Syncro-Med
HEALTHCARE APPLICATIONS

Manuale di Conservazione

SYNCRO-MED S.r.l.

Vers. 5.2 del 27/07/2017

Syncro-Med S.r.l. – Via G.Galilei, 2/A – 39100 BOLZANO
email : info@syncromed.it
Tel. 0471/065901 FAX 0471/065919
Società con socio unico, soggetta alla direzione e coordinamento di FUJIFILM Italia S.p.A.
Capitale Sociale € 200.000,00 i.v. – Cod. Fisc. e Part. IVA n° 02290730213

Emissione del documento

Azione	*Data*	*Nominativo*	*Funzione*
Redazione	27/07/2016	Ivan Salvato Nicola Nardini	RSI RSC
Verifica	02/09/2016	Avv. Luigi Foglia	Studio Legale Lisi
Approvazione	09/09/2016	Nicola Nardini	RSC

Registro delle versioni

N°Ver/Rev/Bozza	*Data emissione*	*Modifiche apportate*	*Osservazioni*
Vers. 1.0	10/06/2011	Prima stesura	
Vers. 2.0	07/03/2014	Seconda stesura	Recepimento DPCM 3 dicembre 2013
Vers. 3.0	28/04/2016	Terza stesura	Adeguamento normativa per Accreditamento
Vers. 4.0	27/07/2016	Quarta stesura	Versione per accreditamento
Vers. 5.0	06/09/62016	Quinta stesura	Versione riformattata per accreditamento
Vers. 5.1	16/01/2017	Prima revisione	Versione revisionata
Vers. 5.2	27/07/2017	Seconda revisione	Versione revisionata

INDICE DEL DOCUMENTO

1. SCOPO E AMBITO DEL DOCUMENTO

Il presente Manuale descrive le procedure gestionali e tecniche adottate, l'organizzazione, i ruoli e le competenze dei soggetti coinvolti a vario titolo nel processo, al fine di permettere a Syncro-Med Srl di fornire e garantire un servizio di Conservazione a norma dei documenti informatici in favore dei propri clienti.

Si precisa inoltre che, allo scopo di garantire la protezione e riservatezza delle informazioni ritenute di interesse primario e non pubblico, alcuni dettagli relativi ad argomenti che coinvolgono aspetti tecnici e progettuali, riguardanti specificatamente la fornitura del servizio di conservazione, non saranno descritti direttamente nel presente Manuale, ma potranno essere realizzati in documenti specifici, quali ad esempio il "Piano della Sicurezza".

Tali documenti, per i quali non sussiste l'obbligo di pubblicazione, potranno essere resi disponibili, se richiesto, in sede di deposito della domanda di accreditamento ed in ogni eventuale aggiornamento della stesa che si rendesse necessario in futuro.

Torna al sommario

2. TERMINOLOGIA (GLOSSARIO, ACRONIMI)

Termine - Acronimo	Descrizione
Accreditamento	Riconoscimento, da parte dell'Agenzia per l'Italia digitale, del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza ad un soggetto pubblico o privato, che svolge attività di conservazione o di certificazione del processo di conservazione
Aggregazione documentale informatica	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura, al formato dei documenti, all'oggetto e agli ambiti di appartenenza dell'Ente
AgID	È l'acronimo di Agenzia per l'Italia Digitale. È una agenzia pubblica italiana istituita dal Governo Monti, ed è sottoposta ai poteri di indirizzo e vigilanza del Presidente del Consiglio dei Ministri o del Ministro da lui delegato.
Archivio informatico	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico
Area organizzativa omogenea	Insieme di funzioni e di strutture, individuate dalla amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario
CA	È l'acronimo di Certification Authority, letteralmente Autorità Certificativa, è un ente di terza parte (trusted third party), pubblico o privato, abilitato a rilasciare un certificato digitale tramite procedura di certificazione che segue standard internazionali e conforme alla normativa europea e nazionale in materia.
Certificatore accreditato	Soggetto, pubblico o privato, che svolge attività di certificazione del processo di conservazione al quale sia stato riconosciuto, dall' Agenzia per l'Italia digitale, il possesso dei requisiti del livello più elevato, in termini di qualità e di sicurezza (vedasi Accreditamento)
Classificazione	Attività di organizzazione logica dei documenti secondo uno schema articolato in voci individuate attraverso specifici metadati
Conservazione	E' il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nel DPCM 03/12/2013.
Consolidamento probatorio	E' il processo che consente di preservare nel tempo la validità legale della firma digitale apposta ad un documento attraverso l'applicazione di una marca temporale
Copia di sicurezza	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 delle vigenti regole tecniche per il sistema di conservazione
DICOM	Acronimo di Digital Imaging and COmmunications in Medicine; è uno standard pubblico che definisce i criteri per la comunicazione, la visualizzazione, l'archiviazione e la stampa di informazioni di tipo biomedico quali ad esempio le immagini radiologiche

Documento analogico originale	Documento analogico, che si contrappone al Documento informatico o Documento digitale. Può essere unico oppure non unico. Nel secondo caso si tratta di un documento cui sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione (es. Fatture, Libri Contabili etc.). Il documento analogico unico, al contrario, non è "ricostruibile" a partire da altri documenti/scritture e tipicamente è caratterizzato da firme autografe (es. assegni).
Documento digitale	Vedasi Documento informatico
Documento informatico	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
Esibizione	Operazione che consente di visualizzare uno o più documenti conservati e di ottenerne una copia
Evidenza informatica	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (all. 1 DPCM 03/12/2013) a partire da un documento informatico o da un insieme di questi.
Firma Digitale	Un particolare tipo di firma elettronica basata su un certificato qualificato e 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
Formato	Modalità di rappresentazione del documento informatico attraverso una specifica sequenza di bit. Comunemente è identificato attraverso l'estensione del file (es. PDF, XML, ecc.)
Hash	Vedasi Evidenza informatica
HL7	Acronimo di Health Level 7; è un'associazione non profit internazionale che si occupa di definire e gestire standard per la sanità in particolare per l'interoperabilità tra sistemi.
IdC	Indice di Conservazione
Identificativo univoco	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico in maniera tale da consentirne l'individuazione certa.
IdPA	Indice del Pacchetto di Archiviazione
IdPV	Indice del Pacchetto di Versamento
Immodificabilità	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero periodo di conservazione garantendo quindi il principio di staticità
Impronta informatica	Vedasi Evidenza informatica.
Integrità	Insieme delle caratteristiche di un documento informatico che determinano il principio di completezza ed inalterabilità
Interoperabilità	Capacità del sistema di conservazione di interagire e comunicare con altri sistemi

	informatici analoghi sulla base di requisiti minimi condivisi
Leggibilità	Caratteristica per la quale le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di vita del documento
Log di sistema	Registrazione cronologica delle operazioni eseguite sul sistema di conservazione per finalità di controllo e verifica degli accessi, oppure di registro e tracciabilità delle modifiche eseguite sulla base dati
Manuale di conservazione	Strumento formale che descrive il sistema di conservazione dei documenti informatici ai sensi dell'Art. 9 delle regole tecniche
Marca Temporale	E' il riferimento temporale che consente la validazione temporale di un documento informatico. È l'equivalente della Data Certa che gli Uffici Postali appongono sui documenti cartacei.
Pacchetto di Archiviazione	Pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche e le modalità indicate nel manuale di conservazione
Pacchetto di Distribuzione	Pacchetto informativo inviato dal sistema di conservazione all'utente a seguito di una richiesta esplicita da parte di quest'ultimo
Pacchetto di Versamento	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato tra le parti e descritto dettagliatamente nel manuale di conservazione
PDF	È l'acronimo di Portable Document Format, formato di file creato da Adobe Systems per lo scambio di documenti. E' uno standard aperto ed in particolare la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.
PEC	Posta Elettronica Certificata; sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici. Ha la medesima valenza della Raccomandata postale.
Presa in carico	Accettazione da parte del sistema di conservazione di un pacchetto di versamento avendone verificata la conformità rispetto alle modalità formalizzate e descritte nel manuale di conservazione
Processo di conservazione	Insieme delle attività finalizzate alla conservazione a norma dei documenti informatici così come esplicitato all'Art. 10 delle regole tecniche del sistema di conservazione
Produttore	Persona fisica o giuridica che produce il pacchetto di versamento e lo inoltra al sistema di conservazione; è quindi responsabile del trasferimento del suo contenuto nel sistema di conservazione.
Rapporto di versamento	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore
Responsabile della Conservazione	E' il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione digitale conformemente a quanto previsto all'art. 7 del DPCM 03/12/2013.
Riferimento	Vedasi Marca Temporale.

temporale	
Sistema di conservazione	Sistema di conservazione a norma dei documenti informatici di cui all'articolo 44 del Codice
SLA	È l'acronimo di Service Level Agreement ovvero Accordo sui Livelli di Servizio per monitorare la qualità del processo di conservazione in rapporto al contratto sottoscritto con il Cliente
Staticità	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali ad esempio le macroistruzioni, i riferimenti esterni, i codici eseguibili, ecc. che determinerebbero una possibile rappresentazione differente in circostanze differenti del documento informatico; è un onere a carico del prodotto software utilizzato per la produzione del documento informatico
Tipologia di firma digitale	La firma digitale implementa tre distinte tipologie di firma: ▪ CAdES sta per **CMS Advanced Electronic Signatures** ▪ PAdES sta per **PDF Advanced Electronic Signatures** ▪ XAdES sta per **XML Advanced Electronic Signatures**
Utente	Persona, Ente o Sistema che interagisce con il sistema di conservazione a norma dei documenti informatici al fine di accedere e fruire delle informazioni necessarie.
XML	È l'acronimo di Extensible Markup Language. Viene utilizzato per definire le strutture dei dati utilizzando dei marcatori (markup tags). È lo standard utilizzato, ad esempio, per l'emissione delle Fatture Elettroniche verso la Pubblica Amministrazione

Torna al sommario

3. NORMATIVA E STANDARD DI RIFERIMENTO

3.1 Normativa di riferimento

Il sistema di conservazione Synapse Theca è stato realizzato in conformità alla normativa vigente in materia di conservazione dei documenti informatici.

Di seguito vengono riportati i principali riferimenti normativi italiani in materia, ordinati secondo il criterio della gerarchia delle fonti:

- Codice Civile [Libro Quinto Del lavoro, Titolo II Del lavoro nell'impresa, Capo III Delle imprese commerciali e delle altre imprese soggette a registrazione, Sezione III Disposizioni particolari per le imprese commerciali, Paragrafo 2 Delle scritture contabili], articolo 2215 bis - Documentazione informatica;
- Legge 7 agosto 1990, n. 241 e s.m.i. – Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi;
- Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa;
- Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. – Codice in materia di protezione dei dati personali;
- Decreto Legislativo 22 gennaio 2004, n. 42 e s.m.i. – Codice dei Beni Culturali e del Paesaggio;
- Decreto Legislativo 7 marzo 2005 n. 82 e s.m.i. – Codice dell'amministrazione digitale (CAD);
- Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 – Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma3, lettera b), 35, comma 2, 36, comma 2, e 71;
- Decreto del Presidente del Consiglio dei Ministri 3 dicembre 2013 - Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005;
- Decreto del Ministero dell'Economia e delle Finanze del 17 giugno 2014 - Modalità di assolvimento

degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto

- Decreto del Presidente del Consiglio dei Ministri del 13 novembre 2014 - Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici nonché di formazione e conservazione dei documenti informatici delle pubbliche amministrazioni
- Circolare AGID 10 aprile 2014, n. 65 - Modalità per l'accreditamento e la vigilanza sui soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici di cui all'articolo 44-bis, comma 1, del decreto legislativo 7 marzo 2005, n. 82.

Torna al sommario

3.2 Standard di riferimento

Si riportano di seguito gli standard di riferimento elencati nell'allegato 3 delle Regole Tecniche in materia di Sistema di conservazione e adottati come riferimento nella progettazione ed evoluzione del sistema di conservazione Synapse Theca:

- ISO 14721:2012 OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione;
- ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);
- ETSI TS 101 533-1 V1.3.1 (2012-04) Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- ETSI TR 101 533-2 V1.3.1 (2012-04)Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;
- UNI 11386:2010 Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali;
- ISO 15836:2009 Information and documentation - The Dublin Core metadata element set, Sistema di

metadata del Dublin Core.

- DICOM Standard - Handling, storing, printing, and transmitting information in medical imaging, including a file format definition and a network communications protocol.

Torna al sommario

4. RUOLI E RESPONSABILITÀ

Nell'ambito della fornitura di servizi di conservazione dei documenti informatici risulta essenziale definire ed implementare una struttura organizzativa in grado di garantire, in termini di qualità, professionalità, sicurezza e aderenza alla normativa in essere, i livelli e le esperienze minime richieste dalla normativa stessa.

Per tale ragione il modello adottato dal Conservatore "Syncro-Med Srl" e la conseguente definizione della struttura organizzativa realizzata, è strutturato in accordo con quanto stabilito dalle vigenti regole tecniche ed in particolare con il DPCM 3 dicembre 2013 - articolo 5 "Modelli organizzativi della conservazione".

Tale modello organizzativo è stato realizzato attraverso la definizione di una struttura organizzata di personale altamente qualificato e con esperienza specifica pluriennale consolidata, opportunamente incaricato attraverso nomine esplicite.

Il modello realizzato segue i principi definiti nello standard ISO 14721:2012 - OAIS (Open Archive Information System) che rappresenta il riferimento indiscusso per l'organizzazione dei principi di conservazione.

Secondo quanto indicato dalle Regole tecniche vigenti (DPCM 3 dicembre 2013 - articolo 6), nell'ambito di un processo di conservazione a norma, si identificano 3 ruoli ("soggetti") fondamentali e ben distinti: il Produttore, l'Utente e il Conservatore, come rappresentato nella seguente figura 1.

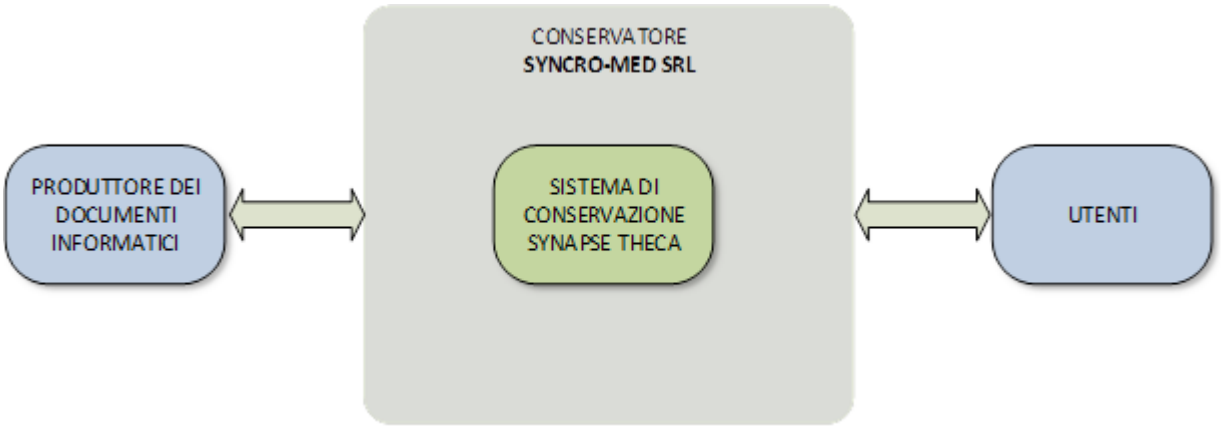

Fig.1 – soggetti coinvolti

Il ***Produttore*** è inteso come persona fisica o giuridica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con responsabile della gestione documentale.

Il Produttore "versa" gli oggetti digitali e le relative informazioni sulla rappresentazione ovvero i metadati da conservare a norma, secondo quanto indicato nelle specifiche tecniche allegate al contratto di affidamento (si parla infatti di "*pacchetti di versamento*" come indicato nel DPCM del 3 dicembre 2013).

Il Produttore, in quanto titolare del documento informatico, è responsabile della formazione del pacchetto di versamento.

L'***Utente*** è il soggetto, come indicato nelle vigenti regole tecniche, che interagisce con i servizi resi disponibili dal sistema di conservazione.

In particolare l'Utente dovrà essere in grado di richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge.

Il Sistema di conservazione dovrà quindi permettere ai soggetti autorizzati l'accesso diretto (anche da remoto) ai documenti informatici conservati estraendo, su richiesta esplicita da parte dell'Utente, i

documenti ricercati (si parla infatti di "*pacchetti di distribuzione*").

Infine il ***Conservatore*** è il soggetto che svolge le attività di conservazione dei documenti informatici tramite il servizio di conservazione (si parla di "pacchetti di archiviazione") ed in ottemperanza a quanto stabilito nel contratto di affidamento.

Il Conservatore, nella persona del proprio Responsabile del servizio di conservazione incaricato, dovrà operare d'intesa con le altre figure costituenti la Struttura Organizzativa, allo scopo di garantire l'attività di conservazione in piena aderenza con quanto specificato nel Modello Organizzativo e conseguentemente in piena osservanza della norma.

Di seguito sono descritti i principali ruoli e le relative attività primarie attribuite, cosi come individuati nel documento "Profili professionali":

Responsabile del servizio di conservazione (RSC)

Il responsabile del servizio di conservazione è colui che si occupa di formalizzare e attuare le politiche complessive del sistema di conservazione, nonché di governare la gestione del sistema di conservazione; inoltre a lui spetta la definizione delle caratteristiche e dei requisiti del sistema di conservazione in accordo con la normativa vigente.

Ha inoltre l'onere e la responsabilità di garantire all'ente Produttore la corretta erogazione del servizio di conservazione; infine gestisce tutte le convenzioni, definisce gli aspetti tecnico-operativi e valida i disciplinari tecnici che specificano gli aspetti di dettaglio e le modalità operative di erogazione dei servizi di conservazione.

Responsabile della funzione archivistica di conservazione (RFA)

Il responsabile della funzione archivistica è colui che definisce e gestisce il processo di conservazione, incluse le modalità di trasferimento da parte dell'ente produttore, di acquisizione, verifica di integrità e descrizione archivistica dei documenti e delle aggregazioni documentali trasferiti, di esibizione, di accesso e fruizione del patrimonio documentario e informativo conservato; definisce il set di metadati di conservazione dei documenti e dei fascicoli informatici.

Inoltre sovraintende il monitoraggio del processo di conservazione e analisi archivistica per lo sviluppo di nuove funzionalità del sistema di conservazione e collabora con l'ente Produttore ai fini del trasferimento in conservazione, della selezione e della gestione dei rapporti con il Ministero dei beni e delle attività culturali per quanto di competenza.

Responsabile del trattamento dei dati personali (RTD)

Il responsabile del trattamento dei dati personali è il garante del rispetto delle vigenti disposizioni in materia di trattamento dei dati personali ovvero garantisce che il trattamento dei dati affidati dal Cliente avvenga nel rispetto delle istruzioni impartite dal titolare del trattamento dei dati personali, con garanzia di sicurezza e di riservatezza.

Responsabile della sicurezza dei sistemi per la conservazione (RSS)

Il responsabile della sicurezza dei sistemi per la conservazione si occupa del monitoraggio continuo e del rispetto dei requisiti di sicurezza del sistema di conservazione stabiliti dagli standard, dalle normative e dalle politiche e procedure interne di sicurezza; inoltre si occupa di segnalare, al Responsabile del servizio di conservazione, ogni eventuale difformità accertata nonché individuare e pianificare le necessarie azioni correttive.

Responsabile dei sistemi informativi per la conservazione (RSI)

Il responsabile dei sistemi informativi per la conservazione gestisce il corretto funzionamento di tutte le componenti hardware e software del sistema di conservazione. Tiene monitorati i livelli di servizio (SLA) concordati con l'ente Produttore e segnala, al Responsabile del servizio di conservazione, eventuali difformità degli SLA, individuando e pianificando le necessarie azioni correttive.

Controlla e verifica inoltre i livelli di servizio erogati da terzi segnalando, sempre al Responsabile del servizio di conservazione, le eventuali difformità.

Infine pianifica lo sviluppo delle infrastrutture tecnologiche del sistema di conservazione.

Responsabile dello sviluppo e manutenzione dei sistemi di conservazione (RSM)

Al responsabile dello sviluppo e manutenzione dei sistemi di conservazione afferisce il compito di coordinare lo sviluppo e la manutenzione delle componenti hardware e software del sistema di conservazione. Governa l'intero ciclo di vita del sistema di conservazione pianificando e monitorando i progetti di sviluppo del sistema unitamente agli SLA relativi alla manutenzione. Si interfaccia, inoltre, con l'ente Produttore in merito alle modalità di trasferimento dei documenti e fascicoli informatici, ai formati elettronici da utilizzare, all'evoluzione tecnologica hardware e software ed alle eventuali migrazioni verso nuove piattaforme tecnologiche. Infine, a tale ruolo compete la gestione dello sviluppo di siti web e portali connessi al servizio di conservazione.

Nella tabella seguente sono riportate le informazioni riguardanti le attribuzioni dei ruoli ai soggetti che attualmente costituiscono la struttura organizzativa descritta.

Ruoli e Nomine

Ruolo	Cognome	Nome	Data di nomina	eventuali deleghe
Responsabile del servizio di conservazione	Nardini	Nicola	08/06/2009	
Responsabile Sicurezza dei sistemi per la conservazione	Veronese	Marco	07/09/2015	
Responsabile funzione archivistica di conservazione	Cafiero	Francesca	16/01/2017	
Responsabile trattamento dati personali	Nardini	Nicola	09/02/2016	

Responsabile sistemi informativi per la conservazione	Salvato	Ivan	09/02/2016	
Responsabile sviluppo e manutenzione del sistema di conservazione	Montel	Marco	08/06/2009	

Torna al sommario

5. STRUTTURA ORGANIZZATIVA PER IL SERVIZIO DI CONSERVAZIONE

5.1 Organigramma

Syncro-Med Srl, in qualità di Conservatore ed in ottemperanza al DPCM del 3 dicembre 2013, ha sviluppato un modello organizzativo i cui ruoli apicali sono espressi nel seguente organigramma:

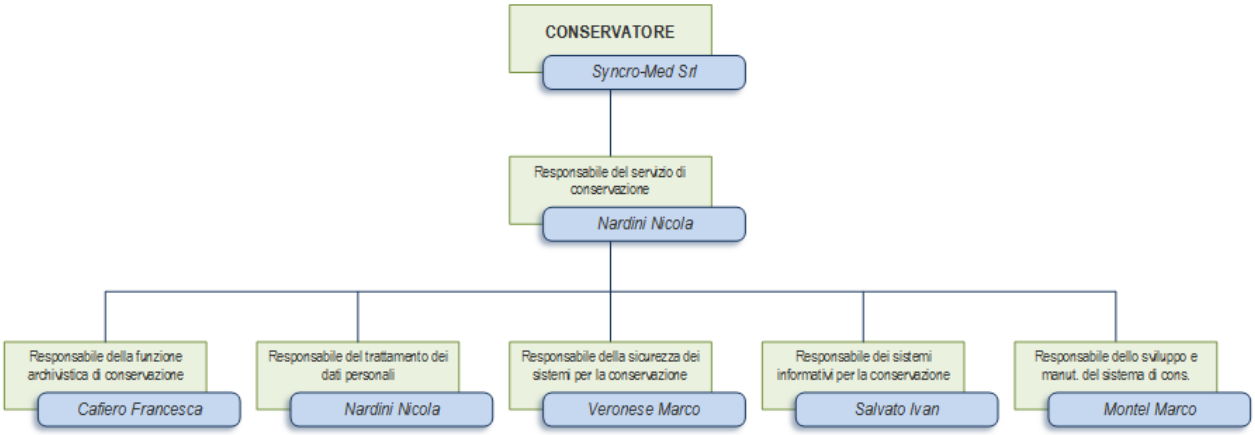

Fig.2 – Organigramma Conservatore

Ciascuno dei responsabili sopra elencati potrà all'occorrenza avvalersi, per lo svolgimento al meglio delle attività e dei compiti ad esso attribuiti, di addetti e/o collaboratori opportunamente e formalmente incaricati.

Torna al sommario

5.2 Strutture organizzative

Nelle varie fasi caratterizzanti il ciclo di vita del processo di conservazione digitale intervengono numerosi soggetti, i principali dei quali indicati e descritti al precedente capitolo 4, ciascuno dei quali è coinvolto a differenti livelli e responsabilità.

In aggiunta ai ruoli previsti espressamente nel DPCM del 3 dicembre 2013 (profili professionali per la

conservazione), nell'ambito della struttura organizzativa Syncro-Med è stata introdotta una nuova figura professionale che si affianca a quelle previste dalla norma.

Tale figura, denominata "Responsabile gestione relazioni con il cliente", ha il compito di gestire i rapporti con il Cliente in ogni fase del processo di conservazione in cui il Cliente abbia e/o richieda la necessita di interagire con la struttura organizzativa del Conservatore Syncro-Med.

Si occuperà quindi, nello specifico, delle seguenti attività primarie:

- interviene nella fase iniziale di attivazione del servizio di conservazione verificando e garantendo la corretta formazione/istruzione del Cliente in merito alle problematiche e peculiarità del processo, sia funzionale che normativo;
- in merito all'attività di verifica e gestione dei pacchetti di versamento, in presenza di problematiche ed errori, si relaziona con il Cliente per chiarire e risolvere, laddove possibile, le problematiche occorse;
- affianca il Cliente, in caso di necessità, nell'attività di preparazione del pacchetto di distribuzione in presenza di un'esibizione;
- affianca il Cliente, in caso di necessità, nel processo di scarto dei pacchetti di archiviazione;
- affianca il Cliente, in caso di necessità, nella stesura e aggiornamento del manuale della conservazione;
- è coinvolta nell'attività di chiusura del servizio e della relativa modalità di comunicazione di chiusura del rapporto con il cliente finale.

Nella tabella seguente sono riepilogate le principali attività che caratterizzano il servizio di conservazione poste in relazione ai ruoli e responsabilità costituenti la struttura organizzativa:

	Responsabile del servizio di conservazione (RSC)	Responsabile della funzione archivistica di conservazione (RFA)	Responsabile del trattamento dei dati personali (RTD)	Responsabile della sicurezza dei sistemi di conservazione (RSS)	Responsabile dei sistemi informativi di conservazione (RSI)	Responsabile sviluppo e manutenzione dei sistemi di conservazione (RSM)	Responsabile gestione relazioni con Cliente (RRC)
Attivazione del servizio di conservazione (a seguito della sottoscrizione di un contratto)	X						X
Acquisizione, verifica e gestione dei pacchetti di versamento presi in carico					X		X
Generazione del rapporto di versamento		X					
Preparazione e gestione del pacchetto di archiviazione		X					
Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione e della produzione di duplicati e copie informatiche su richiesta	X	X					X
Scarto dei pacchetti di archiviazione					X		X
Chiusura del servizio di conservazione (al termine di un contratto)	X						X

	Responsabile del servizio di conservazione (RSC)	Responsabile della funzione archivistica di conservazione (RFA)	Responsabile del trattamento dei dati personali (RTD)	Responsabile della sicurezza dei sistemi di conservazione (RSS)	Responsabile dei sistemi informativi di conservazione (RSI)	Responsabile sviluppo e manutenzione dei sistemi di conservazione (RSM)	Responsabile gestione relazioni con Cliente (RRC)
Conduzione e manutenzione del sistema di conservazione					X	X	
Monitoraggio del sistema di conservazione				X	X		
Change management	X	X	X			X	
Verifica periodica di conformità a normativa e standard di riferimento	X	X		X			
Aggiornamento del manuale di conservazione	X	X					X
Verifica della conformità alle vigenti disposizioni in materia di trattamento dei dati personali			X				

Torna al sommario

6. OGGETTI SOTTOPOSTI A CONSERVAZIONE

Il sistema di conservazione Synapse Theca consiste nell'adozione di regole, procedure e tecnologie al fine di garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità, e reperibilità dei seguenti oggetti:

a) i documenti informatici e i documenti amministrativi informatici con i metadati di catalogazione ad essi associati;

b) i fascicoli informatici con i metadati di catalogazione ad essi associati, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono all'aggregazione documentale.

La soluzione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, se previsto, indipendentemente dall'evolversi del contesto tecnologico.

La soluzione Synapse Theca permette la conservazione di documenti di diversa natura organizzati per strutture logiche omogenee (canali).

Nello specifico è in grado di gestire la conservazione di documenti informatici di natura sanitaria, fiscale e amministrativa. Il processo di conservazione è stato definito in base ad uno studio approfondito della normativa attualmente in vigore; il sistema, inoltre, è in grado di adeguarsi alle scelte di gestione documentale effettuate da ogni singolo cliente.

La definizione completa di tali tipologie corredate dai metadati di catalogazione e le politiche di scarto sono presenti nell'allegato tecnico "Tipologie_documetali.pdf"; di seguito un esempio delle tipologie gestite:

Torna al sommario

6.1 Oggetti conservati

6.1.1 Documenti Fiscalmente rilevanti

Fanno parte di tale tipologia documentale tutti i documenti caratterizzanti una qualsiasi attività (Aziende, Imprese, Professionisti, ecc.) e che abbia una rilevanza ai fini tributari.
Tra questi citiamo a puro titolo d'esempio: Fatture emesse e ricevute, documenti di trasporto, i vari libri (giornale, inventari, cespiti, ecc.), i vari registri (beni ammortizzabili, corrispettivi, fatture emesse, ecc.), bilancio d'esercizio (Stato patrimoniale, Conto economico, Nota integrativa), i libri sociali (Soci, Adunanze e delibere CDA, Adunanze e delibere assemblee soci, ecc.), le varie dichiarazioni (Unico, 730, F24, ecc.), ecc.

Stato analisi	Definita
Norme di riferimento	DMEF 17 giugno 2014 D.Lgs. n.82/2005 CAD DPCM 3 dicembre 2013 DPCM 13 novembre 2014
Termine per la conservazione	Entro il termine di 3 mesi dalla scadenza prevista per la presentazione delle dichiarazioni annuali (tipicamente dicembre dell'anno seguente l'esercizio considerato)
Durata della conservazione	10 anni; 20 se l'Azienda è quotata in borsa
Obblighi Vs. Agenzia Entrate	Indicazione nella dichiarazione dei redditi che la conservazione viene effettuata in modalità elettronica con specifica di quali documenti (situazione mista ammessa). Ove dovuto, pagamento dell'imposta di bollo in un'unica soluzione entro 120 giorni dalla chiusura dell'esercizio.

	Indicazione della conservazione nel Modello A7 e A9.
Metadati obbligatori minimi	Cognome, Nome, Denominazione, Codice Fiscale, Partita IVA, Data documento
Firmati digitalmente	tutti i documenti devono essere firmati: le fatture passive in pdf firmate dal soggetto passivo (eventuale firma automatica); copie analogiche devono essere firmate dal rappresentante legale o da un suo delegato; libri e registri vanno firmati e marcati temporalmente (art. 2215 bis cc .);
Formato del documento	Suggerito: PDF/A Accettato: PDF, XML, TIFF, JPG, TXT

Torna al sommario

6.1.2 Documenti Clinici

In tale tipologia documentale rientrano sia le immagini diagnostiche (eventualmente anche filmati) che i documenti rappresentativi il percorso diagnostico / riabilitativo / lungo degenti, ovvero le varie tipologie di referti (radiologico, cardiologico, screening, laboratorio d'analisi, ecc.) ma anche i

documenti costituenti la CCE (Cartella Clinica Elettronica) nella sua interezza.

Stato analisi	Definita
Norme di riferimento	
Termine per la conservazione	Prima possibile
Durata della conservazione	Immagini diagnostiche: 10 anni per le Referti: a tempo indeterminato CCE : a tempo indeterminato
Obblighi Vs. Agenzia Entrate	N/A
Metadati obbligatori minimi	Identificativo documento, soggetto produttore, soggetto destinatario, data documento; Metadati normati rispetto all'allegato 4 ma da completare nelle specificità in relazione ai singoli contesti clinici
Firmati digitalmente	Referti, tutti i documenti afferenti alla CCE concordati con la struttura erogante;
Formato del documento	Suggerito per Referti e CCE: PDF/A Suggerito per Immagini diagnostiche: DICOM Accettato per Referti e CCE: PDF, XML, TIFF, JPG, TXT

Torna al sommario

6.2 Pacchetto di versamento

Il pacchetto di versamento (PdV) viene generato dal produttore secondo le regole individuate in uno specifico accordo tra le parti (soggetto produttore e soggetto conservatore) in modo tale da assicurare la successiva conservazione dei documenti in esso contenuti e delle relative informazioni connesse (metadati). L'acquisizione di tale pacchetto non può prescindere dalla definizione della sua struttura e della modalità di integrazione.

Queste informazioni sono formalizzate nei documenti tecnici allegati, redatti per ambito di applicazione (clinico, amministrativo "integrazione_amministrativa.pdf").

Di seguito, in fig.3, un esempio del workflow e dello standard di comunicazione HL7 in ambito clinico, formalizzato nel dettaglio nell'allegato "Integrazione_clinica.pdf":

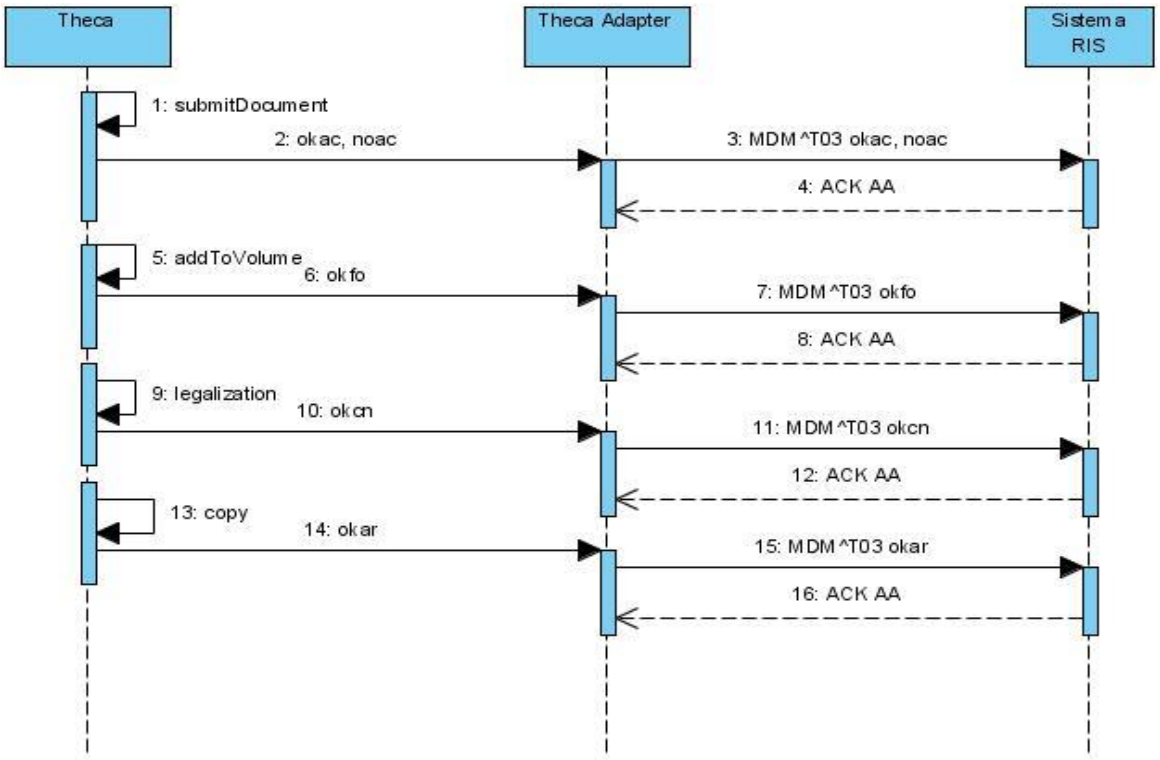

Fig.3 – Esempio di workflow

Il pacchetto di versamento in questo caso sarà così composto:

MSH|^~\&|RIS|SYNCROMED|OP_Application|OP_Facility|20160427114113+0000||MDM^T02^MDM_T02|512856|P|2.5||||||8859/1
EVN||20160427114113+0000
PID|||176165||REFERTOTEST^FIRMATO||19481213000000+0000|M|||||||||RFRFMT01A01A952A
PV1||U|||||||||||||||||||||||||||||||||||USL1|||||||V
TXA||DI||20121231224050+0000|||||^COGNOMEREF^NOMEREFERTANTE|||562714_1|||9-28-736163||LA
OBX|1|ED|562714_1|P7M|MILpRAYJpbGVuYW1lPTs.....=||||||F

La modalità di versamento può avvenire in forma automatizzata, con un'integrazione diretta tra il sistema sorgente e quello di conservazione, oppure manuale, utilizzando dell'apposito task di upload.

La soluzione Synapse Theca inoltre può effettuare controlli di diversa natura e a diversi livelli sul pacchetto e sul suo contenuto in funzione della configurazione scelta dal responsabile della conservazione per quella determinata tipologia documentale.

Torna al sommario

6.3 Pacchetto di archiviazione

Il pacchetto di archiviazione è un derivato di uno o più pacchetti di versamento che vengono affidati all'OAIS con il fine di archiviare i dati contenuti.

E' composto da:

- uno o più documenti o aggregazioni documentali corredate dai necessari metadati di fascicolazione, concordati nel contratto di servizio, sottoposti al processo di conservazione;
- un indice (IPdA) del pacchetto stesso formattato in conformità dello standard UNI SInCRO come da disposizione presente nel DPCM del 3 dicembre 2013.

- rapporto di versamento

Il processo di gestione del pacchetto di archiviazione può essere scomposto nelle seguenti fasi:

- Creazione pacchetto
    - Fascicolazione
        - Il Folder è una raccolta di una tipologia omogenea di documenti, acquisiti su un certo canale, effettuata secondo criteri legati ai metadati a corredo di ogni PdV.
    - Consolidamento del pacchetto
        - Il Pacchetto è una raccolta di fascicoli creato a fronte di criteri temporali o dimensionali definiti in fase di configurazione della soluzione ed è quindi adattabile alle diverse esigenze operative.
- Conservazione pacchetto
    - Consiste nella firma digitale e nell'apposizione della marca temporale del pacchetto ossia dell'indice di conservazione (idPA) e del rapporto di versamento da parte del responsabile della conservazione o di uno dei suoi delegati.

Torna al sommario

6.3.1 Indice del pacchetto di archiviazione (IPdA)

L'IPda è come definito nelle nuove regole tecniche l'evidenza informatica legata ad ogni PDA contente una serie di informazioni, strutturate secondo standard UNI SInCRO, necessarie alla sua conservazione.

Tale standard offre la possibilità di costruire il file in due differenti modalità rispetto ai metadati contenenti le informazioni ulteriori (MoreInfo). Possono infatti essere inseriti direttamente all'interno dell'indice di conservazione (EmbeddedMetadata) o all'esterno (ExternalMetadata). Synapse Theca adotta questa seconda metodologia implementativa andando, all'interno del tag <extrainfo>, solo a referenziare il file xml dei metadati esterno.

Di seguito un esempio del IdPA Synapse Theca:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<IdC ns1:version="1.0" xmlns:ns1=" http://www.uni.com/U3011/sincro//">
        <ns1:SelfDescription>
                <ns1:ID ns1:scheme="local">CLINICA_425_index</ns1:ID>
                <ns1:CreatingApplication>
                        <ns1:Name>Synapse Theca</ns1:Name>
                        <ns1:Version>1.3.3.8</ns1:Version>
                        <ns1:Producer>Syncro-Med</ns1:Producer>
                </ns1:CreatingApplication>
        </ns1:SelfDescription>
        <ns1:VdC>
                <ns1:ID ns1:scheme="local">CLINICA_425</ns1:ID>
                <ns1:VdCGroup>
                        <ns1:Label>CLINICA</ns1:Label>
                        <ns1:ID ns1:scheme="local">IDCANALE1</ns1:ID>
                        <ns1:Description ns1:language="IT">CLINICA</ns1:Description>
                </ns1:VdCGroup>
        </ns1:VdC>
        <ns1:FileGroup>
                <ns1:Label>FOLDERID1</ns1:Label>
                <ns1:File ns1:encoding="binary" ns1:format="application/PDF">
                        <ns1:ID ns1:scheme="local">IDDOCUMENT1</ns1:ID>
                        <ns1:Path>file://87507961//CLIN-882139</ns1:Path>
                        <ns1:Hashns1:function="SHA-256">4F073C3DADBCD</ns1:Hash>
                </ns1:File>
                <ns1:MoreInfo>
                        <ns1:ExternalMetadata>
                                <ns1:ID ns1:scheme="local">IDDOCUMENT1_META</ns1:ID>
                                <ns1:Path>file://87507961//CLIN-882139.xml</ns1:Path>
                                <ns1:Hashns1:function="SHA-256">429A8C5FA426F98DAE761A61</ns1:Hash>
                        </ns1:ExternalMetadata>
                </ns1:MoreInfo>
        </ns1:FileGroup>
      <ns1:Process>
         <ns1:Agent ns1:otherRole="Syncromed" ns1:role="OtherRole" ns1:type="person">
        <ns1:AgentName>
                <ns1:NameAndSurname>
                        <ns1:FirstName>Nome amministratore</ns1:FirstName>
                        <ns1:LastName>Cognome amministratore</ns1:LastName>
                        </ns1:NameAndSurname>
                        </ns1:AgentName>
                        <ns1:Agent_I ns1:scheme="TaxCode">CFRESPONSABILE</ns1:Agent_ID>
                </ns1:Agent>
                <ns1:TimeReference>
                        <ns1:AttachedTimeStamp>2015-11-27T00:00:01+01:00</ns1:AttachedTimeStamp>
                </ns1:TimeReference>
        </ns1:Process>
       </IdC>
```

Torna al sommario

6.4 Pacchetto di distribuzione

Il pacchetto di distribuzione è un pacchetto informativo che viene ricevuto dall'utente (o Consumatore secondo la terminologia OAIS) come risposta ad una richiesta di contenuto inoltrata al sistema di conservazione.

E' formato da:

L'indice del pacchetto di distribuzione definito secondo standard UNI SInCRO:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<IdC ns1:version="1.0" xmlns:ns1="http://www.uni.com/U3011/sincro/">
 <ns1:SelfDescription>
  <ns1:ID ns1:scheme="local">ESIBIZIONE_index</ns1:ID>
  <ns1:CreatingApplication>
   <ns1:Name>Synapse Theca</ns1:Name>
   <ns1:Version>1.3.3.9</ns1:Version>
   <ns1:Producer>Syncro-Med</ns1:Producer>
  </ns1:CreatingApplication>
 </ns1:SelfDescription>
 <ns1:VdC>
  <ns1:ID ns1:scheme="local">ESIBIZIONE1</ns1:ID>
  <ns1:VdCGroup>
   <ns1:Label>ESIBIZIONEMARCO</ns1:Label>
   <ns1:ID ns1:scheme="local">TODO</ns1:ID>
   <ns1:Description ns1:language="IT">ESIBIZIONE1</ns1:Description>
  </ns1:VdCGroup>
 </ns1:VdC>
 <ns1:FileGroup>
  <ns1:Label>FOLDERID1</ns1:Label>
  <ns1:File ns1:encoding="binary" ns1:format="application/NONPDF">
   <ns1:ID ns1:scheme="local">IDOCUMENT1</ns1:ID>
   <ns1:Path>file://R6OCHYYN//REFE-82</ns1:Path>
   <ns1:Hash ns1:function="SHA-
256">F436A47B57DD1BBC7EC85A5128E01E6CA83977397627E0FDEE9281048</ns1:Hash>
  </ns1:File>
  <ns1:MoreInfo>
   <ns1:ExternalMetadata>
    <ns1:ID ns1:scheme="local"> IDOCUMENT1_META</ns1:ID>
    <ns1:Path>file://R6OCHYYN//REFE-82.xml</ns1:Path>
    <ns1:Hash ns1:function="SHA-
256">5FB154BEFBAF078220E94E2D955AC51BC9BE46B5B7E88791A10E94F9B0</ns1:Hash>
   </ns1:ExternalMetadata>
  </ns1:MoreInfo>
```

```
</ns1:FileGroup>
<ns1:Process>
 <ns1:Agent ns1:type="person" ns1:role="OtherRole" ns1:otherRole="Syncromed">
  <ns1:AgentName>
   <ns1:NameAndSurname>
    <ns1:FirstName>Nome amministratore</ns1:FirstName>
    <ns1:LastName>Cognome amministratore</ns1:LastName>
   </ns1:NameAndSurname>
  </ns1:AgentName>
  <ns1:Agent_ID ns1:scheme="TaxCode"> CFUTENTEESIBITORE</ns1:Agent_ID>
 </ns1:Agent>
 <ns1:TimeReference>
  <ns1:AttachedTimeStamp>2016-02-29T09:24:22+01:00</ns1:AttachedTimeStamp>
 </ns1:TimeReference>
</ns1:Process>
</IdC>
```

- I documenti richiesti, ricercati all'interno dell'applicazione grazie ad ai metadati di catalogazione;
- IdPA dei documenti richiesti;
- Un report in formato PDF, come riportato nella figura seguente (Fig.4) con il quale il responsabile del procedimento di conservazione a norma dichiara quali duplicati informatici sono stati prodotti:

Ragione sociale

indirizzo, nn CAP Citta(XX)

tel 00000 - Fax 1111111

VERBALE DI ESIBIZIONE DEI DOCUMENTI CONSERVATI

Il/La Sottoscritto/a admin Nome amministratore, Responsabile (o suo delegato) del sistema di conservazione della documentazione informatica clinica testuale, iconografica e grafica, nell'ambito della scrivente unità operativa, e su espressa richiesta delle Autorità competenti,

DICHIARA

che in data odierna è stato prodotto, in conformità alla regole tecniche previste dall'art. 71 del D.Lgs 82/2005, un supporto di memorizzazione contenente i duplicati informatici dei sottoelencati documenti riferiti al Paziente:

ID Paziente: LjK8inJ4
Nome: VJRO1USU
Cognome: CHO0B2EH
Sesso: M
Data di nascita: 19220624
Codice Fiscale: CTRGRG22H24A390A

Nome documento	Formato	Impronta
1280413	NONPDF	F436A47B57DD1BBC7EC85A5128E01E6CA83977397627E0FDEE9281048BA5A923

Tali duplicati informatici hanno, ai sensi e per gli effetti dell'art. 23 bis, comma1, del D.Lgs 82/2005 il medesimo valore giuridico, ad ogni effetto di legge, dei documenti informatici conservati presso il sistema di conservazione Legale.

Fig.4 – Verbale di esibizione

Torna al sommario

7. IL PROCESSO DI CONSERVAZIONE

L'immagine seguente rappresenta lo standard OAIS (Open Archival Information System) sul quale si basano le componenti logiche funzionali del sistema Synapse Theca. Questo schema definisce le caratteristiche fondamentali di una soluzione finalizzata alla conservazione di documenti informatici, nel rispetto delle regole tecniche vigenti.

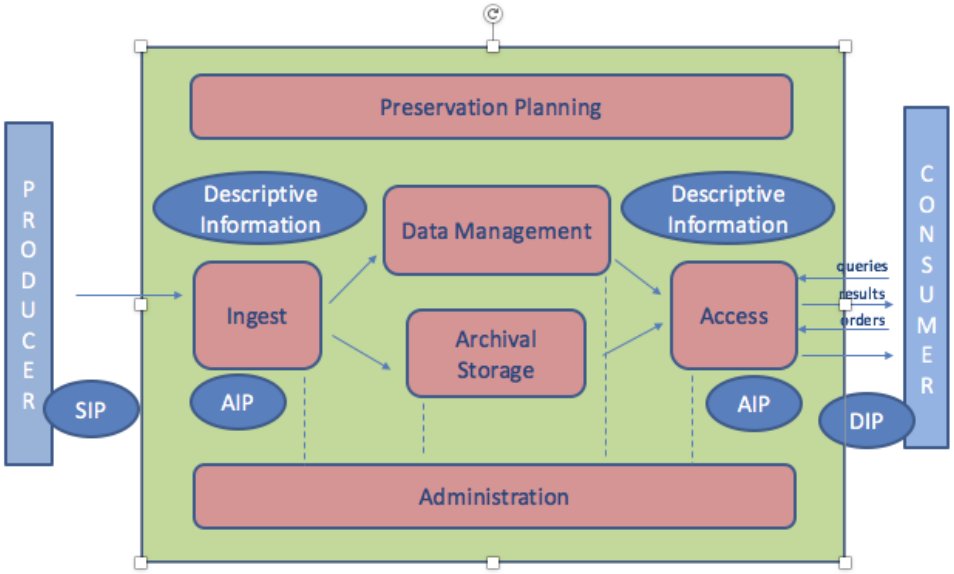

Fig.5 – Modello OAIS

Il sistema di conservazione Synapse Theca garantisce sia una corretta gestione del documento informatico che la sua successiva conservazione adottando modelli organizzativi distinti per le singole fasi.

In fase di gestione il sistema permette di:

- Acquisire documenti, immagini e metadati, verificandone l'integrità e la validità. Tale acquisizione avviene su canali creati in funzione delle tipologie documentali trattate in maniera tale da sottoporre aggregazioni documentali omogenee al flusso di conservazione. Questo

approccio implementativo permette una corretta gestione delle politiche di scarto che, come noto, sono differenti a seconda della tipologia documentale;

- consolidare, ove richiesto, i documenti così come previsto dalle "Linee guida per la dematerializzazione della documentazione clinica in diagnostica per immagini – Normativa e prassi" approvate il 4 aprile 2012 in Conferenza Stato Regioni (Rep. Atti n. 81/CSR del 4 aprile 2012);
- fascicolare i dati in preparazione della conservazione legale;
- predisporre il PdV secondo gli accordi previsti con il Cliente.

La fase di conservazione permette poi di:

- conservare e archiviare i dati, attraverso il processo di creazione delle impronte dei documenti e la costituzione di un file indice, contenente le impronte create, firmato e marcato digitalmente;
- verificare periodicamente la leggibilità dei supporti e la conformità dei PdA;
- riversare, se ritenuto opportuno (ad esempio per motivi di obsolescenza tecnologica e/o fine ciclo di vita dei supporti correnti), i PdA dal supporto corrente ad un nuovo supporto di memorizzazione;
- esibire i dati archiviati.

Torna al sommario

7.1 Modalità di acquisizione dei pacchetti di versamento per la loro presa in carico

L'acquisizione in Synapse Theca al fine della formazione del PdV avviene in due modalità:

- ***manuale*:**
  con l'ausilio di un task di upload web, l'utente può caricare i documenti da conservare e i

relativi metadati necessari per la corretta conservazione (elementi che costituiscono il Pacchetto di Versamento) . Alcuni di questi metadati possono essere impostati obbligatori e ne viene data evidenza con il colore giallo. Inoltre è possibile sottoporre i metadati ad una specifica validazione, verificando ad esempio che i campi data o numerici non vadano ad accettare stringhe di diversa natura.

I metadati da inserire dipendono dal canale, in cui si intende caricare il documento, al quale è legato un modello dati definito con il Cliente. Al termine dell'inserimento di tutti i metadati obbligatori il documento viene versato dal Produttore nel sistema di conservazione. Al termine del caricamento se tutte le validazioni definite per il PdV vengono soddisfatte, il sistema visualizza il messaggio di conferma "*Upload completato*" altrimenti da evidenza dell'eventuale problematica nell'apposito box. Ogni documento acquisito viene preso in carico e aggiunto al pacchetto di versamento che in quel momento risulta aperto per il canale selezionato.

Per ogni documento caricato viene loggato:

- data e ora caricamento
- utente che ha effettuato l'operazione

- ***automatica*:**

  i pacchetti di versamento sono trasmessi agli adapter (vedasi capitolo 8.1) utilizzando una metodologia di integrazione definita nell'allegato tecnico di ciascuna installazione. Vengono scelti gli standard riconosciuti in ognuno dei contesti in cui si sta operando (es: HL7 ambito clinico).

  Le interfacce standard esposte dalla soluzione sono cifrate (es: https) o nel caso non sia possibile, per la natura stessa dello standard, protette dall'infrastruttura (VPN, Firewall) stessa scelta e concordata con il cliente stesso.

  Ogni adapter ha un proprio log che viene portato periodicamente in conservazione e che

contiene:

- data ora della trasmissione
- eventuale problematica
- pacchetto inviato

La chiusura del pacchetto di versamento con la conseguente generazione del RdV ed il suo trasferimento al sistema di conservazione possono essere configurate in modalità

- ***manuale***: in qualunque momento un utente, correttamente profilato, può chiudere il pacchetto di versamento e procedere con la firma e conseguente versamento del PdV al sistema di conservazione;

- ***automatica*** secondo le seguenti modalità:
  - Dimensione massima: la dimensione massima dei pacchetti di versamento è calcolata automaticamente in base alla dimensione minima dei supporti utilizzati. Tale dimensione può essere adattata. Il sistema valida il valore immesso in modo che questo non superi la dimensione dei supporti configurati per quel canale di trasmissione.
  - Temporizzatori: è possibile impostare la creazione automatica dei pacchetti in base a dei temporizzatori che sono di tre tipi:
    - Durata: si stabilisce il tempo massimo di attesa prima che un pacchetto versamento venga versato nel sistema di conservazione (in termini di minuti, ore, o giorni);
    - Intervallo: si stabilisce l'intervallo di tempo a partire dalle ore 0:00AM per un pacchetto versamento prima di essere versato nel sistema di conservazione (in termini di minuti, ore, o giorni); ad ogni intervallo successivo al primo scatta il temporizzatore di chiusura;
    - Calendario: si stabilisce in quali giorni della settima scatta il temporizzatore

di chiusura (con orario fisso alle 0:00AM)

Torna al sommario

7.2 Verifiche effettuate sui pacchetti di versamento e sugli oggetti in essi contenuti

La soluzione Synapse Theca effettua alcune verifiche sui pacchetti di versamento anche sulla base degli accordi intercorsi con il Cliente/Produttore tramite la configurazione della componente logica denominata "adapter" specificata al paragrafo 8.1:

- contenuto:

  a) viene effettuata la verifica che il pacchetto non contenga un documento nullo;
  b) viene verificato che non vi sia un documento informatico identico ad uno precedentemente caricato;

- firma digitale:

  viene effettuata, se la tipologia documentale lo prevede, la verifica della firma che consiste:

  a) nella verifica dell'integrità del documento rispetto all'hash contenuto nella firma digitale.

  b) viene verificato se il certificato di firma è valido e non revocato.

- Identificazione certa del soggetto produttore:

  Per identificare in maniera certa chi ha firmato, viene letto il codice fiscale dal certificato di firma del documento stesso. Configurando l'apposita sezione dell'applicativo, inserendo i codici fiscali accettati, è possibile rifiutare i documenti prodotti da soggetti non previsti;

- Estensione del documento: il sistema può accettare solo determinati formati di documento verificando il contenuto binario del file;

- Errori di provenienza:

  in alcune tipologie di integrazioni è possibile verificare anche il sistema inviante specificato all'interno del messaggio, utilizzato come veicolo per il documento da conservare, oppure

verificando l'identificazione (aetitle) del soggetto produttore presente nel protocollo di integrazione.

Per ogni pacchetto di versamento viene tracciato uno ***storico*** nel quale sono riportati riferimenti temporali relativi alle diverse elaborazioni, nonché la descrizione di ogni singola fase ed una serie di codici che identificano i vari stati che vengono attribuiti al documento (a puro titolo di esempio: "OKAC acquisito", "OKCN conservato" come riportato in fig.6). E' presente il riferimento all'utente che ha preso in carico il documento nei vari momenti della sua elaborazione. I log generati vengono portati in conservazione dalla soluzione stessa in un canale di conservazione dedicato.

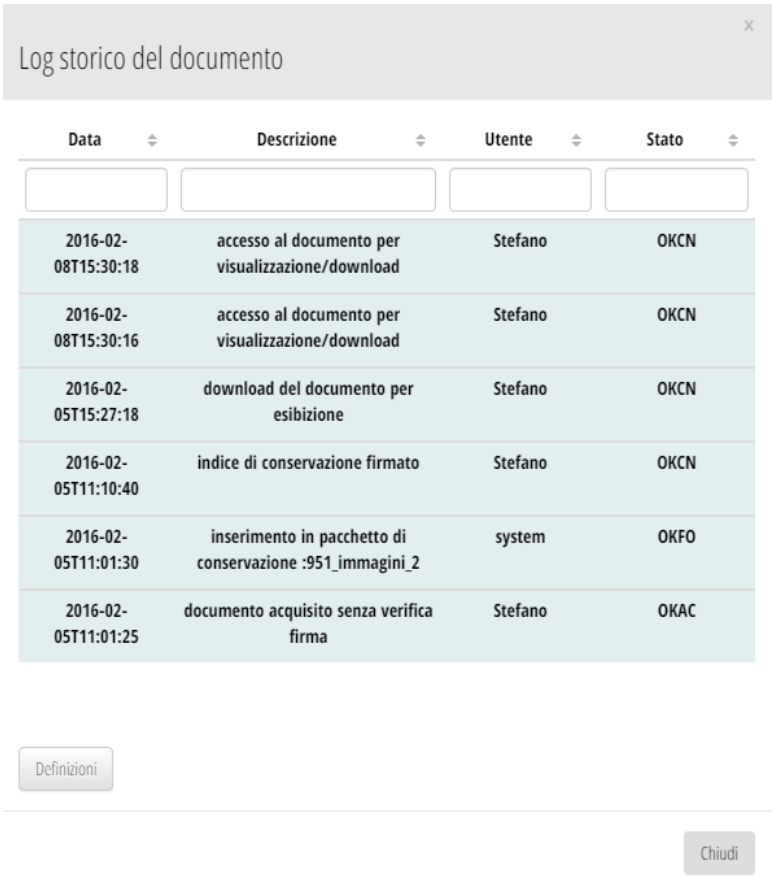

Fig.6 – Esempio di log storico

Di seguito un breve esempio dell'analisi effettuata sui documenti contenuti nel PdV in ambito clinico:

ANALISI DOCUMENTI			
Nome documento	F = forte	M: modificabile	O=obbligatorio
	D = debole	F. non modif.	F= facoltativo
	Firma digitale	**Modifica**	**Conservazione**
Referto clinico	F	F	O
Immagine clinica	F	F	O
Ricovero ordinario	D	F	O
Consulenza internistica	F	F	O

Il PdV potrà essere formato da documenti informatici firmati secondo le specifiche tecniche PadES (ETSI TS 103172), CadES (ETSI TS 103173) e XadES (ETSI TS 103171) ma anche, nel caso l'accordo tra le parti lo consenta, di qualunque altro oggetto informatico in uno dei formati indicati nell'allegato 2 al DPCM 3 dicembre 2013.

Synapse Theca prevede la possibilità di abilitare il consolidamento probatorio che consiste nell'apposizione di una marca temporale rilasciata da una TSA su ogni singolo pacchetto ricevuto in modo da garantirne l'integrità e estendere la validità nel tempo di eventuali firme digitali presenti. Tale consolidamento da un effettivo valore aggiunto nel momento in cui è stato definito un lasso di tempo non trascurabile tra l'invio del PdV da parte del sistema sorgente e l'effettiva presa in carico dal sistema di conservazione con la conseguente generazione del RdV e la successiva creazione del PdA.

A fronte delle verifiche sopracitate è possibile che il pacchetto venga:

1 **accettato**: in questo caso tutte le verifiche sono andate a buon fine quindi il

pacchetto viene caricato ne viene calcolata l'impronta che verrà inserita nel IdPA e vengono acquisiti i suoi metadati ;

2 **identificato non conforme**: grazie ad una particolare configurazione della soluzione è possibile, a fronte di un'anomalia riscontrata, lasciare al RdC la scelta se portare il dato comunque in conservazione. Tale operazione opera verrà tracciata all'interno dello storico del documento.

3 **rigettato**: in questo caso il pacchetto viene rigettato dandone evidenza al sistema sorgente così come definito nell'integrazione concordata.

Torna al sommario

7.3 Accettazione dei pacchetti di versamento e generazione del rapporto di versamento di presa in carico

L'accettazione del PdV, a seconda della modalità di acquisizione concordata (manuale con l'utilizzo del task di upload o automatica mediante l'integrazione concordata in fase progettuale), viene tracciata nei log di seguito riportati:

Versamento automatico (log adapter integrazione):


```
            <XCN.1>BBRRTR58L18L328L</XCN.1>
            <XCN.2>
                <FN.1>WbsLMKbg</FN.1>
            </XCN.2>
            <XCN.3>g7zje3pb</XCN.3>
            <XCN.9>
                <HD.1>CF</HD.1>
            </XCN.9>
        </TXA.9>
        <TXA.12>
            <EI.1>UiGsSfxf</EI.1>
        </TXA.12>
        <TXA.14>
            <EI.1>PS5569263</EI.1>
        </TXA.14>
        <TXA.15>
            <EI.1>bsBBB9DB</EI.1>
        </TXA.15>
        <TXA.16>Referto669100_v1.pdf</TXA.16>
        <TXA.17>LA</TXA.17>
        <TXA.22>
            <PPN.1>BBRRTR58L18L328L</PPN.1>
            <PPN.2>
                <FN.1>8eHaJuzK</FN.1>
            </PPN.2>
            <PPN.3>nEQBRPb7</PPN.3>
            <PPN.9>
                <HD.1>CF</HD.1>
            </PPN.9>
            <PPN.15>
                <TS.1>20120201013103</TS.1>
            </PPN.15>
        </TXA.22>
    </TXA>
    <OBX>
        <OBX.2>ED</OBX.2>
        <OBX.3>
            <CE.1>1561753</CE.1>
        </OBX.3>
        <OBX.4>PDF</OBX.4>
        <OBX.5>
            <ED.2>multipart</ED.2>
            <ED.3>Octet-stream</ED.3>
            <ED.4>Base64</ED.4>
            <ED.5>TWltZS1WZXJzaW9uOiAxLjAKQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvbWl4ZWQ7IGJvdW5kYXJ5PSJTaXNzIgoKLS1TaXNzCkNvbnRlbnQtVHlwZTogYXBwbGljYXRpb24vcGtjczctbWltZTsgc21pbWUtdHlwZT1zaWduZWQtZGF0YTsgbmFtZT0iY29udGVudC5wN20iCkNvbnRlbnQtVHJhbnNmZXItRW
            5jb2Rpbmc6IGJhc2U2NApDb250ZW50LURpc3Bvc2l0aW9uOiBhdHRhY2htZW50OyBmaWxlbmFtZT0iY29udGVudC5wN20iCkNvbnRlbnQtRGVzY3JpcHRpb246IENBZEVTIFNpZ25lZCBlbnZlbG9wZQoKTUlBR0NTcUdTSWIzRFFFSEFxQ0FNSUFDQVFFeER6QU5CZ2xnaGtnQlpRTUVBZ0VGQURDQUJna3Foa2lHOX
            cwQkJ3R2dnQ1NBQklNQgpkTHdsVUVSR0xURXVOQTBLSmVMano5TU5DakVnTUNCdlltb05DaUFnUER3TkNpQWdJQ0F2UVhWMGFHOXlLQ2t2VkdsMGJHVW9LUzlUCmRXSnFaV04wS0NrdlVISnZaSFZqWlhJb1UzVmlJRk41YzNSbGJYTXNJRWx1WXk0cEwwdGxlWGR2Y21SektDa3ZRM0psWVhScGIyNUUKWVhSbEtFUT
            ZNakF4TmpFd01Ua3hNakU0TkRVck1EQW5NREFuS1M5TmIyUkVZWFJsS0VRNk1qQXhOakV3TVRreE1qRTRORFVyTURBbgpNREFuS1M5RGNtVmhkRzl5S0ZOMVlpQlRlWE4wWlcxekxDQkpibU11SUMwZ2NHUmpOeWtOQ2lBZ1BqNE5DbVZ1Wkc5aWFnMEtNaUF3CklHOWlhZzBLUER3dlRHVnVaM1JvSURJME56TXZVM1
            ZpZEhsd1pTOVlUVXd2Vkhsd1pTOU5aWFJoWkdGMFlUNCtEUXB6ZEhKbFlXME4KQ2p3L2VIQmhZMnRsZENaVpXZHBiajBuNzd1L0p5QnBaRDBuVnpWTk1FMXdRMlZvYVVVoNmNtVlRlazVVWTNwcll6bGtKejgrQ2lBZwpQSGc2ZUcxd2JXVjBZU0I0T25odGNIUnJQU2N6TGpFdE56QXhKeUI0Yld4dWN6cDRQU2RoWk
            c5aVpUcHVjenB0WlhSaEx5Y2dQZ29nCklDQWdQSEprWmpwU1JFWWdlRzFzYm5NNmNtUm1QU2RvZEhSd09pOHZkM2QzTG5jekxtOXlaeTh4T1RrNUx6QXlMekl5TFFhKa1ppMXoKZVc1MFlYZ3Ribk1qSno0S0lDQWdJQ0FnUEhKa1pqcEVaWE5qY21sd2RHbHBZiaUJ5WkdZNllXSnZkWFE5SLQ==</ED.5>
        </OBX.5>
        <OBX.11>F</OBX.11>
    </OBX>
    <OBX>
        <OBX.2>CE</OBX.2>
        <OBX.3>
            <CE.1>1561753</CE.1>
        </OBX.3>
        <OBX.4>PDF</OBX.4>
        <OBX.5>
            <CE.2>multipart</CE.2>
            <CE.3>Octet-stream</CE.3>
            <CE.4>Base64</CE.4>
            <CE.5>1</CE.5>
        </OBX.5>
        <OBX.11>F</OBX.11>
    </OBX>
</MDM_T02>
```


```
gen 16, 2017 5:01:58 PM com.syncromed.theca.adapter.service.hl7.HL7Listener receiveMessage
INFO: [HL7LI] REFERTI Ricevuto MDM_T02: 189,0 kB, caricamento in corso...

INFO: [SIGNS] Inizializzazione servizio firma. Classe: com.syncromed.theca.sign.controller.aruba.HsmArubaHashSignRemote
gen 16, 2017 5:03:00 PM com.syncromed.theca.sign.boundary.SignServiceFactory getNewInstance
INFO: [SIGNS] Inizializzazione servizio firma. Classe: com.syncromed.theca.sign.controller.aruba.HsmArubaHashSignRemote
gen 16, 2017 5:03:00 PM com.syncromed.theca.sign.boundary.SignServiceFactory getNewInstance
INFO: [SIGNS] Inizializzazione servizio firma. Classe: com.syncromed.theca.sign.controller.aruba.HsmArubaHashSignRemote
gen 16, 2017 5:03:04 PM com.syncromed.theca.adapter.syncromed.HL7FileImportProcessor sendDocument
INFO: [ACDOC] 1561753 Stato Firma Digitale: SignCheck{description=null, signCheckStatus=signed, certStatus=good, signStatus=validSignature}
gen 16, 2017 5:03:10 PM com.syncromed.theca.helper.FileSystemHelper fileSystemStore
INFO: [STORE] Creato Percorso : F:\REFERTI\IMPORT\BSBBB9DB
gen 16, 2017 5:03:11 PM com.syncromed.theca.adapter.service.hl7.HL7Listener receiveMessage
INFO: [HL7LI] REFERTI Ricevuto MDM_T02: 189,0 kB, caricamento effettuato
```

Fig.7 – Esempio log versamento automatico

Versamento manuale (log applicativo task di upload):

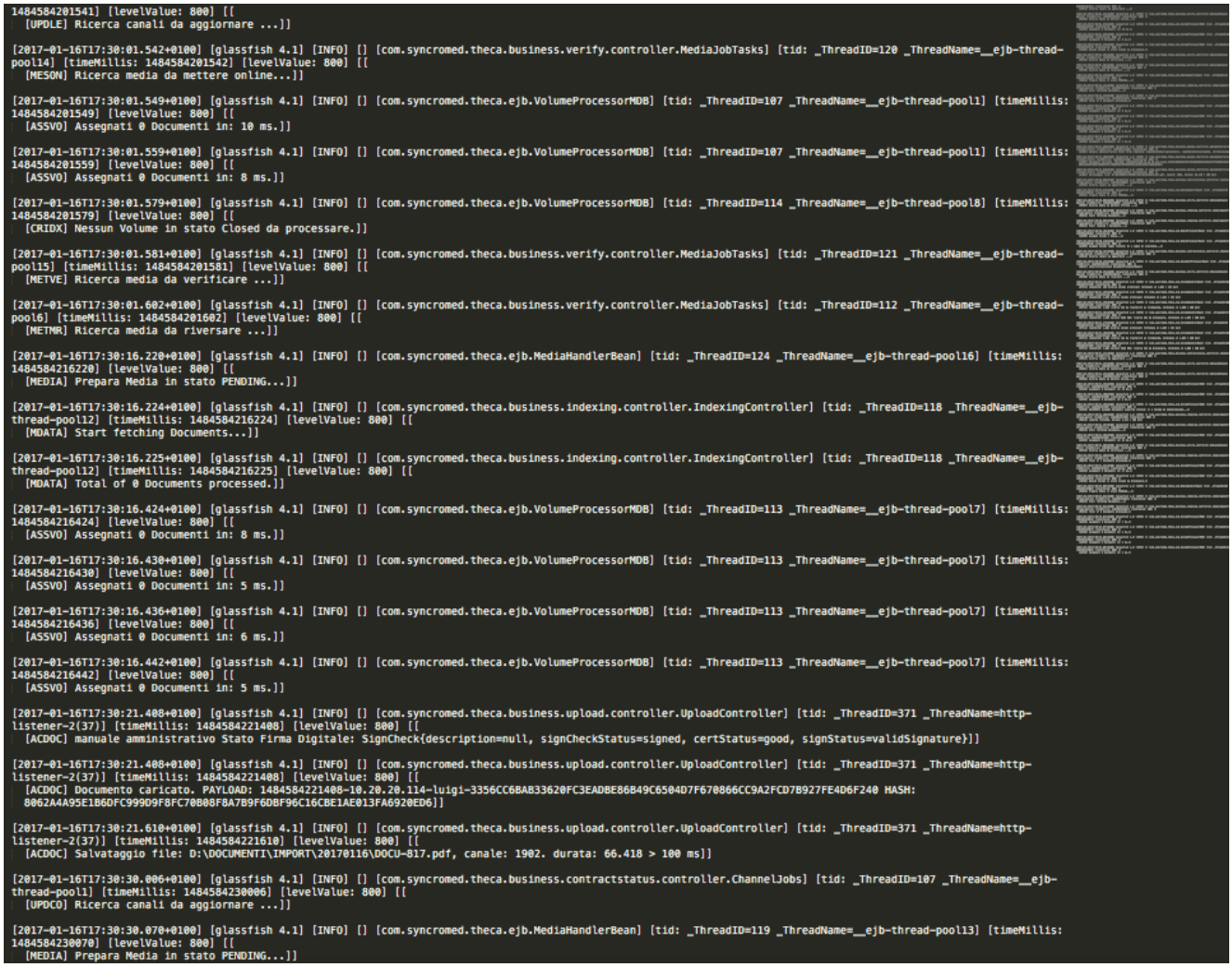

Fig.8 – Esempio log versamento manuale

Entrambe le tipologie vengono portate in conservazione nell'apposito canale dedicato. A seguito dell'accettazione del PdV il sistema provvederà a generare, anche in modo automatico, un rapporto di versamento in formato XML relativo a uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente una marca temporale emessa da una TSA (Time Stamping Authority) accreditata presso AgID. Il RdV, eventualmente firmato, viene conservato insieme ad una o più impronte calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità

concordate con il Produttore. Tale operazione è necessaria per garantire la validità della firma digitale oltre il periodo di validità del relativo certificato di sottoscrizione. Le tempistiche di generazione e l'eventuale sottoscrizione del rapporto di versamento con firma elettronica qualificata o firma digitale apposta dal RdC, vengono descritte nel manuale della conservazione di ogni singolo Produttore e definite in sede di accordo di versamento.

Ogni RdV generato dovrà essere univocamente identificato dal sistema e sarà composto da:

- un riferimento al pacchetto di versamento;
- un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC) relativo alla sua generazione;
- una o più impronte calcolate sull'intero contenuto del pacchetto di versamento al quale si riferisce.

Il RdV viene conservato all'interno del pacchetto di archiviazione composto dai documenti referenzianti all'interno del rapporto stesso. Il RdV potrà essere visualizzato ricercando uno o più documenti in esso contenuti.

Il rapporto di versamento è formato in un momento successivo a quello della ricezione del pacchetto di versamento e precedente o contestuale alla creazione del pacchetto di archiviazione.

La fase di versamento e verifica sono delle attività a supporto del sistema di produzione mentre la creazione del RdV, che viene effettuata al raggiungimento dei limiti configurati sulla creazione del pacchetto, identifica la vera e propria presa in carico del PdV da parte del sistema di conservazione.

Il RdV è generato in formato XML e viene sottoposto in automatico alla firma e alla marcatura temporale insieme all'indice di conservazione relativo al pacchetto di archiviazione creato.

Torna al sommario

7.4 Rifiuto dei pacchetti di versamento e modalità di comunicazione delle anomalie

Il PdV che non soddisfa le verifiche effettuate dal sistema di conservazione viene a seconda della natura di acquisizione gestito come di seguito riportato:

a) acquisizione automatica, tracciato nel file di log dell'adapter con l'indicazione dell'anomalia riscontrata;

b) acquisizione manuale dando evidenza all'utente della problematica riscontrata, impedendo il versamento del documento in conservazione.

Le anomalie che possono comportare il rifiuto di un pacchetto di versamento sono elencate di seguito:

- il PdV non rispecchia il tracciato definito in fase progettuale quindi non può essere correttamente interpretato (es: standard HL7, xsd in caso di struttura xml);
- Il documento non rispecchia il formato concordato;
- il documento è già presente nel sistema;
- il formato dei metadati non rispecchia quanto definito nell'allegato tecnico progettuale;
- l'identificazione del mittente non è possibile o non rispecchia quanto configurato;
- la firma digitale apposta al documento contenuto nel PdV non è valida (certificato scaduto o revocato). Questo tipo di controllo è configurabile a livello di canale di acquisizione o di tipologia documentale. I documenti che non soddisfano i requisiti impostati verranno marcati all'interno della soluzione come "rigettati" e sarà compito del RdC decidere se scartarli definitivamente o procedere comunque con la loro conservazione.

In funzione della modalità di versamento definita in fase progettuale/contrattuale vi saranno differenti tipologie di evidenze dello scarto del PdV:

- *Versamento automatico*:

  In questo caso dove è presente un'integrazione tra il sistema sorgente e quello di conservazione, la notifica della mancata acquisizione del pacchetto di versamento è demandata alla logica implementativa. Ad esempio in contesto clinico, nello standard HL7, vi è un Acknowledge di

risposta ad ogni messaggio inviato nel quale è specificato l'esito del versamento e l'eventuale motivazione di scarto. Le risposte che hanno esito negativo vengono loggate e conseguentemente conservate.

Tale logica verrà applicata, nelle modalità concordate, per ogni tipologia di integrazione e indipendentemente dalla natura e dal contesto in cui si sta operando (es: clinico, amministrativo, ecc).

Di seguito un esempio di log contente un pacchetto in formato hl7 rifiutato a seguito delle verifiche eseguite:

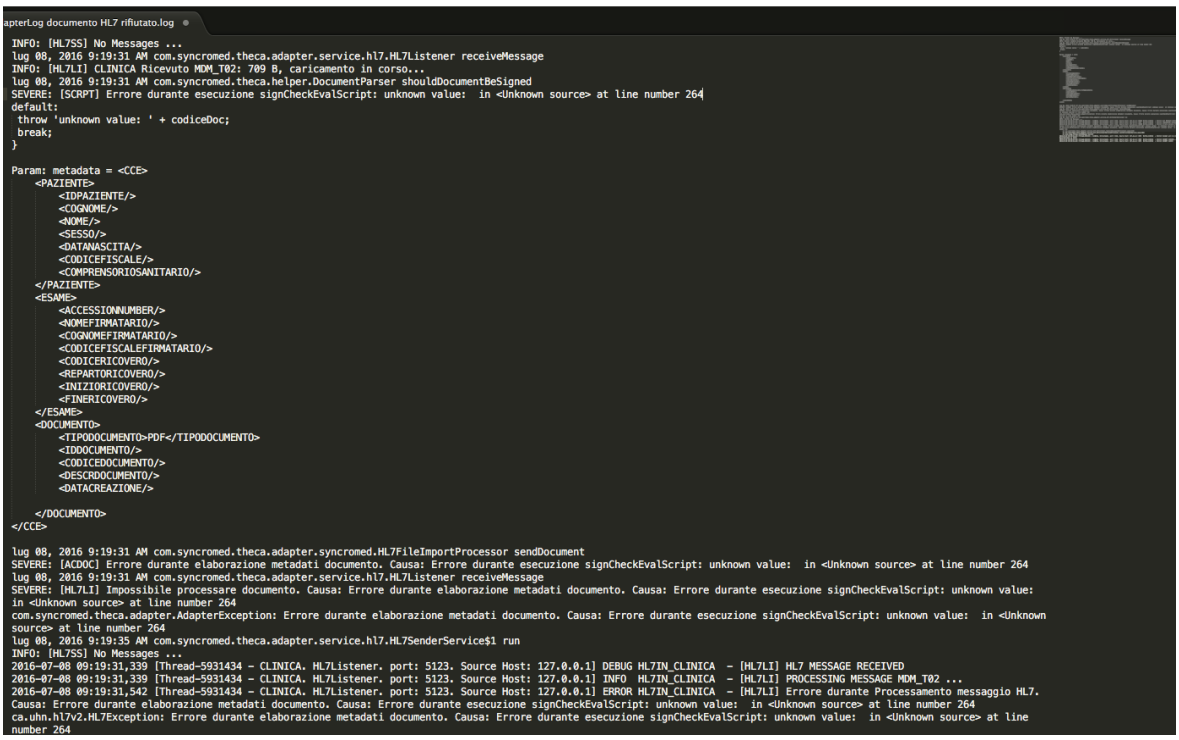

Fig.9 – Esempio di log di rifiuto

- *Versamento manuale*:

  In questo tipo di versamento la soluzione Synapse Theca da immediata evidenza all'utilizzatore del rifiuto del pacchetto, considerato che tutte le validazioni vengono effettuate direttamente in fase di upload (come descritto al punto 7.1).

La comunicazione al sistema sorgente contenente il RdV generato, sarà tracciata all'interno dei log di sistema a loro volta conservati a norma.

Sarà quindi possibile risalire in modo certo all'effettivo momento di inoltro della comunicazione al sistema sorgente.

Torna al sommario

7.5 Preparazione e gestione del pacchetto di archiviazione

Il PdA viene generato a seguito della chiusura del PdV e del relativo RdV.
E' composto dagli oggetti informatici di seguito descritti:

- l'insieme dei documenti contenuti nel PdV non rigettati;
- il RdV stesso;
- IdPA generato secondo lo standard UNI 11386:2010 ("Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali") così come richiamato dall'allegato 4 al D.P.C.M 3/12/13, contiene tutte le impronte (hash 256) dei documenti che compongono il pacchetto di archiviazione.

Attraverso l'applicativo vengono apposte ad ogni indice di conservazione la firma digitale del RdC o del delIl PdA viene generato a seguito della chiusura del PdV e del relativo RdV.
E' composto dagli oggetti informatici di seguito descritti:

- l'insieme dei documenti contenuti nel PdV non rigettati;
- il RdV stesso;

egato ed una marca temporale apposta in modalità automatica dal sistema. L'apposizione della firma e

della marca sull'indice di conservazione così creato completa il processo di conservazione (secondo il D.P.C.M. 3 Dicembre 2013) di tutti i documenti la cui impronta è contenuta nell'indice.

Quando previsto dalla normativa o in presenza di un provvedimento del garante, è possibile prevedere la criptazione dei volumi logici sui quali risiedono i filesystem, dove andranno storati i pacchetti archiviati.

Saranno inoltre disposte delle verifiche periodiche sull'integrità degli archivi, tracciate nei log di sistema ed il loro risultato è evidenziato mediante i "report di verifica". Le eventuali anomalie riscontrate saranno gestite come definito nel paragrafo 9.3.

Torna al sommario

7.6 Preparazione e gestione del pacchetto di distribuzione ai fini dell'esibizione

L'esibizione della documentazione conservata, a fronte di richieste da parte dell'autorità competente, è un altro aspetto gestito dal sistema di conservazione Synapse Theca. Deve essere garantita e conforme a quanto presente dall'art. 10 del DPCM de 3 dicembre 2013. Questa procedura è profilata così come tutte le attività che compongono il flusso di conservazione e quindi richiamabile solo dagli utenti debitamente configurati.

I supporti di memorizzazione sono registrati all'interno del database del sistema di conservazione consentendo una rapida ricerca e selezione del singolo documento, in base alla fornitura degli indici di ricerca previsti per la tipologia documentale in questione (metadati).

Ognuna delle tre fasi dell'esibizione viene eseguita sotto il controllo e la diretta responsabilità del R.d.C ed è gestita da un task dedicato. Le tre fasi che la compongono sono:

- ricerca:
  la ricerca avviene attraverso i metadati a corredo definiti per la tipologia documentale alla quale afferiscono i documenti conservati. I criteri di ricerca corrispondono ai campi dei metadati. Pertanto in base alla tipologia documentale selezionata si visualizzeranno criteri di ricerca diversi. Una volta che l'utente ha inserito i criteri di ricerca può effettuare la "*Ricerca"*. I

documenti che soddisfano i parametri inseriti vengono raggruppati in "Folder" e saranno scaricabili in formato zip. Inoltre, per ciascun documento sarà possibile aprire il log contente tutte le informazioni riguardanti il flusso di conservazione (come descritto 7.2).

- la visualizzazione:

  La visualizzazione avviene attraverso il visualizzatore associato al canale di acquisizione.

- esibizione:

  consiste nella creazione e conseguente distribuzione del pacchetto di distribuzione (definito al punto 6.4) unitamente al verbale di esibizione.

  Le fasi che compongono tale flusso sono:

  - *creazione del pacchetto, fase durante la quale* è possibile visualizzare i documenti
  - *chiusura del pacchetto* con l'apposizione della firma digitale e della marca temporale.
  - *Download* del pacchetto con protocollo https ovvero in formato criptato. Nel caso di richieste particolari da parte del cliente, è possibile eseguire l'operazione di download attraverso vpn e firewall dedicati garantendo un ulteriore livello di sicurezza. E' inoltre possibile, attraverso un'opportuna configurazione, scaricare anche il viewer necessario alla visualizzazione del contenuto del PdD.

E' importante sottolineare che gli eventuali supporti fisici creati, non presenteranno riferimenti esterni che possano permettere l'identificazione dell'ente produttore, dei dati contenuti e della loro tipologia.

Torna al sommario

7.7 Produzione di duplicati e copie informatiche e descrizione dell'eventuale intervento del pubblico ufficiale nei casi previsti

Il RdC o un suo delegato possono produrre duplicato o copie informatiche tramite l'apposito task che può essere utilizzato anche per la creazione dei pacchetti di distribuzione.

Nel caso in cui debba produrre una copia conforme, è sufficiente selezionare tale funzionalità così composta:

- *creazione del PdD*
- *chiusura del PdD*: dove è possibile visualizzare in anteprima i documenti
- *download del PdD*;

  Se si rientra nella casistica per la quale è previsto l'intervento del pubblico ufficiale, la soluzione garantisce tale operazione grazie ad una verifica preventiva del pacchetto e dalla generazione del verbale di esibizione.

Nel caso sia necessario procedere con l'operazione di riversamento dettata da un rinnovo tecnologico (ad esempio passaggio da supporti ottici a NAS) è prevista una funzionalità dedicata. Tale funzionalità prevede:

- l'identificazione del vecchio supporto e la conseguente verifica dello stesso;
- la verifica dei PdA da riversare;
- la copia dei PdA sui nuovi supporti;

L'intera operazione sopra descritta viene tracciata in maniera dettagliata nei log di sistema e visualizzata nel sistema di conservazione attraverso il report evidenziato in fig.10:

VERBALE DI RIVERSAMENTO DIRETTO DEI DOCUMENTI CONSERVATI

Il/La Sottoscritto/a Mario Rossi, Responsabile del procedimento di conservazione sostitutiva della documentazione clinica testuale, iconografica e grafica, nell'ambito della scrivente unità operativa, e su espressa richiesta delle Autorità competenti,

DICHIARA

che si è proceduto, a seguito della verifica periodica dell'integrità degli archivi e della leggibilità degli stessi in conformità alla regole tecniche previste dall'art. 71 del D.Lgs 82/2005 e successive modificazioni, al riversamento dei sottoelencati pacchetti di conservazione:

Data del riversamento	Nome pacchetto di conservazione	Nome media di origine	Nome media di destinazione
08/07/2016 12.00 AM	0000000004	0000000004.1	B00072L5
08/07/2016 12.00 AM	0000000004	0000000004.1	B00073L5

Fig.10 – Esempio di riversamento

Torna al sommario

7.8 Scarto dei pacchetti di archiviazione

Lo scarto dei PdA avviene secondo quanto previsto dalle regole tecniche (Art. 9, comma 1, lettera k) e comunque sempre previa autorizzazione del Cliente opportunamente informato dal Conservatore. Nel caso specifico di archivi pubblici o privati di particolare interesse culturale, tali procedure devono avvenire previa autorizzazione del Ministero dei beni e delle attività culturali e del turismo.

La configurazione, che viene loggata e conseguentemente anch'essa portata in conservazione, dello scarto concordato con il RdC viene effettuata nel task di "configurazione" di ogni singolo canale dove è possibile inserire:

- il tempo di conservazione;
- la modalità di comunicazione al produttore dell'attività di scarto (anche questa comunicazione viene loggata e conseguentemente conservata).
- la tempistica di avviso al RdC dello scarto per ogni singolo PdA

E' presente un report riassuntivo di tutti i pacchetti che hanno terminato il periodo di conservazione, in modo che il produttore possa in qualunque momento averne evidenza.

Torna al sommario

7.9 Predisposizione di misure a garanzia dell'interoperabilità e trasferibilità ad altri conservatori

Synapse Theca implementa gli standard definiti per garantire l'interoperabilità e la trasportabilità del dato tra diversi sistemi di conservazione.

Il PdA e il PdD rispettano lo standard UNI SInCRO 11386:2010 con la scelta per quest'ultimo di gestire i metadati di catalogazione all'esterno dell'indice stesso.

Per poter eseguire una corretta interpretazione di tali dati viene fornito e concordato con il cliente il file xsd dei metadati contenuti nel catalogo esterno.

In caso di cessazione del contratto il cliente può richiedere un'estrazione dei propri dati che verranno forniti secondo gli standard predefiniti. Sarà compito del RdC verificare la completezza delle informazioni fornite.

La soluzione Synapse Theca è anche in grado di caricare pacchetti conservati da altri sistemi grazie ad una procedura dinamica di trasformazione degli indici di conservazione, se documentati, rispetto ai propri standard.

Torna al sommario

8. IL SISTEMA DI CONSERVAZIONE

Di seguito una descrizione dell'architettura del sistema Synapse Theca identificando quelle che sono le sue componenti:

- *logiche*
- *tecnologiche*
- *fisiche*

Torna al sommario

8.1 Componenti Logiche

La soluzione tecnica adottata prevede l'implementazione di tre componenti logiche: Server, Adapter e Client.

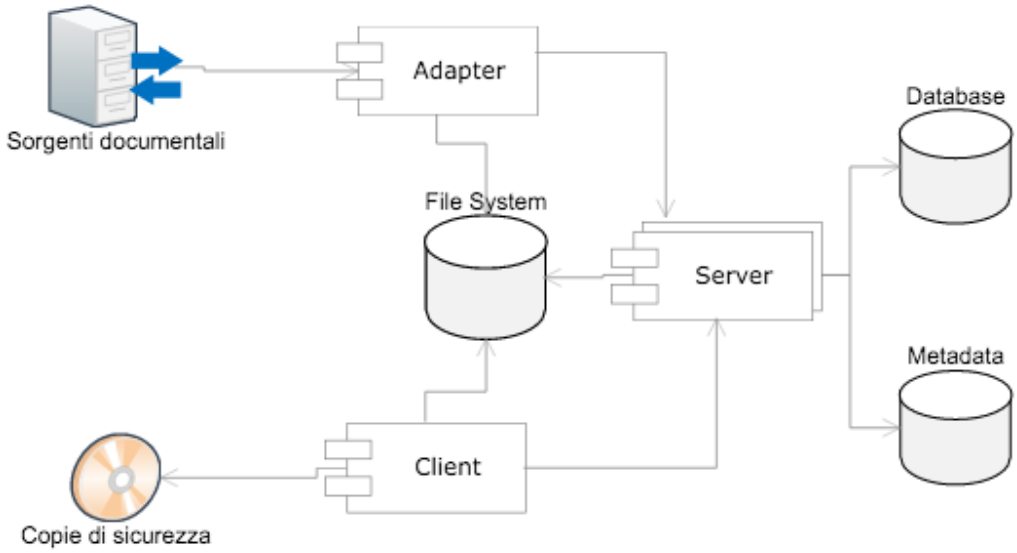

Fig.11 – Componenti logiche

Il componente **Server**:

- coordina le attività di acquisizione,
- gestisce dei pacchetti di conservazione,
- gestisce i processi di verifica,
- offre una interfaccia web per la gestione documentale.

Il componente **Adapter**:

- espone protocolli standard di acquisizione,
- forma i pacchetti di conservazione,
- gestisce la verifica dei documenti,
- gestisce l'integrazione con i device per la produzione delle copie di sicurezza.

Modulo **Client** di front end ha i seguenti compiti:

- offre una interfaccia utente per le attività di gestione di tutto il processo di conservazione

Torna al sommario

8.2 Componenti Tecnologiche

Il sistema di conservazione, come evidenziato nel paragrafo precedente, è basato su componenti logiche che a loro volta sono composte da diversi elementi tecnologici.

La componente *Server* rappresentata di seguito in fig.12, è così composta:

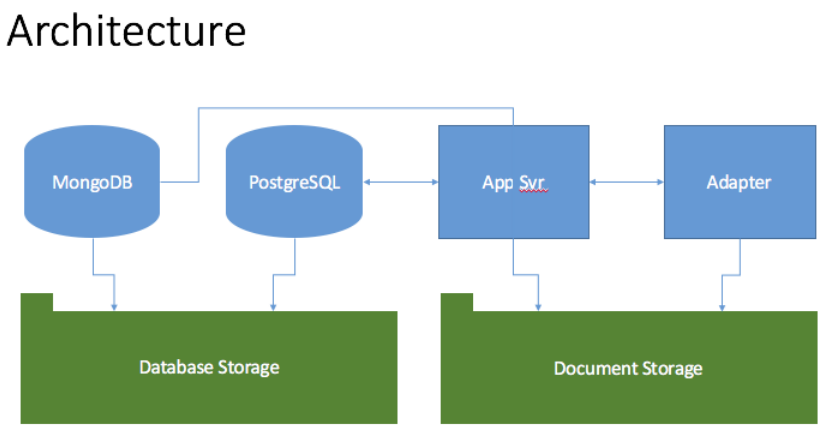

Fig.12 – Componente Server

- due distinti database, uno relazionale dedicato alla gestione del dato e uno dedicato alla gestione e conseguente ottimizzazione dell'indicizzazione.
- Un application server Java EE che racchiude e gestisce tutta la "business logic" della soluzione. E' stato concepito in modo da interagire con il database implementando lo standard JPA così da garantire un livello di astrazione tale da permettere una reale indipendenza dalla scelta del DB stesso.

Il *client* (modulo di front end) è sviluppato con tecnologia $HTML_5$ che ne permette l'utilizzo da qualunque piattaforma, utilizzando il browser senza l'ausilio di plugin esterni.

Gli adapter di integrazione, sviluppati anch'essi secondo standard Java EE e gestiti dal medesimo application server dedicato al cuore della soluzione, implementano i maggiori standard di integrazione (Web Service SOAP, REST, HL7, DICOM, ecc.) e sono stati concepiti con l'intento di avere la massima

flessibilità e dinamicità per eventuali personalizzazioni necessarie nelle varie realtà installate.

Dal punto di vista operativo il sistema Theca sfrutta le metodologie DevOps utilizzando un sistema di Container per rendere più flessibili e quindi garantire la RID (Riservatezza, Integrità, Disponibilità) dei processi di sviluppo – test – qualità – rilascio – produzione degli aggiornamenti.

Torna al sommario

8.3 Componenti Fisiche

La soluzione nasce con è l'obiettivo di essere installabile su infrastrutture concepite con diverse architetture:

- *architettura inHouse*: presso l'infrastruttura del cliente
- *architettura in cloud privato*: situata presso un partner certificato ISO-27001 che garantisca i più elevati standard di Business Continuity e Disaster Recovery.

La soluzione è composta da quattro componenti fondamentali:

- *Application Server*: server fisico o virtuale sul quale viene installato l'application server che gestisce l'intera soluzione;
- *Database Server*: server fisico o virtuale sul quale verrà installato lo strato database dell'applicazione. A seconda della scelta architetturale effettuata ed in funzione del volume di dati da gestire, potrebbe risiedere sullo stesso server descritto del punto precedente;
- *File Server*: spazio disco necessario alla gestione del flusso di acquisizione, legalizzazione, verifica ed esibizione, quindi di tutte le attività eseguite prima della fase di copia di sicurezza o successive se si tratta dell'attività di verifica/riversamento;
- *Device per copie di sicurezza*: In funzione della scelta architetturale effettuata dal cliente, il Sistema è in grado di effettuare le copie di sicurezza su supporti di diversa natura gestendo quindi device eterogenei (LTO, LTO Library, NAS, Blue Ray, DVD). Di seguito un diagramma esemplificativo delle diverse tipologie di device gestiti

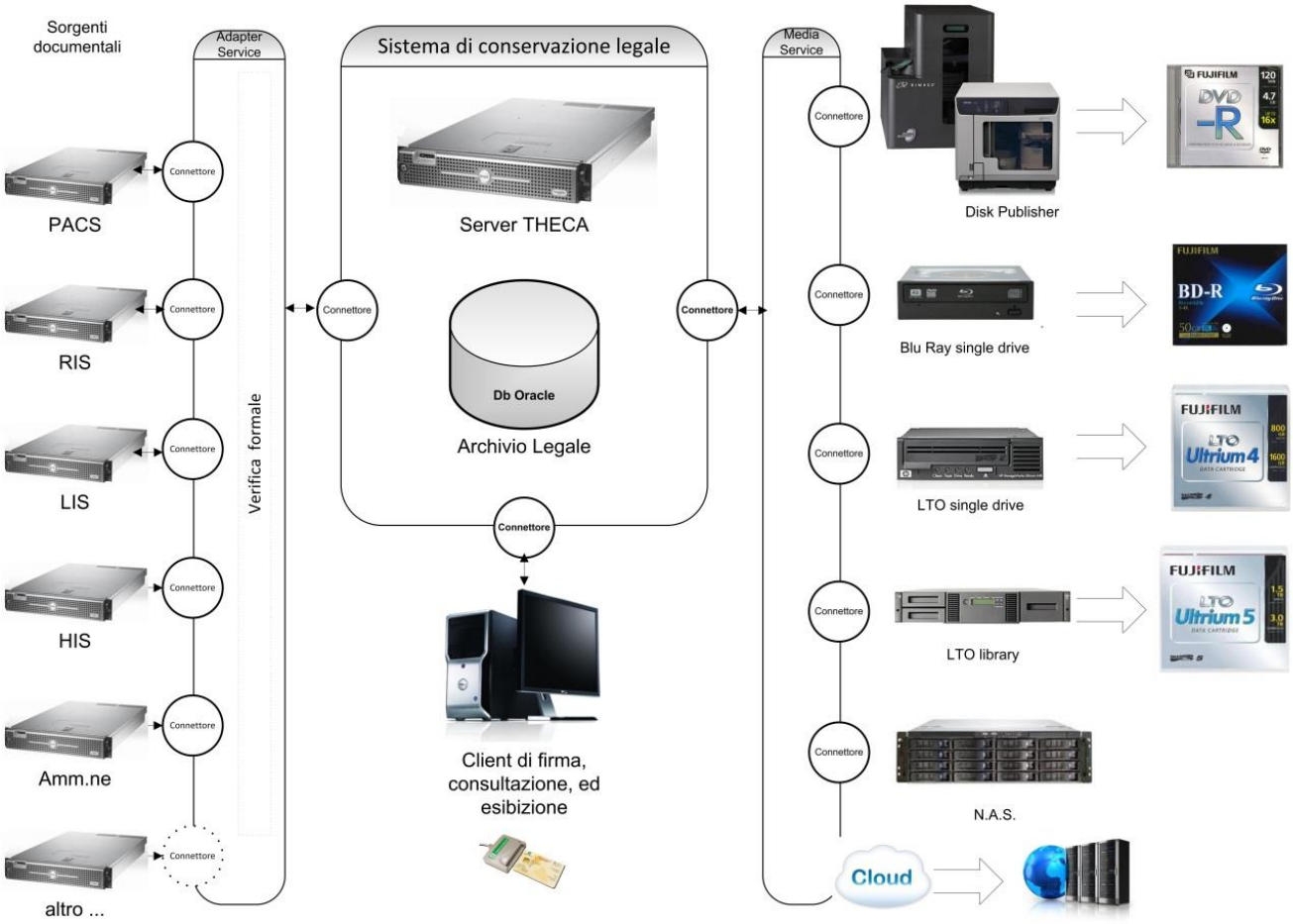

Fig.13 – Componenti Fisiche

Torna al sommario

8.4 Procedure di gestione e di evoluzione

Syncro-Med ha definito e certificato le procedure di gestione della soluzione suddividendo l'attività di supporto da quella di evoluzione in quanto, per la loro diversa natura, necessitano di un approccio differente:

Torna al sommario

8.4.1 Supporto

Per la gestione del supporto è disponibile un sistema di monitoraggio in real time realizzato mediante il prodotto software "Pandora FMS". A fronte di anomalie riscontrate nell'applicativo, grazie alle sonde remote in esso contenute, il personale preposto potrà:

- valutarne la gravità;
- segnalare la problematica aprendo una chiamata sul sistema di Ticketing dedicato.

Una volta presa in carico l'attività di supporto da parte di Syncro-Med, l'attività consisterà nell'analizzare e conseguentemente fissare gli eventuali bug rilevati. Quando il problema non può essere risolto attraverso una configurazione o un adattamento sul campo del software, comportando delle modifiche al codice sorgente, queste saranno gestite secondo il flusso certificato ISO27001, come di seguito schematizzato in fig.14.

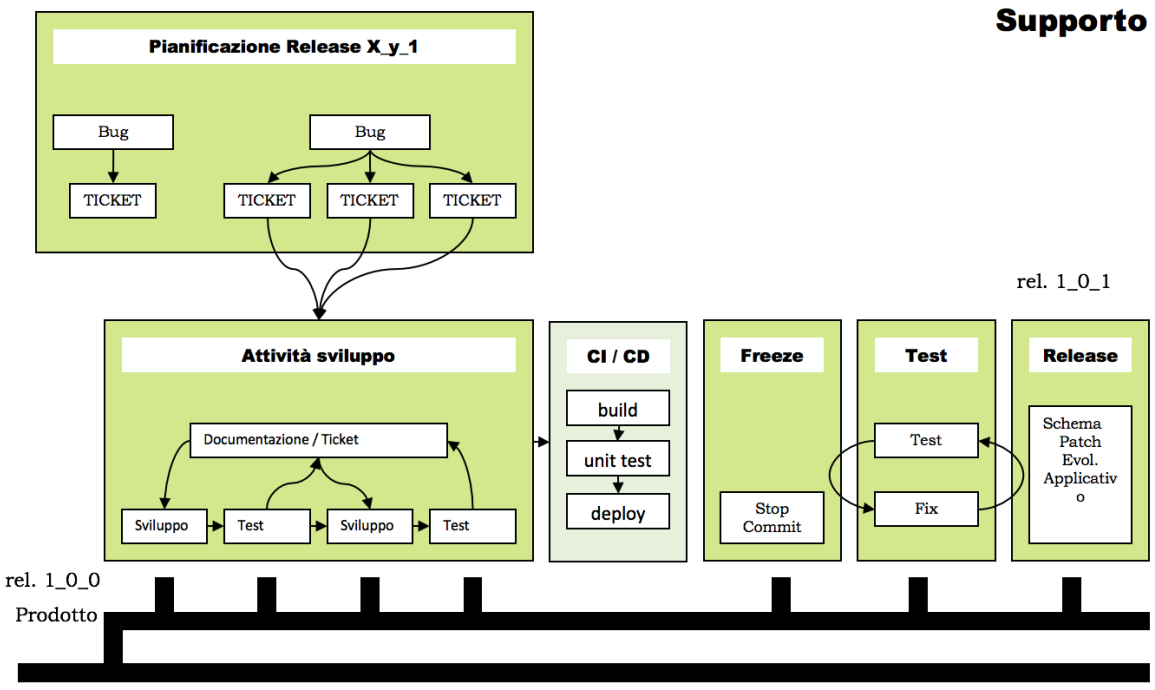

Fig.14 – Flusso di gestione ed evoluzione della soluzione

Una volta rilasciata la versione corretta, sarà compito del personale preposto concordare con il responsabile della conservazione e con il responsabile dei sistemi informativi la messa in produzione.

Torna al sommario

8.4.2 Evoluzione

L'evoluzione dell'applicazione può nascere a fronte di un adeguamento normativo, ad una modifica tecnologica dettata dall'aumento dello standard di sicurezza di uno o più componenti utilizzati (la soluzione è integrata con OWASP per garantire i più alti standard di sicurezza) o da una semplice richiesta di enhacement da parte del cliente stesso.

Verranno analizzati i requisiti, di qualunque natura essi siano, ed in caso di accettazione da parte del quality team, pianificate le attività di sviluppo:

Vi è inoltre un rapporto attivo e continuativo con uno studio legale specializzato in materia di conservazione a norma, con il quale viene effettuato un check periodico delle normative e che si impegna a comunicare tempestivamente eventuali evoluzioni.

Torna al sommario

9. MONITORAGGIO E CONTROLLI

Il processo di monitoraggio copre e registra tutte le fasi del sistema di conservazione, consentendo all'amministratore del sistema di tenere traccia di tutte le operazioni svolte e delle eventuali problematiche riscontrate.

Attraverso uno strumento analitico, intuitivo e di immediata lettura, l'amministratore del sistema è messo nelle condizioni di avere una visione completa dello stato di salute della soluzione attiva, avendo un'evidenza in tempo reale delle eventuali problematiche occorse.

Di seguito, in fig.15, un esempio della tracciabilità degli eventi determinati da ciascun processo.

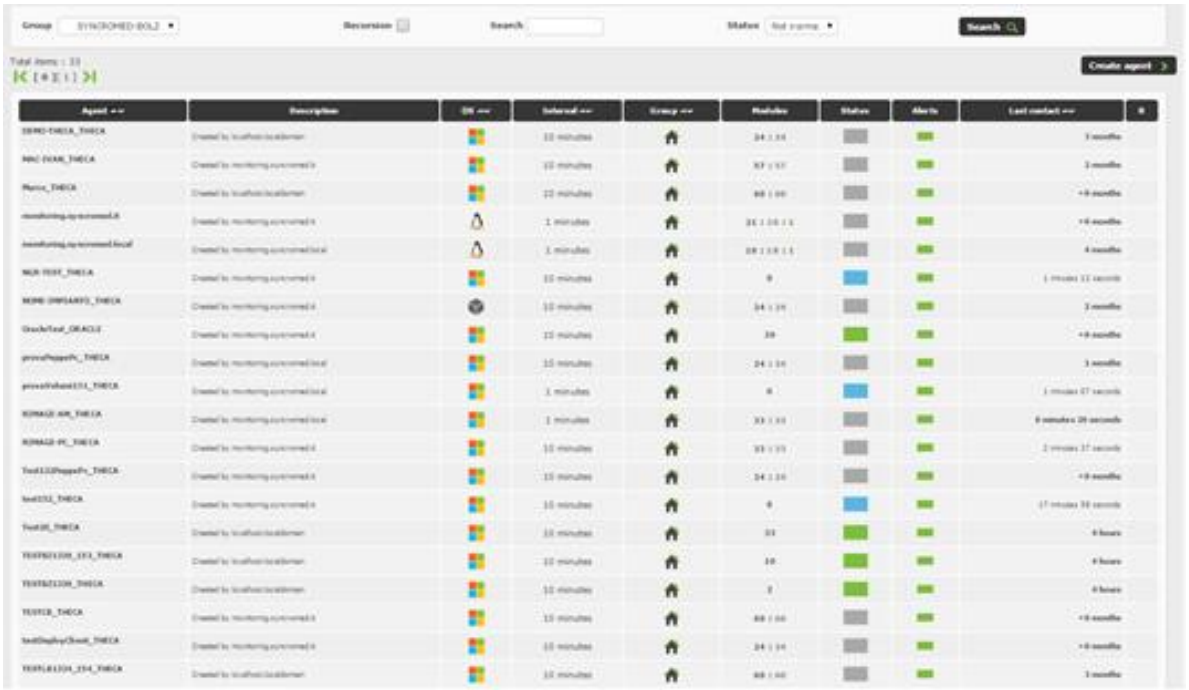

Fig.15 – Esempio di monitor del sistema di conservazione

Torna al sommario

9.1 Procedure di monitoraggio

E' stato scelto un software di monitoraggio flessibile e altamente scalabile. Questo è in grado di monitorare lo stato e le prestazioni del Sistema da una console che ne evidenzia le eventuali problematiche.

Il sistema di monitoraggio interagisce con la soluzione grazie alle sonde remote in essa contenute presenti per ogni fase del flusso di conservazione.

In questo modo è possibile un monitoraggio proattivo che, legato ad una corretta configurazione delle soglie di criticità, mette il personale preposto nelle condizioni di anticipare eventuali problematiche.

Questo strumento permette anche l'implementazione di sonde dedicate all'infrastruttura (ad esempio l'occupazione disco) e alla corretta gestione del database.

E' possibile inoltre configurare "alert" che verranno inviati per email segnalando possibili criticità al personale preposto all'attività di verifica e controllo.

Torna al sommario

9.2 Verifica dell'integrità degli archivi

Il responsabile del processo di conservazione o suo delegato ha l'obbligo di verificare la leggibilità effettiva dei documenti conservati con cadenza periodica non superiore ai cinque anni provvedendo, quando necessario, al riversamento del contenuto dei supporti.

Il modulo di verifica della soluzione Synapse Theca permette all'utente di importare supporti creati per le copie di sicurezza, verificarne la validità del contenuto ed infine se necessario effettuarne il riversamento.

Nello specifico viene verificata la corrispondenza dell'hash (sha-256) presente nell'indice di conservazione con l'hash ricalcolato sul documento prelevato dal media.

L'attività viene riepilogata all'interno di un verbale di verifica prodotto alla chiusura della procedura, differenziando i pacchetti sui quali si ha avuto esito positivo da quelli che hanno riscontrato eventuali problematiche.

Verrà stilato e inserito all'interno del manuale della conservazione da parte del RdC, un calendario delle verifiche periodiche così da avere una pianificazione dell'attività ed un'ulteriore traccia della stessa.

Le operazioni di verifica sono tracciate all'interno dei log di sistema e se ne da evidenza nella soluzione di conservazione, attraverso report dedicati sotto riportati.

- **verifica positiva:**

Il/La Sottoscritto/a Mario Rossi, Responsabile (o suo Delegato) del sistema di conservazione a norma della documentazione informatica

DICHIARA

che si è proceduto, ai sensi dell' art. 44 del D.Lgs 82/2005 e in conformità alla regole tecniche previste dall'art. 71 del D.Lgs 82/2005 e successive modificazioni, alla verifica dei sottoelencati pacchetti di conservazione, attraverso le seguenti operazioni:

- Verifica della leggibilità dei supporti di memorizzazione;
- Verifica della leggibilità dei documenti;
- Verifica dell'integrità delle evidenze informatiche attraverso il controllo del relativo riferimento temporale e della firma digitale;
- Aggiornamento sul sistema di conservazione legale della prossima scadenza di verifica dei pacchetti di conservazione.

Di seguito sono elencati i pacchetti la cui verifica si è conclusa con esito POSITIVO:

Data della verifica	Nome pacchetto di conservazione	Esito
08/07/2016 12.00 AM	REFERTI_5	Valido

LUOGO e DATA — FIRMA DEL DICHIARANTE

Poggio Rusco, 08/07/2016 — Mario Rossi

Fig.16 – Esempio di verifica con Esito Positivo

- **verifica negativa:**

Il/La Sottoscritto/a Mario Rossi, Responsabile (o suo Delegato) del sistema di conservazione a norma della documentazione informatica,

DICHIARA

che si è proceduto, ai sensi dell' art. 44 del D.Lgs 82/2005 e in conformità alle regole tecniche previste dall'art. 71 del D.Lgs 82/2005 e successive modificazioni, alla verifica dei sottoelencati pacchetti di conservazione, attraverso le seguenti operazioni:

- Verifica della leggibilità dei supporti di memorizzazione;
- Verifica della leggibilità dei documenti;
- Verifica dell' integrità delle evidenze informatiche attraverso il controllo del relativo riferimento temporale e della firma digitale;
- Aggiornamento sul sistema di conservazione legale della prossima scadenza di verifica dei pacchetti di conservazione.

Di seguito sono elencati i pacchetti la cui verifica si è conclusa con esito NEGATIVO:

Data della verifica	Nome pacchetto di conservazione	Supporto di memorizzazione	Esito
08/07/2016 12.00 AM	REFERTI_5	REFECD0000005C1	Non valido. Causa: Hash calcolato E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855 diverso da hash archiviato 99B2CB68E1F4C110356C09FE78C2630BB8AA201DE2999BA03B9BFF97DF391DA5 per il documento D:\REFERTI\VOLUMES\REFERTI_5\B9VVAJFW//REFE-885

Fig.17 – Esempio di verifica con Esito Negativo

Torna al sommario

9.3 Soluzioni adottate in caso di anomalie

A fronte delle diverse anomalie riscontrate grazie al sistema di monitoraggio sopra descritto o di segnalazione dell'utilizzatore finale, vengono adottate diverse contromisure a seconda della natura della problematica:

- ***hardware*:**

  a fronte di una problematica hardware, se si tratta di un'installazione in cloud, questa verrà gestita e la continuità operativa sarà garantita dagli elevati standard di business continuity

dell'erogatore del servizio.
Se si tratta di un'architettura inHouse verrà definita, all'interno del piano della sicurezza della singola struttura, la procedura di intervento e conseguente risoluzione del problema.

- ***sistemistica*:**

  anche in questo caso la diversa architettura dell'impianto avrà differenti responsabilità e modalità di intervento. A fronte di problematiche sistemistiche (ad esempio interruzione del corretto funzionamento della rete) saranno predisposti gli interventi da parte del personale interessato secondo le SLA definite in fase contrattuale;

- ***applicativa*:**

  questo tipo di problematiche vengono gestite come descritto nel paragrafo 8.4.1 da parte di Syncro-Med o dai suoi partner.

- ***integrazione*:**

  viene effettuata un analisi della problematica da parte del personale di supporto coinvolgendo, se necessario i riferimenti gestori del sistema interfacciato. Una volta risolta l'anomalia si concorderà il piano d'azione e l'eventuale riallineamento dei documenti non pervenuti.

- ***integrità degli archivi:***

  se a fronte dell'attività di verifica viene riscontrato il problema dell'integrità degli archivi, causata ad esempio da l'illeggibilità di uno dei supporti o un'anomalia del PdA, si procederà con la verifica delle altre copie presenti; a fronte di una problematica estesa a tutte le copie, che impedirebbe il ripristino della situazione corretta, si dovrà procedere con la riacquisizione dei pacchetti di versamento interessati. Tutte queste operazioni sono tracciate nei log di sistema e dovranno essere riportate nel manuale della conservazione.

Torna al sommario