfatti, sia ai fini amministrativi che probatori, anche se realizzati su supporto ottico quando le procedure utilizzate sono conformi alle regole tecniche dettate dall'Autorità per l'informatica nella pubblica amministrazione.
3. I limiti e le modalità tecniche della riproduzione e dell'autenticazione dei documenti di cui al comma 1, su supporto fotografico o con altro mezzo tecnico idoneo a garantire la conformità agli originali, sono stabiliti con decreto del Presidente del Consiglio dei Ministri.
4. Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle amministrazioni pubbliche e sugli archivi privati dichiarati di notevole interesse storico, ai sensi delle disposizioni del Capo II del decreto legislativo 29 ottobre 1999, n. 490.

possibilità d'impiego ai fini della conservazione di altro mezzo idoneo a garantire la conformità dei documenti agli originali e in considerazione dell'evoluzione tecnologica nel frattempo avvenuta" afferma che "la deliberazione consente (Art. 8) di utilizzare un qualsiasi altro supporto di memorizzazione, oltre quelli a tecnologia laser, se non ostino particolari motivazioni e comunque nel rispetto delle regole tecniche previste dalla deliberazione stessa".

CNIPA "ritiene, infatti, che i tecnicismi ... (adottati in fase di conservazione) ... siano idonei a garantire l'integrità del documento nel processo di sua conservazione, qualunque sia il tipo di supporto di memorizzazione, anche se diverso da quello ottico. Soltanto specifiche motivazioni potrebbero suggerire o richiedere l'impiego di una particolare tipologia di supporto".

Se si tiene conto delle affermazioni appena riportate, supportate dal dettato del Ministro dell'economia e delle finanze, nonché dal Codice dell'amministrazione digitale (il comma 1 dell'Articolo 43 fa riferimento solo ad una garanzia di conservazione nel tempo dei documenti) non è imprudente o "contra legem" affermare che: salvo specifiche situazioni, **il processo di Conservazione Sostitutiva può essere effettuato impiegando supporti anche non ottici!**

Resta da interpretare l'Articolo 6 del succitato Testo Unico.

Il mezzo idoneo di cui al comma 1 è più "leggibile" come "strumento/modalità" che non come sinonimo di supporto.

Questa lettura è confortata dal comma 3 che parla di "mezzo tecnico" il cui (qualunque cosa esso sia) impiego si richiede sia regolato da opportuno DPCM.

[Anche dal semplice esame del testo sembra proprio non essere corretto "interpretare" il mezzo - o mezzo tecnico del comma 3 - come sinonimo di supporto o tecnica di registrazione; a tale conclusione conduce anche l'analisi logica del testo, dove i due complementi di mezzo

1. "con la loro riproduzione su supporto fotografico, su supporto ottico"
2. "con altro mezzo idoneo ..."

risultano uniti attraverso la congiunzione avversativa "o", che indica appunto una alternativa.

Il testo, chiaramente, evita quindi di precludere il futuro utilizzo di tecnologie-mezzi più evoluti di quelli attualmente disponibili, precisando al comma 3 che tale utilizzo dovrà comunque essere regolamentato attraverso normative emanate con DPCM.]

Lo stesso Codice dell'amministrazione digitale al comma 2 dell'Articolo 43²⁹ [che riprende l'Articolo 6 del Testo Unico], fa esplicito riferimento ad un "processo idoneo a garantire la conformità dei documenti agli originali".

Tale interpretazione del Testo Unico è molto forzata invero, anche se esprime chiaramente la volontà di CNIPA di consentire l'uso di tecnologie di memorizzazione non ottiche, motivata, come

²⁹ DECRETO LEGISLATIVO 7 marzo 2005, n. 82 - Codice dell'amministrazione digitale.
Articolo 43

Riproduzione e conservazione dei documenti

- 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 sia effettuata in modo da garantire la conformità dei documenti agli originali e la loro conservazione nel tempo, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo **Errore. L'origine riferimento non è stata trovata.**
- Restano validi i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento già conservati mediante riproduzione su supporto fotografico, su supporto ottico o con altro processo idoneo a garantire la conformità dei documenti agli originali.
- I documenti informatici, di cui è prescritta la conservazione per legge o regolamento, possono essere archiviati per le esigenze correnti anche con modalità cartacee e sono conservati in modo permanente con modalità digitali.
- Sono fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi delle pubbliche amministrazioni e sugli archivi privati dichiarati di notevole interesse storico ai sensi delle disposizioni del decreto legislativo 22 gennaio 2004, n. 42.

già detto, dalla convinzione che la tecnologia della firma digitale offra di per sé sufficienti garanzie sull'integrità dei dati.

Resta, per di più, il fatto che il comma 2 dell'Articolo 6 del Testo Unico affidava ad AIPA/CNIPA la sola "regolamentazione" della conservazione realizzata tramite riproduzione su supporto ottico.

Il dettato dell'Articolo 8 della Deliberazione CNIPA 11/2004 appare dunque quantomeno dubbio nella sua legittimità e nella sua coerenza normativa.

Le precisazioni di cui sopra, alla data, sembra rebbero abbastanza prive di conseguenze visto che il Testo Unico è stato sostituito dal Codice dell'amministrazione digitale ... se non per il fatto che le Regole Tecniche di cui all'articolo 71 del Codice dell'amministrazione digitale sono attualmente le Regole Tecniche di cui alla Deliberazione CNIPA 11/2004 che all'articolo 6 del Testo Unico si ispirano e fanno riferimento.

Peraltro, le attuali tecnologie, in particolare quelle Raid per i Dischi magnetici, le procedure di "retention" e "refresh" dei Nastri, quelle di gestione del ciclo di vita delle informazioni, la capacità di gestire quelle che sono chiamate Retention Managed Data, Reference Data o Fixed Content Data [sono sinonimi di dati che devono essere conservati inalterati nel tempo], ed, infine, le procedure di back-up/recovery e disaster recovery, riducono al minimo i rischi di perdita d'informazioni se registrate su supporti scelti con professionalità e corredati di opportuni software di gestione.

In questa sede è opportuno ricordare, inoltre, che le aziende moderne fondano, di fatto, la loro attività, ed i loro profitti, su informazioni disponibili e gestite in formato digitale, utilizzando proprio le tecnologie appena citate.

8.4.1 LA PRASSI

Relativamente al contesto di nostro interesse e tenuto conto di quanto esposto nel paragrafo precedente, come ci si deve comportare nella pratica?

Dal punto di vista normativo non residuano dubbi interpretativi; ci si può quindi affidare alla norma recente (Codice dell'amministrazione digitale, Articolo 43, comma 1) e quindi svincolarsi a priori da un particolare tipo di supporto/tecnologia di registrazione, ma con quali criteri assicurare la "conservazione nel tempo" dei documenti, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71 (alla data la Deliberazione CNIPA 11/2004, che come si è visto dal punto di vista dei supporti/tecnologie di registrazione da impiegare è quantomeno contraddittoria)?

La tentazione di un ulteriore salto in avanti per poter ragionare nell'ottica di impiegare supporti non a tecnologia laser è grande (ciò è enfatizzato dal fatto che la tecnologia ottica non è molto diffusa e che quella magnetica sta diventando sempre più economica ed affidabile).

Sarà bene seguire comportamenti prudentziali e, se possibile, che non vadano contro norma e tecnologia. Pertanto:

1) I dubbi interpretativi, sopra evidenziati, portano a ritenere che la tecnologia ottica (magari WORM) offra certamente le maggiori garanzie di conformità ed affidabilità oggettiva dei supporti fisici; essendo essi amovibili consentono, inoltre una miglior distribuzione geografica delle copie generate, a maggior garanzia delle possibilità di recovery (con successo) di quanto registrato;

2) Le tecnologie più economiche dei CD-R, DVD±R, pur rientrando nella categoria dei supporti ottici e quindi rassicurando sul piano della mera conformità alle norme, presentano caratteristiche di durata oggettivamente limitate alle quali si può ovviare solo con rigorose procedure di

generazione di copie multiple (usando supporti di qualità, di diversi fornitori - o almeno da lotti differenti dello stesso fornitore - e unità di scrittura differenti) e di controllo di quanto registrato;

3) Le tecnologie magnetiche, la cui adozione parrebbe auspicabile da parte di tutti gli attori in gioco, possono offrire adeguate garanzie di durata ed affidabilità grazie all'impiego integrato in sistemi - peraltro di utilizzo molto diffuso e relativamente economico - che assicurino elevata ridondanza, accurate procedure di backup e di disaster recovery e che prevedano, anche, la distribuzione geografica delle copie. Questi comportamenti, peraltro basati su prodotti e sistemi consolidati, potrebbero compensare la minor affidabilità fisica della tecnologia magnetica rispetto a quella ottica.

In conclusione di questo paragrafo, ed in attesa della emissione di nuove regole tecniche - come previste dall'articolo 71 del Codice dell'amministrazione digitale - va precisato per completezza che si stanno verificando casi di Conservazione Sostitutiva realizzati con l'ausilio di supporti NON ottici, con il conforto di una interpretazione dell'articolo 8 Deliberazione CNIPA 11/2004 difforme da quella riportata in questa sede.

8.5 PROCEDURE DI CONSERVAZIONE SOSTITUTIVA

L'implementazione effettiva di procedure e sistemi per la Conservazione Sostitutiva, nei contesti presi in esame dal presente documento, non può che basarsi sull'art. 3 della Deliberazione CNIPA 11/2004.

Tale articolo descrive il processo e lo spiega come una "memorizzazione" su supporti ottici (ma anche non ottici, in base all'art. 8 e come ampiamente discusso nella precedente sez. 8.4) dei documenti oggetto della conservazione, per "terminare" con una operazione di apposizione di riferimento temporale e di firma digitale da parte del responsabile della conservazione.

In particolare si fornisce l'indicazione che la tale riferimento e tale firma digitale debbano essere apposte sull'insieme dei documenti oppure su una evidenza informatica contenente una o più impronte dei documenti o di insiemi di essi. Questa formulazione, di comprensione non immediata per i non addetti ai lavori, è stata introdotta nel 2004 proprio per rispondere i grandi dubbi che la versione del 2001 della stessa Deliberazione aveva lasciato su come si possa apporre una firma digitale ad un insieme di documenti.

L'interpretazione più semplice e più efficace della norma attuale prevede di costruire ex-novo un file di impronte (un'evidenza informatica, come descritta dalle definizioni, coincide con il concetto di file) in modo che contenga una registrazione (record) per ciascun documento e che il record contenga l'impronta (codice hash) dello stesso documento.

Si ricorda che l'impronta, o codice hash, di un documento consiste in una stringa binaria di piccole dimensioni (160 bit) in grado di rivelare ogni alterazione del documento da cui era stata calcolata.

Poiché questo singolo file, contenente le impronte di tutti i documenti appartenenti all'insieme considerato, verrà firmato digitalmente risulta chiaro che qualunque modifica apposta a qualunque documento appartenente all'insieme (chiamiamolo "volume") verrebbe rilevata da una operazione di verifica: l'impronta effettiva del documento alterato non coinciderebbe più con quella registrata nel file delle impronte, mentre la modifica di tale file non sarebbe possibile senza invalidarne la firma digitale.

8.5.1 FORMATO DEL FILE DELLE IMPRONTE

Le regole tecniche non forniscono alcuna prescrizione sul formato che deve assumere il file delle impronte.

Tuttavia pare ragionevole formulare alcune raccomandazioni volte a semplificare l'implementazione dei sistemi, magari ponendo le basi per raggiungere una futura interoperabilità tra diversi sistemi.

- il file dovrebbe contenere una intestazione autoesplicativa, contenente anche riferimenti sull'organizzazione che genera il volume ed altre informazioni che permettano di risalire facilmente, anche a distanza di anni, alla struttura che lo aveva prodotto;
- il file dovrebbe contenere un numero di record (i.e. elementi) pari al numero di documenti effettivamente presenti nel volume. Quantunque la formulazione dell'art. 3 della Delib. CNIPA 11/2004 lasci spazio ad una maggiore flessibilità (indicando la possibilità di includere impronte di documenti o di insiemi di essi), si ritiene di raccomandare almeno in questa fase l'adozione di strutture assolutamente lineari, con un record per ciascun singolo documento;
- ciascun record deve contenere quanto meno un riferimento univoco al documento cui si riferisce e l'impronta del documento stesso.

Va considerata l'opportunità di includere in questi record anche altri elementi di informazione, per esempio il contenuto di campi di indicizzazione: il vantaggio consisterebbe nella possibilità di usare questo stesso file di impronte come veicolo per il trasferimento del contenuto di un volume tra sistemi anche molto diversi. Il limite di questo approccio potrebbe essere la conformità alle norme in materia di privacy, qualora un intero file di impronte dovesse essere esibito con un singolo documento – per certificarne lo stato di “conservato” – mostrando inevitabilmente i campi di indicizzazione di molti altri documenti.

Una soluzione a questo problema può essere la produzione di due file di impronte per ciascun volume: uno “essenziale”, contenente solo le impronte e da usare per eventuale esibizione completa; un altro completo di tutte le informazioni disponibili.

Tra le moltissime opzioni possibili l'adozione di un formato XML per rappresentare il file delle impronte appare una scelta particolarmente ragionevole:

- il formato è intrinsecamente molto flessibile e sono disponibili enormi librerie di software, anche open source, per gestirlo
- la possibilità di associare un foglio di stile consente una presentazione efficace dei contenuti senza pregiudicare la possibilità dell'elaborazione automatica
- pensando all'operazione di sottoscrizione digitale, XML è compatibile con l'encapsulation nei formati di busta crittografica attualmente consentiti (PKCS#7) e, per di più, recentemente CNIPA ha emesso la Deliberazione 18 maggio 2006 n. 34 recante le “Regole tecniche per la definizione del profilo di busta crittografica per la firma digitale in linguaggio XML”..

8.5.2 MODALITA' DI MEMORIZZAZIONE

Riguardo alla modalità di memorizzazione dei documenti in un volume le regole tecniche non forniscono alcun vincolo.

Due sono le macro-opzioni:

- 1 I documenti restano memorizzati nel sistema di gestione che li produce (un database server, un repository basato su prodotti di gestione documentale, ecc.) ed il processo si limita ad individuare i contenuti di ogni volume per associarvi un file di impronte che viene anch'esso memorizzato nel sistema.

Questo approccio è particolarmente interessante quando si tratti di aggiungere le funzionalità di conservazione sostitutiva ad un sistema di archiviazione esistente.

La possibile non obbligatorietà di ricorrere a supporti ottici (vedasi paragrafo 8.4.1.) spiana la strada a questa soluzione, che tra i vantaggi presenta anche quello di mantenere operanti tutte le funzioni di ricerca preesistenti, di norma piuttosto sofisticate e superiori ai requisiti minimi della conservazione.

Lo svantaggio più evidente è che un archivio di conservazione così integrato sarebbe di problematica utilizzazione al di fuori del sistema di gestione che lo produce e mantiene.

- 2 I documenti vengono esportati su volumi costruiti allo scopo. Questo approccio è più semplice dal punto di vista logico ed introduce una netta distinzione tra l'archivio operativo (che resta nella gestione tradizionale) e quello "legale" il cui unico scopo (o almeno lo scopo principale) è quello di adempiere alla conservazione sostitutiva.

I documenti vengono memorizzati in forma di file ben identificati all'interno di una porzione di file system dedicata, esplorabile con le funzioni di base del sistema operativo.

Dovrebbero essere presi accorgimenti per suddividere i file in una appropriata struttura di cartelle onde distribuire il riempimento ed evitare appesantimenti di gestione da parte dei sistemi operativi.

Il file delle impronte viene aggiunto allo stesso file system ed i riferimenti ai singoli documenti possono essere una sorta di link ipertestuale ai documenti effettivi. L'adozione del formato XML e di appropriati fogli di stile rende veramente possibile esplorare un volume con strumenti di base (sistema operativo, browser) senza la necessità di alcuna applicazione specifica.

Questa modalità è anche particolarmente adatta al caso in cui si ricorra effettivamente alla memorizzazione su supporti ottici.

Da quanto sopra si evidenziano vantaggi diversi per entrambi gli approcci.

Sembra ragionevole raccomandare, nel caso di implementazioni basate sull'approccio (1), la disponibilità di funzioni di esportazione (riversamenti diretti) che consentano di produrre volumi organizzati come nel caso (2), decisamente più facili da processare e riacquisire.

8.5.3 DIMENSIONI DEI VOLUMI

Anche su questo argomento nessun vincolo è imposto dalle norme. Non esiste quindi un limite precostituito alla dimensione massima di un volume, intesa sia come quantità di byte che come numero di documenti.

Si può osservare che grandi quantità di dati in senso stretto porrebbero problemi per le operazioni di riversamento, ove i supporti di destinazione non abbiano capacità sufficiente. D'altro canto l'inclusione in un singolo volume di moltissimi documenti, ancorché di piccola dimensione unitaria, significherebbero un numero elevato di record nel file delle impronte e – prevedibilmente – una grande dimensione del file stesso: questo implicherebbe potenzialmente qualche difficoltà per elaborare tale file e tempi significativi per eseguire le operazioni di verifica dell'integrità del volume.

Una raccomandazione ragionevole è quella di contenere la dimensione massima dei dati contenuti in un volume in modo che sia compatibile con lo spazio di memorizzazione su supporti rimovibili di grande diffusione (es. CD, DVD), come pure di contenere il numero di documenti in modo che il file di chiusura risultante non superi una dimensione dell'ordine delle decine di MB.

8.5.4 AGGREGAZIONE DEI DOCUMENTI NEI VOLUMI

Un volume di conservazione sostitutiva di per sé può contenere documenti di qualunque tipologia; tuttavia sembra ragionevole costruire nel tempo volumi che contengano documenti di tipologie omogenee.

Una raccomandazione certamente valida è quella di evitare che documenti distinti ma logicamente associati tra loro (per esempio le immagini multiple di un tomografia) vengano suddivise attraverso due o più volumi, a meno che la cosa non sia assolutamente indispensabile per la ridotta capacità programmata dei volumi.

8.5.5 PROCEDURE DI ACCUMULO E CHIUSURA DEI VOLUMI

A seguito anche delle considerazioni svolte nelle sezioni precedenti si delinea una modalità tipica di gestione del processo di conservazione in una organizzazione.

Si individuano un certo numero di tipologie di documenti da conservare a cui fanno riscontro delle politiche di gestione – massima dimensione di un volume, massimo intervallo di tempo tra due esecuzioni del processo di conservazione – ben determinate. Per ogni tipologia si produrrà dunque una sequenza di volumi pressoché indipendente.

Nell'ambito di una di queste sequenze (si pensi, per esempio, a referti radiologici) avremo un volume in corso di formazione, su cui si accumulano i referti via via prodotti (usciti dalla procedura di consolidamento) in attesa della prossima esecuzione del processo di conservazione, a seguito del quale il volume viene cristallizzato ed effettivamente “conservato”, mentre si apre un nuovo volume di lavoro per accumulare i nuovi referti.

Il processo di conservazione, come noto, prevede alcune operazioni ben definite:

- 1 generazione del file delle impronte; questo potrebbe anche avvenire incrementalmente man mano che i documenti si accumulano; in tal caso dovrà essere eseguita una verifica di integrità per controllare che le impronte calcolate in precedenza corrispondano ai valori già registrati nel file;
- 2 firma digitale del file delle impronte; anche in questo caso si può pensare ad una procedura interattiva, con il Responsabile della Conservazione che siede alla console ed espressamente attiva il processo e firma il file con la propria smartcard, come pure ad un processo totalmente automatico di chiusura del volume ed apposizione della firma digitale. Si veda la sez. 6.1.
- 3 associazione di riferimento temporale; quantunque le regole tecniche non lo specifichino, è quanto mai opportuno che il riferimento in questione sia opponibile ai terzi. L'associazione di una marca temporale è certamente il metodo più semplice e tecnicamente più adatto anche ad una esecuzione totalmente automatica. Tuttavia procedure come la segnatura di protocollo o addirittura procedure basate su registri cartacei possono essere considerati, in funzione dell'assetto organizzativo generale.
- 4 altri adempimenti; sotto questa generica dicitura vanno considerate le attività descritte nell'art. 5 della Delib. CNIPA 11/2004 a carico del Responsabile della Conservazione. In particolare la generazione delle opportune copie di sicurezza, la registrazione dell'avvenuta produzione di un volume, ecc.

8.5.6 INTERVALLI TRA DUE ESECUZIONI DEL PROCESSO DI CONSERVAZIONE

Questo intervallo è in effetti il tempo massimo in cui un singolo documento può restare memorizzato ma non ancora “conservato”.

Per ogni tipologia di documenti dovrà essere trovato il periodo ottimale, ma in generale l'intervallo dovrebbe essere ragionevolmente breve, compatibilmente con l'efficienza delle procedure e con il riempimento dei volumi stessi. L'intervallo minimo potrebbe essere quello di una giornata lavorativa (ma si può scendere al livello di alcune ore, nel caso di flussi molto intensi di documenti e di procedure di chiusura completamente automatiche); l'intervallo massimo potrebbe essere dell'ordine dei 30 giorni, anche se nel caso di documenti consolidati si potrebbe pensare ad intervalli anche più lunghi.

9 ESIBIZIONE DEI DOCUMENTI

Come in precedenza affermato in merito alla conservazione legale della documentazione digitale, anche per la sua esibizione non vi è oggi più motivo alcuno di differenziare fra paziente interno e paziente esterno. Infatti l'esibizione deve essere eseguita dall'unità responsabile della conservazione, con le medesime modalità per il paziente interno e per quello esterno.

9.1.1 REFERTI E IMMAGINI DIGITALI³⁰

È molto importante ricordare che l'informazione medica contenuta nella documentazione referto e immagini non può essere negata al paziente che è, per il Codice in materia di protezione dei dati personali (D. Lgs n. 196/03), la persona fisica a cui si riferiscono i dati. Inoltre l'art. 84 del medesimo Codice asserisce che "I dati personali idonei a rivelare lo stato di salute possono essere resi noti all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a), da parte di esercenti le professioni sanitarie ed organismi sanitari, solo per il tramite di un medico designato dall'interessato o dal titolare. Il presente comma non si applica in riferimento ai dati personali forniti in precedenza dal medesimo interessato. 2. Il titolare o il responsabile possono autorizzare per iscritto esercenti le professioni sanitarie diversi dai medici, che nell'esercizio dei propri compiti intrattengono rapporti diretti con i pazienti e sono incaricati di trattare dati personali idonei a rivelare lo stato di salute, a rendere noti i medesimi dati all'interessato o ai soggetti di cui all'articolo 82, comma 2, lettera a). L'atto di incarico individua appropriate modalità e cautele rapportate al contesto nel quale è effettuato il trattamento di dati". Attraverso questa puntualizzazione si riesce a sfatare la comune convinzione che la documentazione medica possa essere consegnata al paziente solo da un medico. Quando invece dall'art. 84 qui riportato integralmente si evince con chiarezza che incaricati ben individuati (amministrativi, sportellisti) possono essere delegati a trasmettere i documenti direttamente ai pazienti interessati.

Anche il Codice dell'amministrazione digitale (D. Lgs n. 82/05) all'art. 50 riconosce che la disponibilità dei dati deve essere garantita: "1. I dati delle pubbliche amministrazioni sono formati, raccolti, conservati, resi disponibili e accessibili con l'uso delle tecnologie dell'informazione e della comunicazione che ne consentano la fruizione e riutilizzazione, alle condizioni fissate dall'ordinamento, da parte delle altre pubbliche amministrazioni e dai privati".

L'art. 6 della Deliberazione CNIPA n. 11/04 così impone: "Il documento conservato deve essere reso leggibile in qualunque momento presso il sistema di conservazione sostitutiva e disponibile, a richiesta, su supporto cartaceo." Il paziente può quindi espressamente richiedere ed ottenere dalla Struttura sanitaria che la documentazione gli venga consegnata su un supporto diverso da quello su cui gli è stata esibita, previo pagamento di una somma determinata.

Infatti il D. Lgs. n. 196/03 afferma al comma 2 dell'art. 10 che "Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica". Al comma 8 del medesimo articolo viene prevista la corresponsione di un adeguato contributo: "Il Garante può prevedere che il contributo possa essere chiesto quando i dati personali figurano su uno speciale supporto del quale è richiesta specificamente la riproduzione, oppure quando, presso uno o più titolari, si determina un notevole impiego di mezzi in relazione

³⁰ Oggi la documentazione sanitaria informatica di pazienti interni ed esterni viene prodotta al computer, firmata con firma digitale e successivamente sottoposta al procedimento di conservazione legale. L'originale, redatto informaticamente, continua a risiedere nel luogo di archiviazione e poi di conservazione, mentre ciò che circola all'interno e all'esterno della Struttura, sia in forma analogica sia in forma digitale, non è che una sua mera copia.

alla complessità o all'entità delle richieste ed è confermata l'esistenza di dati che riguardano l'interessato".

L'Ufficio del Garante per la protezione dei dati personali, con l'art. 3 della Deliberazione n. 14/2004, sancisce che "Sulla base di una valutazione ponderata delle principali situazioni verificabili, e della circostanza che si tratta anche in questo caso di un contributo, va ritenuto congruo l'importo di euro venti. Si tratta di un importo massimo in quanto, anche in questo caso, il contributo non può comunque eccedere i costi effettivamente sostenuti e documentabili nel caso specifico". Nella Deliberazione il Garante ha voluto così regolare i casi in cui l'interessato chieda che i propri dati siano riversati su particolari "supporti di maggior costo quali audiovisivi, lastre, nastri o altri specifici supporti magnetici". Ma anche dove la gestione della documentazione è totalmente digitale, la richiesta di riversamento delle informazioni sanitarie su supporto analogico da parte del paziente può divenire per la Struttura assai costosa in termini tecnologici, organizzativi e procedurali. E' da ritenersi pertanto che il versamento di un adeguato contributo, da determinarsi di volta in volta da parte della Struttura erogante la prestazione, debba prevedersi anche in caso di richiesta di riversamento dei dati da supporto digitale a cartaceo, seppur quest'ultimo materialmente di irrisorio costo.

L'art. 6, co. 3 della Deliberazione CNIPA n. 11/04 ricorda che "Qualora un documento conservato venga esibito su supporto cartaceo fuori dall'ambiente in cui è installato il sistema di conservazione sostitutiva, deve esserne dichiarata la conformità da parte di un pubblico ufficiale se si tratta di documenti per la cui conservazione è previsto il suo intervento".

10 APPLICAZIONE DELLA DEMATERIALIZZAZIONE NEI SISTEMI CLINICI

Nei capitoli precedenti sono stati analizzati i molteplici temi riguardanti la dematerializzazione della documentazione clinica, con il puntuale richiamo delle norme e con l'aggiunta delle possibili soluzioni tecnologiche ed organizzative per poterla avviare nei contesti del Laboratorio e della Diagnostica per Immagini.

In questo capitolo verranno invece operativamente previsti i passaggi ritenuti necessari per poter dematerializzare i vari documenti, individuandone le fasi ed usufruendo dei concetti sostanziali sin qui riportati.

Le norme e le prassi illustrate nei capitoli precedenti possono apparire molto spesso troppo astratte dalla realtà quotidiana e di difficile implementazione, in quanto eterogenei sono i contesti in cui ci si avvia ad applicare la dematerializzazione dei documenti oggetto di queste linee guida. Per aiutare chi dovrà decidere quali procedure applicare riportiamo un sistema informativo per la dematerializzazione dei referti radiologici e di Laboratorio, partendo dalla sua configurazione più semplice e comunque a norma di legge. Successivamente riporteremo lo scenario per la dematerializzazione delle immagini radiologiche. Sottolineiamo che sarà necessario, prima di applicare la dematerializzazione, effettuare per ogni particolare scenario una accurata analisi del rischio informatico e medico-legale per decidere quale soluzione adottare, che dovrà conseguentemente portare alla stesura di un documento programmatico della sicurezza (DPS), come previsto dalla norma.

Lo spirito che ci ha portati a fare questa sintesi si basa su due semplici concetti: i sistemi informativi adottati devono ottemperare alla normativa vigente e nel contempo devono possedere un grado di sicurezza adeguato all'ambito applicativo e alle informazioni trattate. In particolare ricordiamo che il termine *a norma* si riferisce a sistemi che sono realizzati seguendo espressamente le norme vigenti, mentre il termine *sicurezza* si riferisce a sistemi in cui si è effettuata una accurata analisi del rischio informatico e di quello medico-legale al fine di escluderli o minimizzarli.

Nella descrizione degli use case si inseriranno solo le peculiarità tecniche/organizzative richieste dal legislatore o ritenute indispensabili dagli addetti ai lavori per il processo di dematerializzazione. Verranno qui omessi altri componenti non direttamente riguardanti la dematerializzazione, ma comunque obbligatori per legge, quali ad esempio quelli richiesti dalle norme sulla privacy. Si sottolinea quindi che le sole implementazioni descritte non sono sufficienti a ritenere un sistema a norma nella sua globalità.

Per rendere l'esposizione più chiara ed efficace, sarà utilizzato il formalismo di cui si avvalgono già le linee guida IHE, introducendo quindi la descrizione UML³¹ dei vari scenari, con l'individuazione degli indispensabili attori coinvolti, definiti come i sottosistemi informativi aventi ben determinate funzionalità, che, a seconda che si trattino referti o immagini diagnostiche, nello specifico qui debbono essere:

³¹ UML (Unified Modeling Language, "linguaggio di modellazione unificato") è un linguaggio di modellazione e specifica basato sul paradigma object-oriented. Il nucleo del linguaggio fu definito nel 1996 da Grady Booch, Jim Rumbaugh e Ivar Jacobson sotto l'egida dello OMG, che tuttora gestisce lo standard di UML. Il linguaggio nacque con l'intento di unificare approcci precedenti (dovuti ai tre padri di UML e altri), raccogliendo le best practices nel settore e definendo così uno standard industriale unificato.

- **Report Creator:** il sistema informativo che è in grado di redigere un referto; nel mondo reale un sistema RIS o un sistema LIS hanno al loro interno questa precisa funzionalità;
- **Acquisition Modality:** ogni sistema informativo di acquisizione e produzione di immagini diagnostiche, quali Tomografi Computerizzati, sistemi di Radiografia Digitale, Ecografi, Tomografi a Risonanza Magnetica, ecc.;
- **Image Manager/Image Archive:** sistema informativo di gestione e memorizzazione delle immagini diagnostiche, quale ad esempio un archivio PACS;
- **Time Server:** un sistema che è in grado di fornire un tempo certo, sincronizzato con una precisione almeno del secondo. Si consiglia a questo proposito di utilizzare, ove possibile, le indicazioni tecnologiche contenute nel profilo di integrazione IHE Consistent Time (Technical Framework ITI)³².

Si noti che questo organo eroga l'informazione di tempo da utilizzare per contrassegnare l'ora di applicazione delle firme digitali (signing time) e per la registrazione (logging) di tutte le operazioni significative. La precisione di questo servizio è di evidente e fondamentale importanza, mentre la disponibilità di un livello di certificazione della sua qualità aumenta l'attendibilità delle registrazioni.

- **Certification Authority (CA):** un service provider in grado di erogare il servizio di emissione di certificati di chiave pubblica per la firma digitale ed eventualmente per altre applicazioni come ad esempio l'autenticazione forte. La CA eroga anche il servizio di pubblicazione dello stato di sospensione e revoca dei certificati di propria emissione.

Si assume in questo contesto che la CA sia gestita da un Certificatore accreditato presso il CNIPA³³; onde assicurare la massima valenza giuridica dei certificati utilizzati.

In conseguenza della normativa vigente il Certificatore ha anche la responsabilità della personalizzazione dei dispositivi di firma (smartcard e simili) distribuiti, nonché quella di realizzare procedure accurate per l'identificazione dei titolari di certificato e l'associazione tra il titolare ed il dispositivo assegnato.

- **Time Stamping Authority (TSA):** Un sistema in grado di erogare il servizio di validazione temporale dei documenti da dematerializzare³⁴.
- **Sistema di Archiviazione:** sistema informativo in grado di garantire il procedimento di archiviazione secondo la Deliberazione CNIPA n.11/04; questo sistema può essere inglobato all'interno del sistema di conservazione, tuttavia si mantiene separato per evidenziare il suo importante ruolo per la classificazione documentale;
- **Sistema di Conservazione:** sistema informativo in grado di garantire il procedimento di conservazione secondo la Deliberazione CNIPA n.11/04.

Commento [1]: Manca nei vari capitoli precedenti la definizione di validazione temporale! ----
13/09/2006, 08.39----Claudio Saccavini

³² Il profilo Consistent Time IHE è descritto a pag. 45 e ss nel Technical Framework ITI

(http://www.ihe.net/Technical_Framework/upload/ihe_iti_tf_2.0_vol1_FT_2005-08-15.pdf)

³³ I Certificatori accreditati sono soggetti pubblici o privati che emettono certificati qualificati conformi alla normativa europea e nazionale in materia. Inoltre ai sensi della normativa vigente, hanno richiesto ed ottenuto il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza. Forniscono i servizi di certificazione inerenti la firma digitale e possono rilasciare certificati di autenticazione per conto delle pubbliche amministrazioni che rilasciano smart card conformi alla Carta nazionale dei Servizi (CNS).(http://www.cnipa.gov.it/site/it-IT/Attivit%c3%a0/Certificatori_accreditati/)

³⁴ Si faccia riferimento al Codice dell'amministrazione digitale, Capo 1, , Sezione I, ed alle successive norme tecniche.

10.1 DEMATERIALIZZAZIONE DEI REFERTI

Per aiutare la comprensione del procedimento di dematerializzazione dei referti radiologici e di Laboratorio si descrive in figura 10.1 il flusso necessario a tale scopo.

Il Report Creator provvede a redigere il referto secondo le proprie logiche e nel proprio contesto, (RIS o LIS) (1). Successivamente provvede ad apporre la firma digitale al documento prodotto, seguendo tutta la procedura prevista dalle norme ed esplicitata nei capitoli precedenti, inclusa l'autenticazione del sottoscrittore sulla smart card (2-3). Il referto così formato viene sottoposto a memorizzazione, ovvero viene salvato nel Report Creator. I referti firmati con firma elettronica qualificata esistono giuridicamente da questo momento.

Successivamente, in un tempo congruo con le esigenze specifiche del contesto di applicazione, si sottopongono i referti firmati al processo di conservazione ottica sostitutiva (4). Il passaggio dei referti dal sistema Report Creator al sistema di conservazione può essere eseguita secondo qualsiasi protocollo, tuttavia si consiglia di utilizzare uno standard, come un messaggio HL7 di tipo ORU o MDM, oppure un messaggio Document Submission XDS.

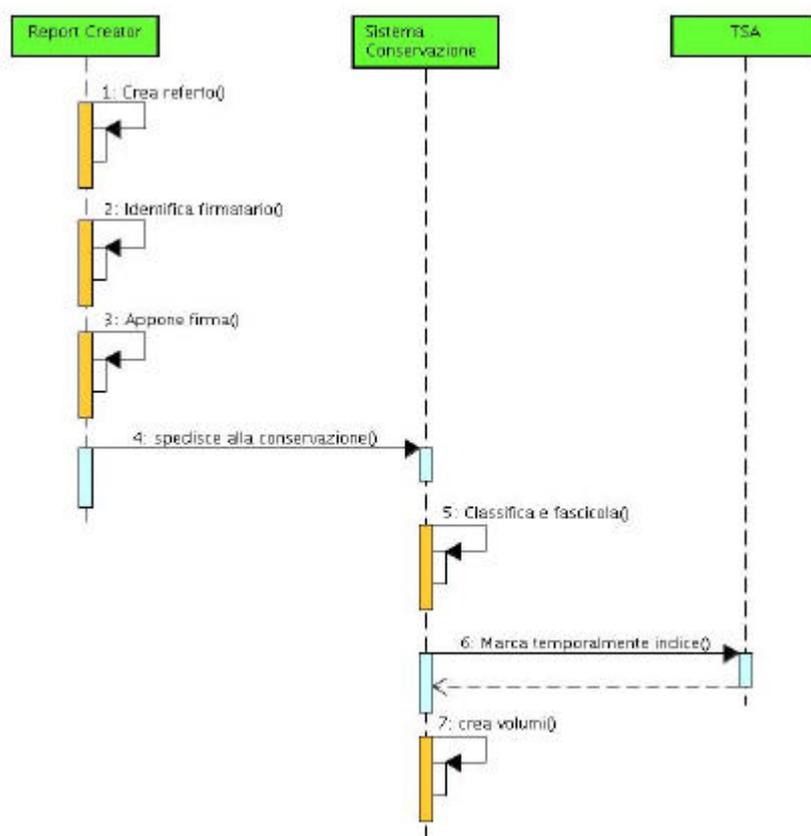


Figura 10.1: diagramma di sequenza del processo di dematerializzazione

Dopo avere ricevuto i referti firmati il sistema di conservazione sottopone i documenti al processo di classificazione e fascicolazione, escludendo gli eventuali referti che non abbiano le caratteristiche richieste da tali procedure (quali ad esempio quelli in cui sia omesso qualche dato essenziale come l'identificativo univoco del paziente) (5). È importante sottolineare che i

documenti che non superano positivamente il processo di classificazione e fascicolazione, come descritto in un precedente capitolo, devono essere gestiti nel cosiddetto *scarto*. Il procedimento di fascicolazione porta alla generazione di un volume di referti identificato da un file indice. Al file indice vengono quindi apposti un riferimento temporale opponibile ai terzi, cioè una marca temporale (6) da richiedersi ad una TSA, e la firma digitale del Responsabile della conservazione sostitutiva. E' importante ricordare che quest'ultimo ruolo è di fondamentale importanza per il raggiungimento degli scopi della gestione documentale e della dematerializzazione; egli va espressamente individuato e formalmente nominato, tenendo conto anche delle caratteristiche approfondite da un apposito Tavolo di lavoro del CNIPA in materia.



Figura 10.2: use case Responsabile della Conservazione

I dati così trattati verranno riversati su un idoneo supporto e da questo momento saranno conservati legalmente in modo sostitutivo per i tempi prescritti dalle specifiche normative di riferimento (7).

E' necessario a questo punto sottolineare che sotto l'aspetto organizzativo, una volta individuati il flusso documentale interno, i sistemi ed i soggetti coinvolti, vanno anche attivate le procedure per la gestione dell'infrastruttura dei certificati, delle chiavi pubbliche e dei dispositivi di firma (smart card).

In particolare deve essere individuata una Certification Authority (CA), la quale provveda ad emettere i dispositivi di firma con inserite le chiavi di firma, oltre che a garantire l'associazione in maniera univoca della chiave privata ad un ben preciso soggetto (Firmatario) e ad emettere il relativo certificato.



Figura 10.3 : Rapporto firmatario e CA

Inoltre è alla Certification Authority che il Firmatario dovrà rivolgersi per la risoluzione di qualsiasi problema inerente il proprio dispositivo di firma: nel caso di rinnovo del certificato per naturale scadenza dello stesso, oppure in caso di smarrimento o di furto. Soprattutto in questi due ultimi casi il firmatario dovrà prendere contatto con la CA ed informarla immediatamente, affinché essa provveda a sospendere o revocare tempestivamente il certificato di firma.

Lo use case sopra descritto rappresenta la configurazione minimale atta a garantire un sistema per la dematerializzazione dei referti a norma. Tuttavia il sistema così com'è strutturato presenta una molteplicità di lacune sul piano della sicurezza. Nei seguenti paragrafi si andranno ad analizzare una serie di misure di sicurezza che aiuteranno a limitare o ad annullare i rischi derivanti dalla dematerializzazione dei referti.

Una differenza sostanziale fra la firma autografa e quella digitale risiede nei requisiti necessari alla associazione dei dispositivi elettronici utilizzati dal firmatario, o meglio sta nella necessità di legare indissolubilmente una sequenza di bit ad una persona fisica. La soluzione adottata dalla norma, già ampiamente descritta in queste linee guida, è rappresentata dalla coppia chiave privata/chiave pubblica e dal relativo certificato che la CA emette, garantendo l'associazione ad una ben determinata e formalmente identificata persona fisica. Purtroppo questo legame, che era "biologico" nella firma tradizionale, diventa ora elettronico. Nasce pertanto l'esigenza forte di collocare nel tempo il momento in cui la suddetta associazione firma-firmatario era garantita come sussistente e legalmente valida. Poiché detta associazione ed il tempo della sua validità non sono ancorabili a certezze biologiche e naturali, affidabilità e sicurezza del sistema devono poter essere ottenute tecnologicamente. A titolo di esempio, si pensi alla chiave privata serbata sulla smart card: la norma impone che vi sia un rigoroso dovere di custodia da individuarsi in capo al titolare e che il supporto sia diligentemente custodito dal titolare della firma stessa. Ma il supporto fisico può essere smarrito o sottratto, mettendo in serio pericolo la certezza della connessione automatica fra la firma ed il firmatario, il quale deve essere quindi messo nella possibilità di richiedere immediatamente l'annullamento o la sospensione dell'associazione. E' così che il tempo informatico diviene un elemento di fondamentale importanza giuridica e probatoria.

Consistent Time

Si deve preliminarmente osservare che, per la validità giuridica della scrittura privata-referto, il legislatore non prevede quali elementi essenziali la data e l'ora di composizione e firma del documento. Il momento temporale è ritenuto invece come necessario se si vogliono soddisfare pretese probatorie. Anche leggendo con attenzione il caso d'uso sopra esposto, si può notare come non vi sia imposizione normativa o necessità di associare un tempo alla firma del referto, in modo da poter definire con certezza il momento in cui esso è stato firmato. E' evidente che questa mancanza cozza con le esigenze proprie dei sistemi informativi che gestiscono i referti e tutte le informazioni cliniche, dove invece la fedele sequenzialità degli eventi è sentita come principio nodale. Si pensi al caso paradossale dove, a causa di un disallineamento degli orologi dei sistemi, le immagini radiologiche abbiano un momento temporale successivo a quello del referto, invero frutto della loro interpretazione clinica.

Per superare un tale problema è stato introdotto un apposito profilo di integrazione proposto da IHE, ovvero il Consistent Time (CT), descritto nel Technical Framework del dominio ITI. La semplice soluzione, basata sul protocollo "network time" largamente utilizzato, permette di allineare in modo preciso gli orologi di tutti i sistemi informativi sanitari coinvolti. Il beneficio di adottare questa soluzione per la dematerializzazione è quello di poter essere ragionevolmente garantiti che le informazioni temporali inserite in modo automatico all'interno dei documenti generati dai sistemi siano coerenti con il flusso del paziente.

E' più che evidente che il Consistent Time non è elemento o sistema previsto dalla norma ai fini della corretta dematerializzazione della documentazione clinico-sanitaria. Esso è però una valida misura di sicurezza adottabile nel trattamento delle informazioni. Tuttavia, il tempo così ottenuto non è previsto dalla norma come un elemento di prova "opponibile ai terzi", e deve essere invece classificato come una prova semplice³⁵.

Signing Time

Inoltre, per aumentare la sicurezza del sistema sopra descritto, in modo completamente automatico e non modificabile dall'utente, all'atto dell'apposizione della sottoscrizione si può inserire un attributo interno alla stessa firma digitale, contenente la data e l'ora in cui viene

³⁵ E' bene sottolineare come la non opponibilità ai terzi non significhi che il tempo così ottenuto, - da un punto di vista probatorio - non valga nulla. Varrà infatti come presunzione semplice (che è una prova) e come tale potrà essere discrezionalmente utilizzata e riconosciuta dal giudice a supporto di una sua ipotetica decisione (ovviamente contro di essa potrà farsi valere la prova contraria).

apposta. Così siamo in grado di legare in modo molto stretto il documento al dato temporale, garantendolo proprio con la stessa firma digitale da possibili successive alterazioni. Tale attributo, denominato "signing time", è previsto nella stessa firma digitale, e la sua apposizione è sincrona al processo di sottoscrizione, ovvero si riferisce in modo indissolubile ad essa. Si tratta di un forte elemento per l'aumento della sicurezza del sistema, ma non è oggetto di imposizione normativa alcuna e comunque non è annoverabile fra le prove opponibili ai terzi.

Validazione temporale

La norma³⁶ prevede di poter applicare al documento alternativamente ben quattro tipi di riferimento temporale che, a differenza di quelli descritti nei paragrafi precedenti, possa essere considerato una prova opponibile ai terzi.

La segnatura di protocollo e la posta elettronica certificata risultano di difficile applicazione pratica ai casi trattati in queste linee guida e quindi non verranno presi in considerazione qui, anche se effettivamente previsti dalla norma. Per quanto riguarda la conservazione ottica sostitutiva si può affermare che, per la tipologia di documenti qui trattati (referti e immagini), vi è l'obbligo normativo di sottoporli sempre e comunque a tale procedimento di validazione temporale. Tuttavia il tempo che intercorre fra la firma del documento e l'avvio del processo di conservazione può essere ritenuto troppo lungo e quindi far propendere per un ulteriore livello di sicurezza, introducendo nel flusso anche l'elemento della marca temporale.

Tutti i procedimenti di validazione temporale sono asincroni rispetto a quello di sottoscrizione, ovvero sono effettuati in un momento diverso e sicuramente successivo al processo di firma. La validazione temporale è quindi in grado di dare la certezza che il referto già firmato esiste (dal punto di vista probatorio con riconoscimento di opponibilità ai terzi) a partire dal momento in cui viene applicata al documento; ma non esclude, anzi, che il documento sia esistito precedentemente, fino a prova contraria (prova semplice).

La validazione temporale mediante apposizione di marca temporale ad un documento informatico equivale quindi alla determinazione della data certa, che nel nostro ordinamento si può ottenere per la documentazione analogica nei previsti seguenti modi: con la morte del soggetto, con l'accertamento giudiziale, con la sottoposizione dello scritto alla formalità di registrazione presso l'Ufficio del Registro, con la vidimazione presso notaio o altro ufficio pubblico.

Dal parallelismo con l'ambito analogico appena qui sopra riportato, si evince facilmente che la marca temporale riguarda il tempo, non concerne la firma. Quindi la marca non deve essere assolutamente intesa come un metodo o un mezzo per il disconoscimento della firma. Come assai ben chiarito nell'apposito capitolo sulla "Valenza probatoria del documento informatico sottoscritto" delle presenti linee guida, attraverso apposito procedimento, il titolare potrà avviare il disconoscimento della firma digitale solo giudizialmente, portando la prova che essa non è a lui riconducibile.

³⁶ Il DPCM 13.1.04, all'art.1, co.1, così recita: "g) riferimento temporale, informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici; h) validazione temporale, il risultato della procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi; i) marca temporale, un'evidenza informatica che consente la validazione temporale". L'art.1, co.1, lett. bb del D.lgs n.82/05 reitera il concetto asserendo che la validazione temporale è "il risultato della procedura informatica con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi".

L'art.39 del DPCM 13.1.04 prevede, oltre alla marca temporale, altri tre sistemi per utilizzare la validazione temporale che sia opponibile ai terzi: "a) il riferimento temporale contenuto nella segnatura di protocollo di cui all'art. 9 del decreto del Presidente del Consiglio dei Ministri, 31 ottobre 2000, pubblicato nella Gazzetta Ufficiale 21 novembre 2000, n. 272; b) il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti in conformità alle norme vigenti; c) il riferimento temporale ottenuto attraverso l'utilizzo di posta certificata ai sensi dell'art. 14 del testo unico.

Verifica del potere di firma

Come si è visto nel precedente paragrafo, un punto assai delicato per tutta la sicurezza del sistema di dematerializzazione è la verifica della validità del certificato di firma e il conseguente posizionamento nel tempo del documento firmato. Ovvero si parla della situazione in cui un certificato di firma risulta scaduto, revocato o sospeso ed il referto firmato non posizionabile nel tempo per poter provare che era stato firmato prima della scadenza/sospensione/revoca del certificato.

L'art.21 del D.lgs n.82/05 asserisce che "3. L'apposizione ad un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico revocato, scaduto o sospeso equivale a mancata sottoscrizione. La revoca o la sospensione, comunque motivate, hanno effetto dal momento della pubblicazione, salvo che il revocante, o chi richiede la sospensione, non dimostri che essa era già a conoscenza di tutte le parti interessate". Resta affidato alla libera valutazione del Giudice il riconoscimento della rispondenza di un tale documento al requisito della forma scritta (art. 20, co. 1 bis, D.lgs n. 82/05) e se utilizzarlo ugualmente a scopi probatori. Ancora al Giudice viene riconosciuta comunque la facoltà di accertare, anche attraverso altri mezzi di prova, la conformità dei fatti e delle cose rappresentate nel documento.

Per evitare l'insorgenza di un simile problema interpretativo, un approccio è sicuramente quello di apporre un riferimento temporale al documento firmato, in modi e tempi descritti nei precedenti paragrafi. Ma al fine di scongiurare l'eventualità di dover gestire a posteriori la valenza giuridica, probatoria e quindi anche clinica di un documento sottoscritto con firma avente certificato scaduto/revocato/sospeso, vi è la possibilità di verificare la validità del certificato al momento della apposizione della firma stessa. Normalmente (ed è buona regola che ciò sempre avvenga, anche perché imposto dalla normativa vigente) i sistemi RIS e LIS verificano sempre, mediante il controllo degli accessi, le credenziali dell'utente, in modo da poter verificare immediatamente se egli è abilitato a sottoscrivere. Se a questa usuale procedura si aggiunge anche la verifica della validità del certificato di firma, allora si è in grado di stabilire con certezza non solo che il soggetto aveva le credenziali per poter firmare, ma anche che il suo certificato di firma era valido al momento della firma stessa (potere di firma). Questa è una misura di sicurezza di fondamentale importanza in quanto, unitamente all'apposizione del riferimento temporale sul referto, ci permette di essere sicuri che il referto redatto e firmato sia, dal punto di vista clinico (nei tempi) e medico-legale (nella validità), un documento che possiamo tranquillamente distribuire ai soggetti interessati.

I modi operativi per realizzare la verifica del potere di firma sono molteplici, ma purtroppo attualmente non normati.

Registration Authority

Si è precedentemente visto che un ruolo importantissimo nella dematerializzazione viene rivestito dalla Certification Authority, soprattutto nella gestione della vita dei certificati di firma. Molto spesso può essere utile affiancare alla CA anche un organismo organizzativo (Registration Authority – RA), interno alla Struttura sanitaria, il quale gestisca le attività di emissione dei dispositivi di firma e di sospensione/revoca dei certificati associati. Questo approccio organizzativo può risultare molto vantaggioso in quanto l'ambito di utilizzo dei dispositivi di firma che si sta trattando è ben preciso e indissolubilmente legato al rapporto contrattuale fra il medico firmatario e la Struttura sanitaria. Inoltre il datore di lavoro può unilateralmente revocare o sospendere l'uso delle smart card di un soggetto all'interno della propria struttura, così come, in base all'art.32, co.3, il Certificatore che rilascia i certificati qualificati di firma deve "g) procedere alla tempestiva pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del titolare o del terzo dal quale derivino i poteri del titolare medesimo". Molto spesso ove si è proceduto all'istituzione della Registration Authority interna alla struttura sanitaria, ci si è appoggiati operativamente alle unità dei Sistemi Informativi o dell'Ufficio Personale, i quali hanno gestito in modo parallelo sia il badge personale che il dispositivo di firma. Dal punto di vista della

sicurezza, la presenza di una RA all'interno della Struttura sanitaria rappresenta un notevole valore aggiunto per permettere di ottenere tempestive revoche/sospensioni dei certificati di firma, ma soprattutto immediate revoche/sospensioni del potere di firma. Per meglio comprendere questo punto basti pensare ad un medico, appartenente ad una determinata Struttura sanitaria e titolare di un certificato di firma emesso da una CA a livello Regionale, il quale si trasferisca in un'altra Struttura della stessa Regione: il certificato di firma rimarrà valido anche dopo il trasferimento, ma il potere di firma dovrà assolutamente essergli revocato nella prima Struttura ed eventualmente attivato presso la seconda.

Archiviazione elettronica

Questo procedimento spesso viene trascurato nei sistemi di dematerializzazione, soprattutto perché non obbligatorio per la norma. Onde fare chiarezza appare necessario portare alcune astratte definizioni e qui interpretarle e calarle nell'ambito sanitario che ci interessa. La norma (Deliberazione CNIPA n.11/04, art.1, co.1, lett.f) definisce *memorizzazione* "il processo di trasposizione su un qualsiasi idoneo supporto, attraverso un processo di elaborazione, di documenti analogici o informatici, anche sottoscritti". Nei sistemi RIS e LIS questo è da vedersi come il procedimento di salvataggio del referto firmato. Altresì la medesima Deliberazione definisce l'*archiviazione elettronica* come "il processo di memorizzazione, su un qualsiasi idoneo supporto, di documenti informatici, anche sottoscritti, univocamente identificati mediante un codice di riferimento, antecedente all'eventuale processo di conservazione". Parrebbe che l'unica differenza sia legata al codice univoco, ma in effetti si può individuare qualche elemento in più: in effetti per conservare analogicamente o elettronicamente i referti bisogna che essi siano sottoposti prima al processo di classificazione e fascicolazione. In particolare l'attività di classificazione appare essere molto delicata, perché prevede di entrare nel merito del documento, con verifica della presenza al suo interno degli elementi ritenuti necessari quali nome del paziente, identificativo univoco del paziente, etc. Se pensiamo ad uno scenario, normativamente plausibile, in cui tutta la conservazione ottica sostitutiva dei documenti da dematerializzare venga effettuata all'esterno della Struttura sanitaria, risulta difficile ipotizzare che attività preliminare di questo procedimento sia anche lo svolgimento della verifica degli elementi previsti dalla classificazione. Risulta quindi una buona regola di sicurezza l'inserimento di un sistema di archiviazione, interposto fra la memorizzazione (sistema RIS o LIS) ed il sistema di conservazione ottica sostitutiva, al fine di supportare correttamente proprio le funzionalità della classificazione.

10.2 DEMATERIALIZZAZIONE DELLE IMMAGINI RADIOLOGICHE

Per chiarezza e coerenza con i profili IHE Radiologia attualmente in uso nella quasi totalità dei sistemi di produzione delle immagini diagnostiche e nei relativi sistemi di gestione, si mutueranno qui alcuni attori direttamente dal profilo Radiology Scheduled Workflow (SWF).

Riprendendo proprio quest'ultimo profilo, dopo l'acquisizione, le immagini diagnostiche vengono spedite al sistema di gestione e di memorizzazione (Image Archive). Risulta evidente che sia il formato delle immagini sia il protocollo di comunicazione devono essere DICOM in accordo con le specifiche tecniche contenute nel profilo IHE SWF.

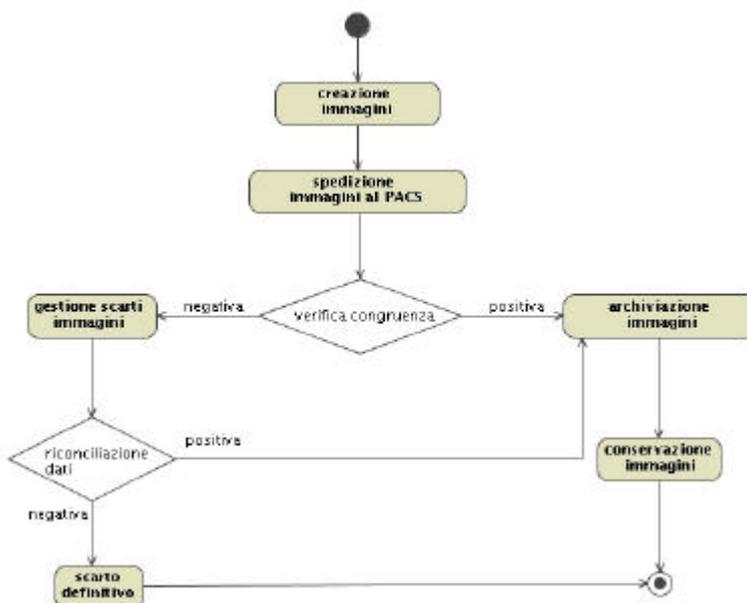
Come già più sopra sottolineato in tema di referti, è fondamentale che, prima della fase di acquisizione (Creazione Immagini), la modalità abbia sincronizzato il suo tempo in modo da realizzare la coerenza temporale con tutti gli altri sistemi in gioco (Maintain Time).

In un momento successivo, le immagini verranno spedite al sistema di archiviazione (Archiviazione), il quale provvederà alla loro verifica di coerenza e ad eventuali correzioni e/o aggiunte. Tale processo mira ad allineare il contenuto dell'intestazione DICOM (header dei file DICOM) ai dati realmente contenuti nei vari sistemi informativi aziendali (generalmente RIS), al fine di non permettere la conservazione di documenti immagine privi delle informazioni necessarie alla loro gestione successiva (vedi ad esempio mancanza di identificativi del paziente, etc.).

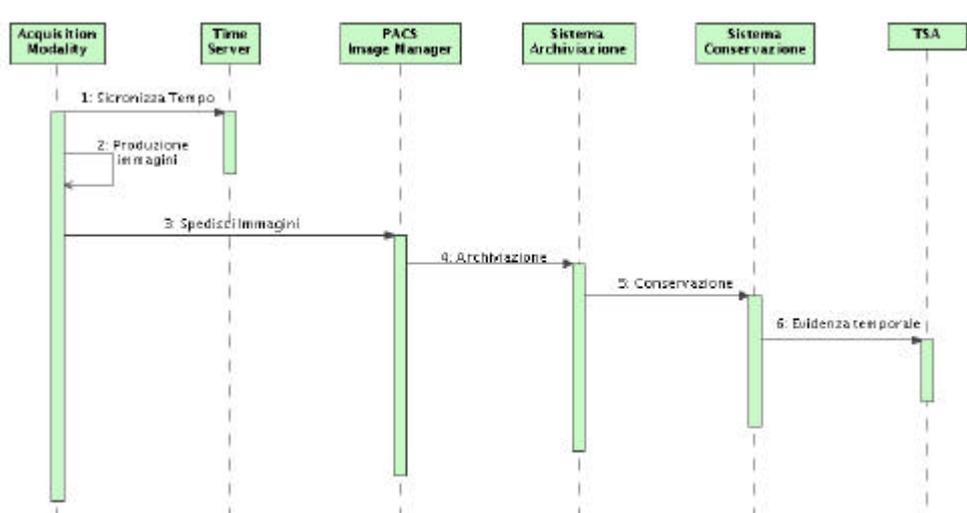
Risulta evidente che bisognerà adottare delle procedure per la gestione di queste non conformità, facendo sì che si possa provvedere a modificare i dati incorretti o ad aggiungere quelli mancanti. Inoltre dovrà essere gestita la possibilità che esistano delle situazioni in cui le immagini prodotte debbano essere scartate dal processo di archiviazione per impossibilità di effettuare le operazioni di riconciliazione.

Infine si provvede a sottoporre i documenti immagine alla conservazione, in analogia con quanto precedentemente esposto. Risulta evidente che tutte le immagini spedite all'Image Manager/ Image Archive devono essere sottoposte alla procedura di conservazione.

Si noti l'importanza della procedura di verifica della congruenza dei dati contenuti nell'immagine radiologica: molto spesso le informazioni anagrafiche sono inserite nella apparecchiatura radiologica direttamente dal Tecnico Sanitario di Radiologia Medica, con elevato margine di errore. Da alcuni dati di letteratura e da esperienze maturate dagli autori risulta che circa il 3% delle informazioni inserite manualmente risulta errato.



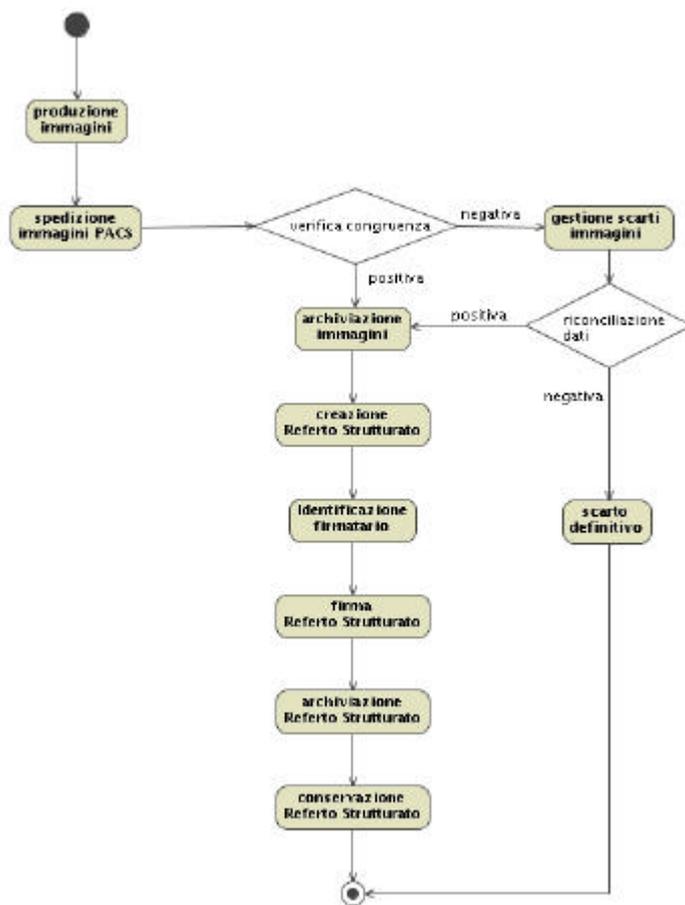
Lo stesso scenario è riportato in un diagramma sequenziale.



10.3 DEMATERIALIZZAZIONE DEL REFERTO RADIOLOGICO STRUTTURATO

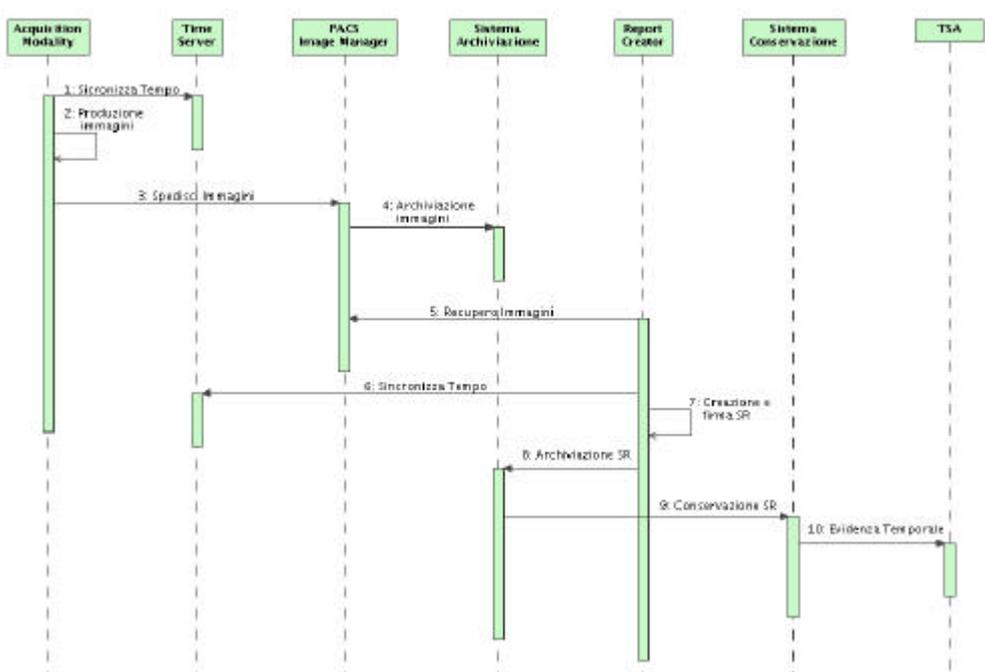
Si definisce Referto Strutturato un documento informatico in formato CDA o DICOM contenente delle informazioni testuali (come nel tradizionale referto radiologico) strutturate insieme ad informazioni iconografiche. Il documento informatico così ottenuto è una fusione fra il referto radiologico e la documentazione iconografica, fissando la relazione fra le due diverse entità in modo da renderle inscindibili. Tale documento per essere dematerializzato deve obbligatoriamente essere firmato digitalmente e conservato a tempo illimitato.

Riportiamo qui sotto il diagramma di flusso per la dematerializzazione del referto strutturato.



Si presume che il Servizio di Radiologia che gestisce il referto strutturato abbia un sistema RIS/PACS ad alto livello di integrazione che gli permetta di produrre questi documenti informatici. In ogni caso valgono le considerazioni fatte per la dematerializzazione del referto radiologico, ovvero la differenziazione fra essere parte o meno di un sistema informativo aziendale che risponde a precisi requisiti di sicurezza.

Sotto riportiamo il diagramma sequenziale di questo caso d'uso.



Si noti che le immagini radiologiche che non concorrono alla documentazione del referto strutturato, ovvero che non sono "contenute" nello stesso, vengono sottoposte a procedimento di archiviazione e mantenute in questo stato per almeno cinque anni.

11 NORMATIVA E LINEE GUIDA DI RIFERIMENTO

11.1 NORMATIVA DI RIFERIMENTO DI CARATTERE GENERALE

- Codice di Deontologia Medica
- Codice Civile
- Codice Processuale Civile
- Codice dei beni culturali e del paesaggio D.Lg. 22 gennaio 2004, n.242.
- Circolare Ministero della Sanità, n. 61 del 19 dicembre 1986
- D. L.gs n. 196/03
- Allegato B del D. L.gs n. 196/03
- L. n.59/97
- D. L.gs n.82/05, Codice dell'amministrazione digitale
- D. L.gs n. 159/06, Disposizioni integrative e correttive al D. L.gs n.82/05
- Technical Framework IHE

11.2 NORMATIVA DI RIFERIMENTO PER DOCUMENTAZIONE DI DIAGNOSTICA PER IMMAGINI

- D. P. R. n. 128/1969
- Circolare del Ministero della Sanità n. 61/86
- D. L.gs n. 230/1995
- D. M. 14.2.1997
- Direttiva 97/43/EURATOM
- D. L.gs n. 187/2000
- PACS-Italia, Società Italiana di Radiologia Medica (cap.1.6, La documentazione per il paziente. Aspetti legali)

11.3 NORMATIVA DI RIFERIMENTO PER REFERTI DI LABORATORIO DI ANALISI

- D.P.R. n. 128/1969
- Circolare del Ministero della Sanità n. 61/86
- D.P.C.M. 10.2.84

11.4 NORMATIVA DI RIFERIMENTO PER FIRMA DEI DOCUMENTI

- Direttiva 1999/93/CE
- DPCM 13.1.04
- Deliberazione CNIPA n.11/04
- D. L.gs n.82/05, Codice dell'amministrazione digitale
- EESSI (European Electronic Signature Standardization Initiative)

11.5 NORMATIVA DI RIFERIMENTO PER CONSOLIDAMENTO

- DPCM 13.1.04
- Deliberazione CNIPA n.11/04
- D. L.gs n.82/05, Codice dell'amministrazione digitale

11.6 NORMATIVA DI RIFERIMENTO PER CONSERVAZIONE SOSTITUTIVA

- EESSI (European Electronic Signature Standardization Initiative)
- Deliberazione CNIPA n.11/04

11.7 NORMATIVA DI RIFERIMENTO PER L'ESIBIZIONE

- D. L.gs n. 196/03
- D. L.gs n.82/05, Codice dell'amministrazione digitale
- Deliberazione CNIPA n. 11/04
- Deliberazione n. 14/2004 Ufficio del Garante privacy

12 GLOSSARIO

Di seguito si riporta un glossario dei termini utilizzati nel documento.

Termine	Definizione
Archiviazione immagini	Processo di registrazione di immagini su appositi sistemi per la successiva conservazione, con contemporanea attribuzione ad ognuna di esse di un unico codice identificativo (processo antecedente alla conservazione)
Certificato di firma digitale	Attestato elettronico che collega i dati utilizzati per verificare la firma digitale al titolare, confermandone l'identità informatica dello stesso
Certificato qualificato di firma digitale	Certificato di firma digitale conforme ai requisiti di cui all'allegato I della direttiva 1999/93/CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva (i certificatori di cui all'elenco pubblico gestito dal CNIPA soddisfano tutti a tali requisiti)
Classificazione	Attribuzione a ciascun documento di una classifica che lo inserisce all'interno di un piano di classificazione (si veda 'Titolario'), consentendo di contestualizzarlo, capirne la funzione, metterlo in relazione con gli altri documenti appartenenti allo stesso procedimento e garantirne la reperibilità nel tempo
Conservazione sostitutiva	Processo di memorizzazione dei documenti informatici, e/o delle immagini dei documenti analogici direttamente sui supporti ottici, che termina con l'apposizione, sull'insieme di quanto memorizzato, della firma digitale da parte del responsabile della conservazione, che attesta il corretto svolgimento del processo e di una marca temporale. Il processo di conservazione sostitutiva di documenti analogici originali unici si conclude con l'ulteriore apposizione del riferimento temporale e della firma digitale da parte di un pubblico ufficiale per attestare la conformità di quanto memorizzato al documento d'origine. Questo processo è impiegato per conservare nel tempo i documenti garantendone disponibilità, integrità e autenticità
Consolidamento del documento	Processo per collegare l'esistenza del documento firmato ad un istante di tempo certo e dimostrabile
CRL Certificate Revocation List	Elenco dei certificati non più validi, revocati o sospesi (CSL), pubblicato periodicamente a cura del certificatore che li ha emessi
Dematerializzazione	Trasformazione della documentazione clinica testuale e iconografica in formato digitale
Documento analogico	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).
Documento informatico	Nella sua accezione più comune corrisponde a un documento cartaceo Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti. Di fatto documento che viene generato in formato digitale e vive come tale: può essere firmato elettronicamente o non firmato
Esibizione documenti	Processo per rendere disponibili dati personali sullo stato di salute al paziente
Firma elettronica non qualificata (leggera)	Insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica
Firma elettronica qualificata	Firma elettronica ottenuta attraverso una procedura informatica che garantisce la connessione univoca al firmatario, creata con mezzi sui quali il firmatario può conservare un controllo esclusivo e collegata ai dati ai quali si

	riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati, che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma
Firma digitale	Particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Iconografia	Immagine a supporto del referto medico
Identity Management	Capacità di un sistema informativo di radiologia di identificare un soggetto e di assegnare a questo un ruolo nel sistema stesso
Immagine analogica	Immagine in formato cartaceo
Immagine digitale	Immagine in formato elettronico
Marca Temporale	Informazione opponibile a terzi, contenente la data e l'ora, che viene associata ad uno o più documenti informatici La Marca Temporale è associata al/ai documento/i informatico/i e rilasciata a cura di un certificatore
Marcatura temporale	Procedura informatica per l'apposizione di una 'marca' al documento informatico, contenente alcuni dati tra i quali la data e l'ora di creazione del documento, con la sottoscrizione digitale da parte di un Certificatore
PACS Picture Archiving and Communication System	Sistema per l'archiviazione e la presentazione di immagini del settore biomedico
Protocollo DICOM (Digital Imaging and Communication in Medicine)	Criteri per la comunicazione, visualizzazione, archiviazione e stampa di informazioni di tipo biomedico quali ad esempio immagini radiologiche
Referto radiologico	Documento testuale contenente i risultati dell'atto medico radiologico
Referto strutturato	Referto caratterizzato dalla commistione di testo e immagini rilevanti per la diagnosi
Scarto documenti	Processo di smaltimento di documenti attuabile all'esaurimento dell'utilità giuridico-amministrativa degli stessi e con la mancanza di apprezzabile interesse come fonte storica
Scrittura privata	Documento analogico o informatico sottoscritto rispettivamente con firma chirografa o firma digitale
Scrittura privata riconosciuta	Documento analogico o informatico che fa piena prova sino a querela di falso (c.p.c. 221) della provenienza delle dichiarazioni di chi lo ha sottoscritto (es. scritture private la cui sottoscrizione autenticata da notaio o altro pubblico ufficiale a ciò autorizzato; scritture private la cui sottoscrizione è riconosciuta da colui contro il quale esse sono prodotte; scritture private la cui sottoscrizione, già disconosciuta da colui contro il quale esse sono prodotte, sia state positivamente sottoposta a processo di verifica; scritture private la cui sottoscrizione digitale, già disconosciuta da colui contro il quale esse sono prodotte, sia positivamente verificata per la mancata prova contraria alla presunzione di riconducibilità dell'utilizzo del dispositivo di firma al suo titolare)
Tempo di conservazione	Intervallo temporale con obbligo di mantenimento dei referti e delle immagini e indicazione dei soggetti responsabili dell'adempimento
Titolario	Quadro di classificazione costituito da categorie, articolate in classi e sottoclassi che rispecchiano le funzioni dell'ente. Individua in quale categoria/funzione e, all'interno della categoria, in quale classe e sottoclasse si trova il fascicolo in cui inserire il documento da archiviare, unendolo ai documenti appartenenti allo stesso procedimento.
Total Testing Process	Processo di generazione e autenticazione, con la presenza di sistemi e di griglie di allarme che permettano di identificare, correggere e prevenire, in tempo reale, anomalie su referti di laboratorio e immagini radiodiagnostiche

