Azienda Ospedaliera Universitaria Federico II
Integrata con il Servizio Sanitario Regionale

ALLEGATO ALLA DELIBERAZIONE N° 396 DEL 24 SETTEMBRE 2013

Manuale della Conservazione Sostitutiva dell'A.O.U. Federico II

ELENCO REVISIONI
REVISIONS RECORD SHEET

Revisione Revision	Data Date	Pagine rev. Rev. pages	Annotazioni Note
1	2013-06-27	All	First Emission

LISTA DELLE ABBREVIAZIONI
ABBREVIATIONS LIST

Abbreviazione **Abbreviation**	**Descrizione** **Description**
BMP	Bitmap Image File
CAdES	CMS Advanced Electronic Signature
CSV	Comma Separated Values
DICOM	Digital Imaging and COmmunications in Medicine
JPEG	Joint Photographic Experts Group
LAN	Local Area Network
MD5	Message-Digest Algorithm 5
PACS	Picture Archiving and Communication System
PKCS	Public-Key Cryptography Standards
RAID	Redundant Array of Independent Disks
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPOF	Single Point of Failure
UO	Unità Operativa
URL	Uniform Resource Locator
WAN	Wide Area Network

Indice

1. Scopo 0
1.1. Identificazione 0
1.2. Descrizione del documento 0
2. Documenti di riferimento 1
3. Introduzione 2
4. Dati di identificazione e definizioni 3
4.1. Dati identificativi della Certification Authority (C.A.) 3
4.2. Dati identificativi dei documenti da trattare 3
4.3. Luogo di conservazione dei documenti 3
4.4. Definizioni Normative 4
5. Compiti e doveri del Responsabile della Conservazione Sostitutiva 6
5.1. Punti di attenzione rispetto ai compiti del responsabile 6
5.2. Archiviazione Elettronica e Conservazione Sostitutiva 7
5.2.1. Archiviazione Elettronica 7
5.2.2. Conservazione Sostitutiva 7
6. Servizio di Conservazione Sostitutiva 8
6.1. Descrizione 9
6.2. Strumenti 10
6.2.1. Struttura File di controllo 10
6.2.2. Struttura File di chiusura 11
6.3. Organizzazione 12
6.4. Procedure 13
6.4.1. Modalità di apposizione della firma digitale da parte del Responsabile della Conservazione 13
6.4.2. Procedura di esibizione 13
6.5. Verifiche periodiche e aggiornamento 14
6.5.1. Scadenziario delle verifiche periodiche 14
6.5.2. Aggiornamento 14
6.5.3. Verbali delle verifiche periodiche 14
7. Copie di Sicurezza 16
7.1. Modalità di produzione 16
7.2. Conservazione 17
7.3. Gestione degli eventi catastrofici 19
7.4. Tempi di conservazione 20
8. Manutenzione del software applicativo 21
9. Privacy 22
10. Note 23
1. Appendice A 24
Certification Authority 24

Elenco delle tabelle

Tabella 1 – Documenti di riferimento 1
Tabella 2 – Definizioni Normative 5
Tabella 3 – Tempi di conservazione 20
Tabella 4 – Personale coinvolto 24
Tabella 5 – Personale autorizzato ai locali (installazione primaria) 24
Tabella 6 – Personale autorizzato ai locali (installazione secondaria) 24
Tabella 7 – Firma Digitale 25
Tabella 8 – Marca Temporale 25

Elenco delle figure

Figura 1 – Conservazione remota 19

Scopo

1.1. Identificazione

Titolo: Azienda Ospedaliera Universitaria "Federico II" - Manuale della Conservazione Sostitutiva

Identificativo: DOC-MCS

Versione: 1

Data emissione: 2013-03-25

1.2. Descrizione del documento

Il presente documento descrive il sistema di Conservazione Sostitutiva per l'Azienda Ospedaliera Universitaria "Federico II" e del relativo servizio di Archiviazione Legale fornito da Theorem@ S.r.l. nell'ambito della gara europea a procedura aperta per l'affidamento, per anni tre, dei servizi necessari alla gestione, manutenzione ed evoluzione del sistema informativo dell'Azienda Ospedaliera Universitaria Federico II (CIG 1424112E62).

L'Azienda Ospedaliera Universitaria "Federico II" intende sottoporre a conservazione sostitutiva, utilizzando il servizio sopra menzionato, i propri documenti e immagini gestite dal proprio sistema PACS.

In particolare, il presente documento ha lo scopo di descrivere:

- le competenze, i ruoli e le responsabilità degli attori coinvolti nel processo;
- come è implementato il processo di conservazione e gli aspetti operativi per arrivare alla produzione del dispositivo contenente la documentazione digitale;
- il processo di apposizione della Firma Digitale, della Marca Temporale e tutti gli aspetti procedurali inerenti la registrazione dei dispositivi sostitutivi;
- le procedure di verifica dei documenti e di gestione delle copie di sicurezza.

Il documento recepisce le indicazioni fornite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA, dal 29 dicembre 2009 DigitPA), e in particolare le "Regole Tecniche per la riproduzione e conservazione di documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali" (Deliberazione n.11/2004 del 19 febbraio 2004), nonché le successive "Note Esplicative delle Regole Tecniche per la riproduzione e conservazione dei documenti su supporto ottico".

2. Documenti di riferimento

	Identificativo.	Titolo	Revisione	Data emissione
1.	-	Decreto Legislativo n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale	-	2005-03-07
2.	-	Deliberazione CNIPA n. 11/2004 e relative note esplicative	-	2004-02-19
3.	-	Decreto Legislativo n.52	-	2004-02-20
4.	-	Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009	-	2009-03-30

Tabella 1 – Documenti di riferimento

3. Introduzione

La conservazione sostitutiva è una procedura informatica, regolamentata dalla legge italiana, in grado di garantire nel tempo la validità legale di un documento informatico.
La possibilità di "sostituire" documenti cartacei con contenuti informatici sottoposti a processo di conservazione sostitutiva consente di eliminare la copia originale analogica e di attribuire valore legale e di esibizione nei confronti di terzi ai contenuti elettronici.
Il presente documento disciplina l'archiviazione di referti e immagini prodotti dai servizi di diagnostica dell'A.O.U. effettuato con il sistema di Conservazione Sostitutiva per l'Azienda Ospedaliera Universitaria "Federico II" e del relativo servizio di Archiviazione Legale fornito da Theorem@ S.r.l. nell'ambito della gara europea a procedura aperta per l'affidamento, per anni tre, dei servizi necessari alla gestione, manutenzione ed evoluzione del sistema informativo dell'Azienda Ospedaliera Universitaria Federico II (CIG 1424112E62).

La conservazione sostitutiva è un processo caratterizzato da tre elementi fondamentali:

- firma digitale e impronta;
- marca temporale;
- documento informatico.

La **firma digitale** è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi crittografiche, in grado di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un loro insieme.
La firma digitale permette quindi a un documento di adempiere ai requisiti di autenticità, integrità, riservatezza e non ripudiabilità rendendolo così completamente sostituibile a quello analogico.
L'impronta è una sorta di riassunto univoco del documento ottenuto applicando un algoritmo matematico.
La **marca temporale** è un procedimento informatico mediante il quale si appone al documento, o all'insieme di documenti, la data e l'ora in cui viene ultimata correttamente la procedura di conservazione ossia si appone un riferimento temporale in modo da rendere opponibile ai terzi il riferimento temporale del documento conservato.
La marca viene rilasciata da una Time Stamping Authority e serve a certificare che un certo documento (o insieme di documenti) esisteva ad una data e, se abbinato alla firma, esisteva in quella precisa forma.
Inoltre un **documento informatico** deve essere statico, non contenere macro-istruzioni o codice eseguibile e non modificabile, ovvero il contenuto non deve essere alterabile durante le fasi di accesso e conservazione nonché restare immutabile nel tempo.

4. Dati di identificazione e definizioni

Ai fini dell'esecuzione del Servizio, l'Azienda Ospedaliera Universitaria "Federico II" è Responsabile della Conservazione nella persona indicata (Responsabile) in appendice (rif. Appendice A), che agisce ai sensi dell'art. 5 della Deliberazione CNIPA (rif. 2).
Il Responsabile espleterà tutte le funzioni inerenti al processo di Conservazione Sostitutiva e, in particolare, i processi di apposizione di firme digitali e marche temporali, essendo dotato di un certificato qualificato emesso secondo la normativa vigente in tema di firma digitale. Tale certificato, installato sulla propria SmartCard, è utilizzato dal processo di certificazione dei lotti di documenti da sottoporre a Conservazione Sostitutiva.
In base a quanto previsto all'art.5 comma 3 della deliberazione CNIPA (rif. 2), il Responsabile della Conservazione, per la parte operativa delle attività, si avvale a sua volta di personale appartenente alla struttura e indicata in appendice (Appendice).

4.1. Dati identificativi della Certification Authority (C.A.)

I certificati di firma digitale utilizzati dal processo di Conservazione Sostitutiva e le marche temporali sono rilasciate dalla Certification Authority specificata in appendice (Appendice).

4.2. Dati identificativi dei documenti da trattare

I documenti da sottoporre a conservazione sostitutiva fanno riferimento alle classi documentali definite dall'Azienda Ospedaliera Universitaria "Federico II" e riportate nel seguito del presente documento.

4.3. Luogo di conservazione dei documenti

I documenti risultanti dal processo di Conservazione, ovvero i documenti firmati e marcati temporalmente, vengono conservati, come indicato nel seguito del documento, in locale presso l'Azienda Ospedaliera Universitaria "Federico II" e in remoto, allo scopo unico di una replica per il piano di Disaster Recovery, presso il Data Center gestito dall'Azienda Theorem@ S.r.l..
In particolare:

- **copia locale**: Azienda Ospedaliera Universitaria "Federico II", Via S. Pansini, 5 – 80131 Napoli – Edificio 7/D presso locali tecnici SIA. contiene tutte le immagini e referti collegati archiviati legalmente. Ulteriore copia delle immagini è effettuata su supporti installati nei locali della centrale telefonica;
- **copia remota**: Theorem@ S.r.l., Via Mandrizzo, snc – 84084 Fisciano (SA) – presso locali tecnici piano interrato ad accesso controllato. Contiene la sola copia (replica) tutte le immagini e referti collegati archiviati legalmente; presenti nella copia locale.

4.4. Definizioni Normative

Termine/Acronimo	Definizione
Documento	Per documento s'intende la rappresentazione informatica o in formato analogico di atti, fatti e dati intelligibili direttamente o attraverso un processo di elaborazione elettronica.
Documento analogico	Per documento analogico s'intende un 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, microfiches, microfilm), come le magnetizzazioni su nastro (esempio: cassette e nastri magnetici audio e video). Si distingue in documento originale e copia
Documento analogico originale	Per documento analogico originale s'intende un documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento informatico	La rappresentazione informatica di atti, fatti e dati intelligibili attraverso un processo di elaborazione elettronica.
Firma digitale	Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore 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.
Impronta	La sequenza di simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash.

Termine/Acronimo	Definizione
Funzione di hash	Una funzione matematica che genera, a partire da una generica sequenza di simboli binari (bit), un'impronta in modo tale che risulti di fatto impossibile, a partire da questa, determinare una sequenza di simboli binari (bit) che la generi, ed altresì risulti di fatto impossibile determinare una coppia di sequenze di simboli binari per le quali la funzione generi impronte uguali. La nuova deliberazione introduce principalmente modifiche nei formati di firma e marca dei documenti, utilizzando nuovi algoritmi. La firma digitale viene realizzata facendo un riassunto del file (hash o digest) e successivamente cifrando questo riassunto con la chiave privata presente nel dispositivo del Responsabile della Conservazione. Il tutto viene poi ricomposto in un unico file. La precedente deliberazione prevedeva che il digest venisse creato con algoritmo SHA-1, che la cifratura fosse realizzata con algoritmo di RSA e che il documento iniziale insieme al certificato utente e alla firma venissero ricomposti in un file formato PKCS#7. La nuova deliberazione ha introdotto una versione più robusta della stessa famiglia di algoritmi, lo SHA-256. In questo caso la cifratura viene effettuata con algoritmo RSA e chiave a 1024 e il tutto viene ricomposto nel formato CAdES, ritenuto indispensabile per rispettare le norme europee sulla firma digitale.
Riferimento temporale	Informazione, contenente la data e l'ora, che viene associata ad uno o più documenti informatici da una procedura informatica.
Marca temporale	Una marca temporale è un'evidenza informatica risultato di una procedura informatica, con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi.
TSA	Time Stamping Authority. Ente terzo che emette i certificati di marcatura temporale
TSS	Time Stamping Service. Servizio di marcatura temporale che emette marche temporali utilizzando il certificato emesso da una TSA. Questo servizio deve rispettare i requisiti del RFC 3161 e il titolo IV del DPCM 13 gennaio 2004

Tabella 2 – Definizioni Normative

5. Compiti e doveri del Responsabile della Conservazione Sostitutiva

Ruolo, funzioni e compiti del Responsabile del procedimento di conservazione sono stabiliti nella loro connotazione fondamentale dall'Art. 5 della Deliberazione CNIPA 11/2004.
Si tratta quindi della figura centrale intorno alla quale gravita la progettazione, l'organizzazione, la gestione e la manutenzione del sistema di conservazione sostitutiva.
Le connotazioni giuridiche di tale figura si devono ancora considerare in evoluzione.
Il primo documento interpretativo ufficiale, di origine tributaria, che si occupa della figura è la Circolare 36e/2006, al punto 7.4:

"Il responsabile della conservazione di norma si identifica con il contribuente, salva la facoltà di quest'ultimo di designare un terzo; nel caso di contribuenti diversi dalle persone fisiche, spetta agli stessi il potere di nominare il responsabile della conservazione che potrà essere sia un soggetto legato da un rapporto qualificato (un socio o un amministratore) sia un terzo esterno alla società, all'associazione o all'ente".

Un rilevante intervento interpretativo, le cui conseguenze non appaiono ancora del tutto esplorate dalla dottrina, è invece contenuto nella Risoluzione 161/e del 9 luglio 2007:

"Eventuali inadempienze dei suddetti obblighi che diano luogo all'applicazione di sanzioni vanno, dunque, essere addebitate al soggetto tenuto al rispetto delle prescrizioni in materia di corretta tenuta e conservazione della contabilità. Tuttavia, la disciplina del concorso di persone nell'illecito, contenuta nell'articolo 9 del d.lgs. 18 dicembre 1997, n. 472 – secondo cui quando più persone concorrono in una violazione, ciascuna di esse soggiace alla sanzione per questa disposta – comporta che se l'applicazione della sanzione è conseguenza di un azione o omissione, dolosa o colposa, dell'incaricato della conservazione questi è tenuto a rispondere della sanzione in concorso con il contribuente".

La Risoluzione, per la prima volta, pur ribadendo il principio generale della responsabilità diretta del contribuente per quanto riguarda inadempimenti nella corretta gestione dei documenti tributari, apre un varco verso un coinvolgimento solidale del Responsabile della conservazione, per quanto riguarda lo svolgimento delle attività ad esso attribuite.

5.1. Punti di attenzione rispetto ai compiti del responsabile

L'Art. 5 della Delibera 11/2004 del CNIPA (rif. 2) prevede solo funzioni che devono essere considerate minimali, pertanto si deve ricordare che il responsabile della conservazione deve predisporre procedure idonee per gestire:

- la presa in carico dei documenti;
- gli accessi di autorità e polizia finanziaria;

- gli accessi di autorità e polizia giudiziaria;
- gli accessi del cliente (compresi revisori, certificatori, etc.) e dei suoi aventi causa;
- le patologie del rapporto di servizio (nel caso dell'outsourcing);
- la successione nel contratto (nel caso dell'outsourcing);
- il passaggio di consegne (nel caso dell'outsourcing);
- la produzione di copie conformi;
- l'invio telematico delle impronte degli archivi all'Agenzia delle Entrate (se a questo incaricato).

Il presente manuale consente di standardizzare le procedure e di consolidarle nel know-how aziendale.
Il tema è collegato alla gestione delle procedure di auditing interno e, da ultimo, anche agli adempimenti collegati alla legge 23/01.

5.2. Archiviazione Elettronica e Conservazione Sostitutiva

5.2.1. Archiviazione Elettronica

Il processo di archiviazione inizia con l'apposizione del riferimento temporale e della firma digitale qualificata ad ogni singolo documento informatico ed immagini e termina con la sua memorizzazione su un qualunque supporto elettronico.

5.2.2. Conservazione Sostitutiva

Il processo di conservazione è un processo che si prolunga nel tempo ed è finalizzato a rendere un documento informatico ed immagini non deteriorabile e disponibile per il periodo per il quale la sua conservazione è obbligatoria a termini di legge.
La conservazione dovrà garantire nel tempo l'autenticità e l'integrità dei dati oggetto di archiviazione.
L' archiviazione elettronica garantisce, attraverso il riferimento temporale, l'esistenza in un dato tempo di un documento informatico ed immagini nonché la sua autenticità e integrità attraverso la firma digitale.
La conservazione sostitutiva garantisce, nel tempo, tramite la marcatura temporale e la firma digitale del responsabile della conservazione, l'integrità, l'autenticità e la non modificabilità del documento informatico ed immagini così come esso è stato prodotto in fase di archiviazione.
I principali vantaggi applicativi della conservazione sostitutiva sono la progressiva eliminazione dei vecchi archivi cartacei, la loro trasformazione in archivi digitali e la possibilità di inviare, ricevere, archiviare direttamente documenti informatici con valore legale e rilevanza fiscale.
La conservazione sostitutiva è quindi uno strumento indispensabile che permette di smaterializzare l'intero ciclo di vita di ogni documento aziendale, dalla sua emissione alla sua conservazione digitale, garantendone al contempo la rilevanza ai fini legali.

6. Servizio di Conservazione Sostitutiva

Il processo di Conservazione prevede tre fasi principali:

1. creazione del volume relativo ai documenti ed immagini da sottoporre a Conservazione;
2. verifiche ed inserimento dei documenti ed immagini in lotti omogenei;
3. chiusura dei lotti e Conservazione.

Nell'implementazione del processo di Conservazione sono coinvolte le seguenti entità principali che costituiscono il Lotto di Archiviazione:

- **Pacchetto**: è un file in formato archivio **ZIP**. Rappresenta l'insieme di documenti/immagini da sottoporre a Conservazione ed è composto dai seguenti file/directory:
  - **DICOMDIR**: contiene i riferimenti univoci a tutti i file che costituiscono il Pacchetto. Un DICOMDIR è strutturato come una "Directory" per file DICOM e contiene 4 livelli gerarchici (PAZIENTE, STUDIO, SERIE, IMMAGINE). Quindi, per ogni file presente nella directory indicizzata (vedi directory DICOM di seguito), nel DICOMDIR vengono memorizzate le quatto informazioni gerarchiche descritte sopra e relative al file stesso. La struttura del file DICOMDIR segue lo standard DICOM.
    Questo file, di fatto, costituisce il file attributi che contiene i valori degli attributi DICOM di ogni singolo documento, nonché il riferimento (percorso relativo) del singolo file.
  - **DICOM**: è la directory contenente i file indicizzati dal file DICOMDIR;
  - **documenti/immagini**: sono tutti i file indicizzati dal file DICOMDIR, generalmente immagini e referti.

  Il file viene nominato secondo il seguente formato:

  [NOMEFILE].zip

  dove [NOMEFILE] rappresenta il nome assegnato dal sistema automaticamente (ad esempio: 2011031334).
  I documenti/immagini vengono resi statici e non modificabili, ovvero, il Pacchetto (file ZIP) non contiene MACROISTRUZIONI o CODICI ESEGUIBILI. In ogni caso, le immagini e i referti DICOM sono già documenti statici.

- **File di controllo**: file in formato **XML** contenente la dimensione in byte del **Pacchetto** e la sua impronta hash. Viene utilizzato per verificare l'integrità di ogni Pacchetto.
  Il file viene nominato secondo il seguente formato:

[NOMEFILE]-check.xml

dove [NOMEFILE] rappresenta il nome assegnato al Pacchetto e "-check" è un suffisso costante (ad esempio: 2011031334-check).

- **Documenti/Immagini**: sono le entità base di tutto il processo. Dopo la creazione automatica del **Pacchetto**, l'applicazione di gestione censisce ogni documento/immagini presente nel pacchetto come "entità documento", permettendone così la ricerca, l'estrazione, etc..
- **File di chiusura**: file di testo, con estensione **TXT**, che contiene informazioni relative al nome del Pacchetto, all'impronta hash, etc.. E' il file che viene firmato digitalmente dal Responsabile della Conservazione e marcato temporalmente.
  Il file viene nominato secondo il seguente formato:

  [NOMEFILE].txt

  dove [NOMEFILE] rappresenta il nome assegnato al Pacchetto (ad esempio: 2011031334).

  Questo file subisce delle variazione della propria estensione nel momento in cui viene firmato e marcato, più precisamente:

  i. dopo l'apposizione della firma digitale: [NOMEFILE].txt.p7m
  ii. dopo la marcatura temporale: [NOMEFILE].txt.p7m.tsd

  Quindi, a conclusione del processo, il file diventa: [NOMEFILE].txt.p7m.tsd

6.1. Descrizione

La realizzazione del Servizio è essenzialmente racchiuso nell'esecuzione delle seguenti operazioni:

1. generazione dell'impronta (hash) del **File di controllo**;
2. memorizzazione dell'impronta del **File di controllo** nel **File di chiusura**;
3. apposizione della Firma Digitale al **File di chiusura**;
4. richiesta di una Marca Temporale associata al **File di chiusura** precedentemente firmato;
5. memorizzazione del **Pacchetto**, del **File di controllo** e del **File di chiusura** firmato digitalmente e della Marca Temporale su supporto con caratteristiche di alta affidabilità e alta permanenza del dato, per un periodo temporale prestabilito (rif. Tempi di conservazione).

Il servizio fornisce, per eseguire tutte le operazioni sopra descritte e mediante strumenti informatici descritti di seguito, un'interfaccia che consente anche di:

- effettuare ricerche all'interno del repository documentale, sulla base degli indici definiti;
- visualizzare i risultati della ricerca;
- visualizzare il documento risultante dalla ricerca effettuata;
- effettuare l'estrazione di uno o di tutti i documenti risultanti dalla ricerca effettuata;
- verificare, in caso di esibizione dei documenti, la Marca Temporale e la Firma Digitale del lotto di documenti in cui ogni documento è stato inserito.

6.2. Strumenti

Le tre fasi principali elencate all'inizio, ossia la creazione del volume relativo ai documenti ed immagini da sottoporre a Conservazione, le verifiche ed inserimento dei documenti in lotti omogenei e la chiusura dei lotti e Conservazione vengono eseguite mediante un software fornito in dotazione.
Tale software applicativo, modulo di MERLINO ENTERPRISE di Theorem@ S.r.l. e denominato "MEADIGSIG", consente di eseguire i passi sopra descritti mediante la pressione, in sequenza, di tre pulsanti:

1. "Carica archivi": carica i volumi creati automaticamente dal sistema PACS e relativi ai documenti ed immagini da sottoporre a Conservazione rendendoli pronti per l'archiviazione;
2. "Archivia": esegue le verifiche necessarie e inserisce i documenti ed imamgini in lotti omogenei (Pacchetto);
3. "Esegui": applica la firma digitale, mediante richiesta di codice PIN, e della marca temporale al File di controllo. In questa fase il lotto viene spostato nel repository documentale, più precisamente in un'area di memorizzazione dell'installazione primaria da cui non può essere più rimosso. Consiste nella chiusura dei lotti e Conservazione.

Il software in dotazione consente anche di recuperare particolari documenti e/o immagini dal repository documentale. Grazie alla funzione "Recupera Studi" è possibile ricercare un particolare paziente per nominativo e per intervallo di data. Il software visualizzerà tutti gli esami estratti dai lotti di archiviazione che rispondono al criterio di ricerca impostato. Selezionando lo specifico studio, questo verrà ripristinato in una cartella, preventivamente configurata, che conterrà, oltre ai documenti e alle immagini, anche un visualizzatore per la corretta visualizzazione delle immagini senza l'ausilio di strumenti esterni. Ulteriori dettagli vengono descritti di seguito in Procedure.

6.2.1. Struttura File di controllo

Il File di controllo serve a verificare l'integrità e l'avvenuto trasferimento del file di dati del Pacchetto. E' un file XML che deve avere la seguente struttura:

<?xml version="1.0" encoding="UTF-8"?>

<pacchetto>
<size>[dimensione Pacchetto]</size>
<hash type="MD5">[hash Pacchetto]</hash>
</pacchetto>

6.2.2. Struttura File di chiusura

Il formato del File di chiusura, che come anticipato è un normale file di testo, è il seguente:

ID Lotto: [NOMEFILE]
Pacchetto: [NOMEFILE].zip
Impronta Pacchetto: [HASH]
Data conservazione: yyyy-mm-dd hh:mm:ss
File di controllo: [NOMEFILE]-check.xml
Impronta File di controllo: [HASH]
Classe Documentale: radiologia
Algoritmo calcolo impronte: MD5
Numero documenti: [numero totale **documenti/immagini**]
Responsabile Conservazione: [COGNOME NOME]
Titolo Responsabile Conservazione: RESPONSABILE CONSERVAZIONE SOSTITUTIVA
Organizzazione Responsabile Conservazione: Azienda Ospedaliera Universitaria "Federico II"

Come anticipato, questo file contiene tutte le informazioni relative ai file, sia documenti/immagini che di controllo, destinati alla Conservazione Sostitutiva. In particolare si possono riconoscere le seguenti informazioni:

- identificativo univoco del lotto di archiviazione (ID Lotto)
- nome del Pacchetto
- impronta hash del Pacchetto
- data conservazione corrispondente alla data e all'ora di sistema in cui viene effettuata l'archiviazione definitiva, quindi corrispondente all'atto di apposizione della firma e della marca temporale
- nome del File di controllo associato al Pacchetto
- impronta hash del File di controllo
- identificativo della classe documentale di appartenenza del lotto (Classe Documentale)
- algoritmo utilizzato per il calcolo dell'impronta (Algoritmo impronta archivio)
- numero totale dei documenti/immagini presenti, ossia il numero esatto dei file (le directory vengono escluse da questo computo) contenuti nella cartella DICOM del Pacchetto.
- Nome, Titolo e Organizzazione di appartenenza del Responsabile della Conservazione

L'algoritmo utilizzato per il calcolo dell'hash, ossia l'impronta del Pacchetto, è l'MD5. Come ogni algoritmo di hash, l'MD5 produce un message digest, o "impronta del messaggio", di lunghezza fissa partendo da un messaggio di lunghezza variabile. La sicurezza di un algoritmo di hash risiede nel fatto che la funzione non sia reversibile (non sia cioè possibile risalire al messaggio originale conoscendo solo questo dato) e che non deve essere mai possibile che si riescano a creare intenzionalmente due messaggi diversi con lo stesso digest. L'algoritmo MD5 produce un digest del messaggio di 128 bit (16 byte) che è rappresentato da una sequenza di 32 caratteri in notazione esadecimale.

6.3. Organizzazione

La presente sezione illustra le responsabilità e i passi del processo di Conservazione Sostitutiva.
Di seguito sono indicati i passi del processo (le azioni) la cui responsabilità è a carico del Responsabile della Conservazione:

1. verifica della consistenza dei flussi dati: tutti i file, prima di essere avviati al processo di Conservazione Sostitutiva, sono così come "estratti" dal sistema PACS. Sono quindi analizzabili e vanno verificati prima di procedere con la Conservazione. In questa fase, il processo ha "fascicolato" i documenti ed immagini, ossia ha raggruppato tra loro secondo logiche funzionali. Dal punto di vista organizzativo, la fascicolazione è importante perché consente l'accesso più immediato a documenti tra loro correlati; dal punto di vista tecnico è importante sottolineare che, documenti dello stesso fascicolo, vengono inseriti nello stesso Pacchetto.
2. archiviazione documenti ed immagini e memorizzazione degli stessi: produzione del Pacchetto contenente tutti i file da archiviare e relativi al pacchetto stesso. Nello stesso momento, il sistema produce il File di controllo associato al Pacchetto e, infine, il File di chiusura.
3. esecuzione del processo di Conservazione Sostitutiva dei lotti di documenti digitali ed immagini mediante l'apposizione di Marca Temporale e Firma Digitale al File di chiusura.
4. verifica avvenuta Conservazione mediante gli strumenti messi a disposizione dall'interfaccia utente del sistema.
5. verifica Marca Temporale e Firma Digitale applicata mediante gli strumenti messi a disposizione dall'interfaccia utente del sistema.
6. ricerca e visualizzazione dei documenti ed immagini conservati tramite interfaccia utente del sistema;
7. esibizione dei documenti ed immagini conservati;
8. verifica periodica dell'effettiva leggibilità dei documenti ed immagini conservati.

A queste operazioni e in modo del tutto automatico, il servizio associa un meccanismo di replicazione dei dati in luogo remoto (archiviazione in luogo sicuro dei dati archiviati).

6.4. Procedure

Il sistema utilizza, per soddisfare il requisito di apposizione del riferimento temporale richiesto per la procedura di conservazione prevista dalla deliberazione CNIPA, Art. 5 comma 1 lett. g (rif **2**), le Marche
Temporali fornite dall'Azienda Ospedaliera Universitaria "Federico II". Le marche temporali emesse devono essere firmate da un certificato emesso da un'Authority accreditata.
La generazione di una Marca Temporale è ottenuta attraverso una sottoscrizione digitale apposta su una evidenza informatica e fornisce la prova dell'esistenza di tale evidenza informatica al momento di generazione della marca stessa. Apporre una marca temporale ai documenti informatici sottoscritti digitalmente permette di verificare la firma oltre il periodo di validità del certificato di sottoscrizione.
Le marche temporali utilizzate nel processo di Conservazione Sostitutiva sono di tipo "attached" (ovvero
sono contenute nello stesso file per il quale si richiede il servizio di marcatura temporale) e devono avere una validità superiore o uguale agli anni di conservazione dei Documenti ed immagini. Tale formato capace di tenere marca temporale e documento firmato insieme in un unico file, viene chiamato "TimeStamp and Data" e ha estensione "tsd". Mentre i formati precedenti erano semplicemente contenitori di documenti firmati e marcati separati (detached), il formato attached è un vero e proprio nuovo formato specifico per documenti marcati. La deliberazione Deliberazione CNIPA/45 (con le modifiche apportate dalla Determinazione 69/2010) introduce anche una nuova modalità di marcatura: se al documento informatico si devono applicare due o più firme e il tempo di apposizione di ciascuna firma è rilevante, si applica una marca ad ogni firma. Questo formato si chiama CAdES-T.

6.4.1. Modalità di apposizione della firma digitale da parte del Responsabile della Conservazione

Le chiavi crittografiche corrispondenti al certificato qualificato del Responsabile della Conservazione per l'apposizione della firma digitale sono memorizzate in una SmartCard conforme alla normativa vigente relativa ai dispositivi sicuri per la creazione della firma digitale.
La firma digitale del Responsabile della Conservazione è apposta tramite una procedura automatica la cui attivazione è effettuata tramite l'inserimento di un pin da parte del responsabile medesimo, il quale in questo modo afferma la propria volontà nell'apposizione della firma stessa sui singoli File di chiusura.

6.4.2. Procedura di esibizione

L'esibizione dei documenti conservati avviene, da parte di personale autorizzato, mediante l'interfaccia di una applicazione di esibizione documenti che il sistema rende disponibile automaticamente.

L'interfaccia permette ad un utente abilitato di ricercare ed eventualmente visualizzare i documenti sottoposti al processo di Conservazione Sostitutiva presenti all'interno dell'archivio.

6.5. Verifiche periodiche e aggiornamento

Il Responsabile delle Conservazione Sostitutiva, con cadenza annuale, controllerà la consistenza e l'integrità dei lotti di documenti e dei relativi file attributi, file di indice e file di chiusura, eseguendo o delegando l'esecuzione di una procedura di controllo che interesserà un adeguato campione dei Lotti sottoposti a Conservazione Sostitutiva.
La procedura sarà effettuata sui dati presenti all'interno del sistema di archiviazione e sulle copie presenti sul sistema remoto (replica).

6.5.1. Scadenziario delle verifiche periodiche

Si distinguono due procedure di verifica:

1. verifica dell'integrità e della consistenza dei lotti di documenti generati dal Processo di Conservazione;
2. verifica dell'effettiva leggibilità dei documenti inseriti all'interno dei lotti.

La prima procedura, con cadenza almeno semestrale, è eseguita dal Responsabile della Conservazione, come descritto in precedenza.
Per la seconda procedura il Responsabile della Conservazione, con cadenza almeno annuale verificherà che, per i formati dei file utilizzati per la conservazione dei documenti, sia disponibile sul mercato un visualizzatore aggiornato e conforme alle specifiche del singolo formato di file. Il visualizzatore fornito a corredo è un file eseguibile (binario) compatibile con piattaforme Microsoft Windows a 32 e 64 bit.

6.5.2. Aggiornamento

Ogni anno, il Responsabile della Conservazione valuta la congruità del presente manuale e del piano di conservazione e li aggiorna in base alle necessità riscontrate e agli aggiornamenti legislativi in materia. Il Responsabile della Conservazione comunica gli aggiornamenti agli organi dell'amministrazione con funzioni di responsabili nonché ai dirigenti.

6.5.3. Verbali delle verifiche periodiche

Tutte le procedure di verifica, gli eventuali interventi sul software applicativo, le modifiche delle configurazioni, l'assegnazione delle deleghe a svolgere opportune operazioni, nonché tutti gli avvenimenti importanti o ritenuti tali dal Responsabile della Conservazione ai fini del corretto svolgimento del processo di conservazione sostitutiva saranno opportunamente tracciati mediante Verbali.
La definizione del template da adottare per la redazione di ogni singolo verbale è a carico del Responsabile della Conservazione che seguirà, per la sua definizione, le regole e le

procedure del Sistema di Qualità dell'Azienda Ospedaliera Universitaria "Federico II". Anche la redazione di ogni singolo verbale è a carico del Responsabile della Conservazione.

7. Copie di Sicurezza

Il sistema prevede un apposito processo per la generazione di copie di sicurezza nel rispetto della vigente normativa.
Le copie di sicurezza vengono custodite su un sistema remoto e replicato, così come indicato di seguito.

7.1. Modalità di produzione

La Conservazione Sostitutiva è generalmente associata all'utilizzo di supporti ottici (CD-ROM, DVD-ROM, etc.). Questo garantisce un'elevata affidabilità, per la natura stessa del supporto, ma comporta un intervento umano consistente e un processo di archiviazione fisica e catalogazione che può risultare complesso e farraginoso.
L'archiviazione di lungo termine su hard disk, invece, in sostituzione di supporti ottici e nastri, rappresenta una soluzione più efficiente e, sotto molti aspetti, più sicura.
Il sistema si basa su sistemi di memorizzazione costituiti da hard disk con elevati livelli di ridondanza, che non richiedono l'intervento umano e consentono di realizzare un archivio storico/legale on-line. Questo garantisce ai medici e agli operatori autorizzati di recuperare le immagini diagnostiche in tempi molto brevi.

Il sistema è strutturato su due livelli d'installazione:

1. installazione primaria: sistema locale presso l'Azienda Ospedaliera Universitaria "Federico II";
2. installazione secondaria: sistema remoto presso Data Center gestito direttamente dal personale autorizzato dall'Azienda Theorem@ S.r.l.

Questo consente di avere un primo livello di archiviazione direttamente presso l'Azienda Ospedaliera Universitaria "Federico II", evitando problemi connessi alla mancata erogazione (dovuta a manutenzione o guasti di causa maggiore) della connessione alla rete Internet. In tal caso il sistema, essendo presente anche in locale (installazione primaria), continuerà a funzionare correttamente. A connessione ripristinata, le due installazioni (primaria e secondaria) avvieranno il processo di sincronizzazione per l'allineamento dei dati senza inficiare le prestazioni e le normali funzionalità dell'archiviazione sostitutiva.
I vantaggi di tale soluzione sono:

- immune a problemi legati alla mancanza temporanea della connessione alla rete Internet;
- dati facilmente recuperabili, senza pericolo di perdita;
- a differenza di nastri e supporti ottici, non sono necessari interventi costanti e di manutenzione;
- spazio fisico (aree o locali dedicati) richiesto ridotto al minimo;
- accesso casuale (random access) e veloce;

- semplice protezione da disastri tramite replica in rete;
- verifica dei dati memorizzati;
- un investimento per il futuro, indipendente dalla disponibilità di dispositivi specifici per la lettura;
- integrabile con qualsiasi infrastruttura di rete, preesistente e non.

7.2. Conservazione

Come anticipato, la conservazione dei dati viene fatta su due sistemi di archiviazione separati:

1. **installazione primaria** (copia locale): comprende l'installazione e la configurazione delle unità necessarie alla conservazione dei dati prodotti dalla Conservazione Sostitutiva presso l'Azienda Ospedaliera Universitaria "Federico II". L'unità per l'archiviazione comprende un numero di Hard Disk che garantisce, anche nel caso di guasto contemporaneo di più dischi, che nessun dato venga perduto.
2. **Installazione secondaria** (copia remota): comprende l'installazione e la configurazione delle unità necessarie alla replica della conservazione sostitutiva effettuata dall'Azienda Ospedaliera Universitaria "Federico II" presso il Data Center gestito dall'Azienda **Theorem@ S.r.l.**. Per stabilire un'effettiva continuità operativa e la possibilità di implementare un efficiente piano di Disaster Recovery, è necessario considerare due fattori fondamentali:

    1. elevata disponibilità: occorre garantire che i dati siano accessibili anche in caso di errore umano, atti vandalici o violazioni della protezione dovute a vulnerabilità del software;
    2. possibilità di ripristinare i dati in caso di evento disastroso: per fare fronte rapidamente ed efficacemente a un evento disastroso, sia esso naturale o doloso, il dispositivo di archiviazione locale viene ridondato nel Data Center remoto. In questo modo, oltre alla replica totale dell'intera configurazione in un luogo geograficamente distante, è presente anche la possibilità di passaggio alla seconda installazione in caso di guasto di quella primaria (modalità di alta disponibilità).

    Al riguardo la società Theorem@ S.r.l, gestore del servizio, ha dichiarato che :

    - Il Data Center remoto, di proprietà di proprietà di REM S.r.l. in liquidazione, già REM S.p.A., (stesso opificio che ospita la sede legale e operativa di Theorem@ S.r.l.), è equipaggiato di tutti i dispositivi di sicurezza necessari a garantire l'integrità e la privacy dei dati.
    - L'accesso ai locali è consentito solo a personale autorizzato mediante dispositivi di controllo accesso biometrici. I dati biometrici sono gestiti secondo le normative vigenti. I nominativi delle persone autorizzate all'accesso sono indicati in appendice (Appendice). Inoltre, sia il perimetro

dell'edificio che i locali che ospitano il data center (ossia l'installazione secondaria), sono sottoposti a video-sorveglianza continua e conforme all'Art 13 del D.Lgs 196/2003. La dichiarazione della società Theorem@ S.r.l. deve essere acquisita dal Responsabile della Conservazione e rinnovata almeno con cadenza annuale

- Periodicamente, con cadenza settimanale, i sistemi hardware vengono verificati secondo procedure definite per garantire la continuità del servizio e l'integrità dei dati. Della citata verifica è redatto un verbale riassuntivo dalla società Theorem@ S.r.l. che viene acquisito dal Responsabile della Conservazione.
- Si sottolinea che l'installazione secondaria descritta in questo documento, costituisce solo una replica dei dati per l'implementazione delle politiche di Disaster Recovery e quindi del recupero dei dati in caso di disastro. La copia relativa al processo della Conservazione Sostitutiva è la sola installazione primaria, costituita dal dispositivo di archiviazione locale.
- Ogni anno il Responsabile della Conservazione congiuntamente al personale del Servizio Informatico dell'A.O.U. esegue una verifica presso il Data Center remoto, di proprietà di proprietà di REM S.r.l. in liquidazione, già REM S.p.A., (stesso opificio che ospita la sede legale e operativa di Theorem@ S.r.l.), per la verifica e consistenza dei dati archiviati e dei dispositivi di sicurezza necessari a garantire l'integrità e la privacy dei dati.

Questa soluzione è progettata per essere fortemente scalabile, in modo da poter essere affiancata ed integrata in soluzioni per la riduzione drastica dei tempi di fermo macchina (down time) e l'aumentando dell'affidabilità e della capacità di carico elaborativo.

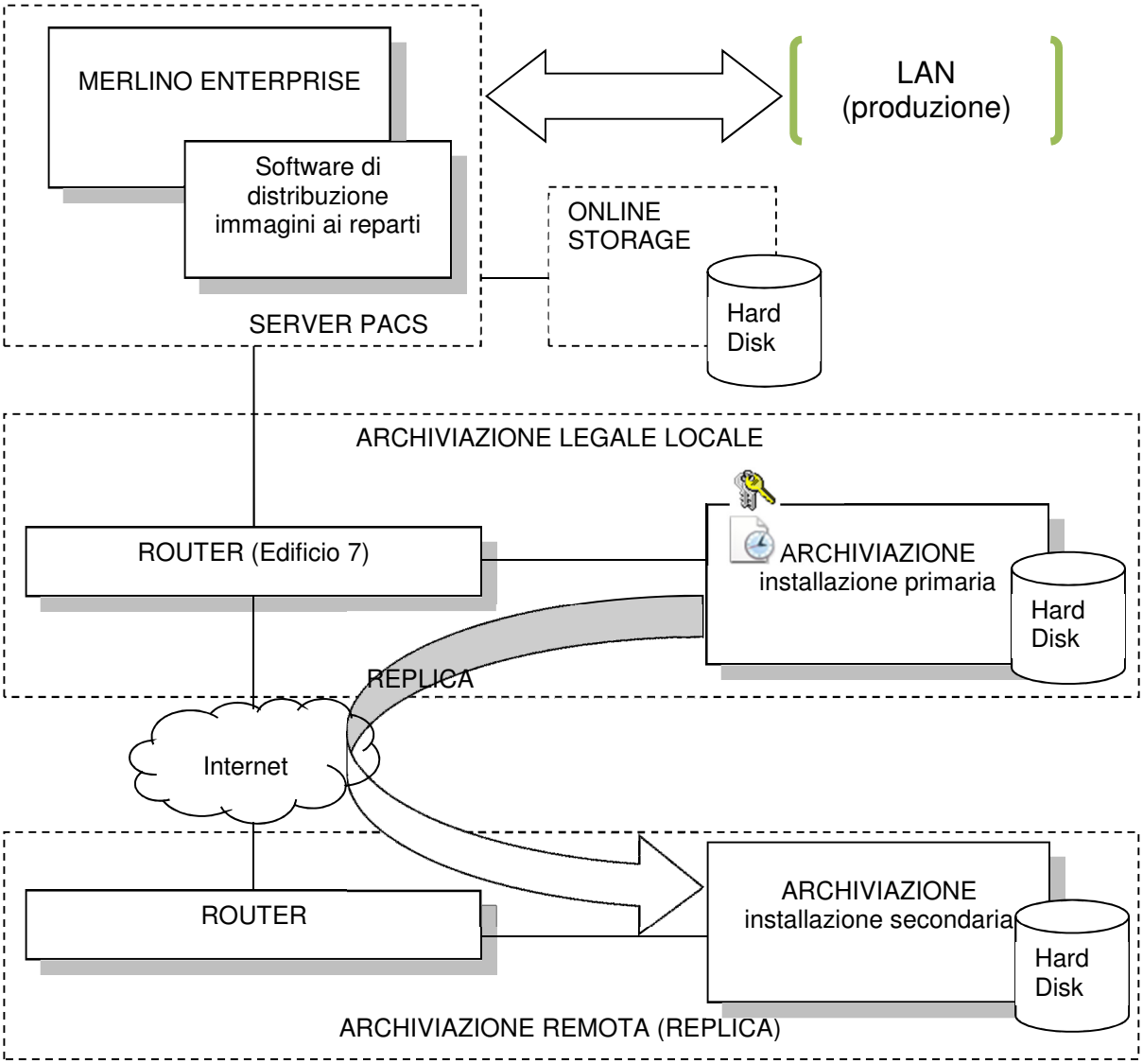

Figura 1 – Conservazione remota

7.3. Gestione degli eventi catastrofici

In caso di evento catastrofico che pregiudichi, in tutto o in parte, il repository primario (installazione primaria) dei dati sottoposti a conservazione, il Responsabile della Conservazione, coadiuvato dal personale preposto dell'Azienda Theorem@ S.r.l., provvederà, utilizzando le copie di sicurezza del'archivio remoto (installazione secondaria), al corretto ripristino dell'intero archivio.

Un'apposita procedura preleverà i dati da tutte le copie di sicurezza generate, ne verificherà l'integrità, e procederà nuovamente al salvataggio di tutti gli elementi su un nuovo sistema di Conservazione Sostitutiva, ovvero su quello preesistente, dopo aver sostituito le parti danneggiate dall'evento catastrofico.

Il verificarsi dell'evento catastrofico e l'esecuzione della procedura di ripristino dell'archivio devono essere registrai in un apposito Verbale, così come descritto in Verbali delle verifiche periodiche.

7.4. Tempi di conservazione

In radiologia digitale cade la necessità di differenziare gli esami eseguiti da pazienti ricoverati ed esami eseguiti da pazienti esterni. Tutti gli esami prodotti possono essere processati dalla Conservazione Sostitutiva.

Referto analogico		
Paziente	**Tempo**	**Responsabile**
Interno	Illimitato	Direzione Sanitaria
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	Paziente o UO di Diagnostica per Immagini
Referto Digitale		
Interno	Illimitato	Responsabile della Conservazione Sostitutiva
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	Paziente o Responsabile della Conservazione Sostitutiva
Immagini Analogiche		
Interno	Non inferiore ai 10 anni	UO di Radiologia o Paziente
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	UO di Diagnostica per Immagini o Paziente
Immagini Digitali		
Interno	Non inferiore ai 10 anni	Responsabile della Conservazione Sostitutiva
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	Paziente o Responsabile della Conservazione Sostitutiva
Referto Strutturato		
Interno	Illimitato	Responsabile della Conservazione Sostitutiva – Direzione Sanitaria
Esterno	Non previsto dalle norme nazionali. Possibilità di previsione da parte di norme regionali	Paziente o Responsabile della Conservazione Sostitutiva

Tabella 3 – Tempi di conservazione

8. Manutenzione del software applicativo

E' a cura dell'Azienda Theorem@ S.r.l. mantenere le versioni aggiornate del software per la generazione dei Lotti di Documenti ed immagini sottoposti a Conservazione Sostitutiva.
A tale scopo, tutto il software realizzato per il processo di conservazione sostitutiva e per i processi ad esso collegati si trova all'interno di un sistema di gestione del software, di proprietà esclusiva dell'Azienda Theorem@ S.r.l. che ne detiene tutti i diritti, in grado di mantenere il versioning del codice sorgente sviluppato e recuperare eventuali versioni precedenti.

9. Privacy

Per quanto riguarda l'accesso ai dati da parte di personale dell'Azienda Ospedaliera Universitaria "Federico II", si farà riferimento alle procedure di gestione della privacy presenti nella documentazione di riferimento dell'Azienda stessa.
Per quanto riguarda l'accesso ai dati da parte di personale appartenente all'Azienda Theorem@ S.r.l., solo ed esclusivamente per motivi di carattere tecnico e necessari al corretto funzionamento delle procedure di Conservazione, si farà riferimento alle procedure di gestione della privacy dell'Azienda stessa.
Allo scopo e per le sole finalità legate all'esecuzione del servizio, il Responsabile della Conservazione è Responsabile del Trattamento dei dati, ai sensi del D.Lgs 196/2003: "Codice in materia di protezione dei dati personali", autorizza il personale appartenente all'Azienda Theorem@ S.r.l. ad accedere e visualizzare i documenti sottoposti a Conservazione Sostitutiva per i soli scopi di verifica della leggibilità dei documenti conservati e per attività di supporto al Responsabile della Conservazione.

10. Note

In ultimo, vengono riportati brevi riferimenti alla Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi, frutto dell'intesa tra il Governo, le Regioni e le Province autonome della Conferenza Stato Regioni del 04/04/12.

Il documento "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi", rappresenta un passaggio evolutivo fondamentale per l'utilizzo di informazioni riguardanti lo stato di salute del cittadino.

Le linee guida stabiliscono come debba essere gestito l'intero processo di conservazione sostitutiva della documentazione sanitaria clinica in diagnostica per immagini, secondo le differenti possibilità di analisi: clinica, organizzativa e medico legale.

Il succitato documento sul quale è stato acquisito il parere tecnico di DigitPA (Ente nazionale per la Digitalizzazione della Pubblica Amministrazione), nonché dell'autorità garante per la protezione dei dati per-sonali è stato sottoposto all'esame della conferenza Stato-Regioni, per la stipula dell'Intesa ai sensi dell'art. 8, comma 6 della legge 5 giugno 2003, n. 131, tra il Governo le Regioni e le Provincie autonome di Trento e di Bolzano sul documento recante "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi".

La prima bozza delle linee guida scritte nel 2007 era stata successivamente aggiornata nel 2009 e quindi aveva ricevuto una valutazione positiva da parte del Garante per la Privacy per recepire le novità normative in materia di tutela dei dati personali. Ora manca soltanto la pubblicazione in Gazzetta Ufficiale a seguito di una intesa raggiunta in seno alla Conferenza Stato-Regioni e Province autonome Trento e Bolzano.

Le linee guida si rivolgono alle strutture sanitarie pubbliche, private per fornire le indicazioni valide per gestire e conservare a norma i documenti clinici digitali.

Il documento in questione non tratta la dematerializzazione dei documenti di archivi analogici e digitali preesistenti sia testuali che iconografici.

Esse costituiscono lo strumento per sviluppare dei processi che siano favorevoli alla dematerializzazione che, realizzata contribuisce, da una parte, ad aumentare il livello di sicurezza e affidabilità per quanto concerne la produzione e gestione della documentazione sanitaria in formato digitale e, dall'altro, a favorire l'interscambio delle informazioni in formato digitale e l'interoperabilità tra coloro che sono preposti alla cura dei cittadini.

Questo documento fornirà ai Direttori Generali, ai Direttori Sanitari, ai Direttori dei Sistemi Informativi e dei Dipartimenti e Unità Operative di Diagnostica per Immagini, Radiologia, Medicina Nucleare le linee guida per gestire la documentazione clinica testuale e iconografica, formata in modalità digitale, in ottemperanza alla normativa vigente in ambito di documentazione clinica di diagnostica per immagini, di firma dei documenti, di consolidamento, conservazione ed esibizione dei documenti.

1. Appendice A

Di seguito vengono indicati i riferimenti e i ruoli del personale coinvolto nel processo di Conservazione.

Ruolo	Azienda	Nome e Cognome
Responsabile della Conservazione	Azienda Ospedaliera Universitaria "Federico II"	**Dott. Ciro Varchetta**
Delegato Responsabile della Conservazione	Azienda Ospedaliera Universitaria "Federico II"	**DA NOMINARE da parte del Das Diagnostica per immagini**
Assistenza Tecnica	Theorem@ S.r.l.	Bernardino Amoruso Carmine Sessa Rosario Giordano

Tabella 4 – Personale coinvolto

Il personale autorizzato all'accesso ai locali tecnici che ospitano il dispositivo locale sono:

Ruolo	Azienda	Nome e Cognome
S.I.A. Resp. Inf. Az.	A.O.U. federico II	Naviglia Mariano
S.I.A. Resp. Reti	A.O.U. federico II	Esposito Giulio
S.I.A. Resp. Sistemi Appl. Osp	.A.O.U. federico II	Toscano Guglielmo
Assistenza Tecnica	Theorem@ S.r.l.	Bernardino Amoruso Carmine Sessa Rosario Giordano

Tabella 5 – Personale autorizzato ai locali (installazione primaria)

Il personale autorizzato all'accesso ai locali tecnici che ospitano il dispositivo remoto sono:

Ruolo	Azienda	Nome e Cognome
S.I.A. Resp. Inf. Az	A.O.U. federico II	Naviglia Mariano
S.I.A. Resp. Reti	A.O.U. federico II	Esposito Giulio
Capo settore S.I.A.	A.O.U. federico II	Toscano Guglielmo
S.I.A. Resp. Sistemi Appl. Osp	Theorem@ S.r.l.	Bernardino Amoruso Carmine Sessa Rosario Giordano

Tabella 6 – Personale autorizzato ai locali (installazione secondaria)

Certification Authority

Denominazione	CN	OU	O	C
InfoCert	InfoCert Servizi di Certificazione	Ente Certificatore	INFOCERT SPA	IT

Tabella 7 – Firma Digitale

Denominazione	CN	OU	O	C
InfoCert	InfoCert Servizi di Certificazione	Ente Certificatore	INFOCERT SPA	IT

Tabella 8 – Marca Temporale