REGIONE DEL VENETO
AZIENDA OSPEDALIERA DI PADOVA

DELIBERAZIONE DEL COMMISSARIO n. 735 del 11/07/2016

OGGETTO: Adozione del manuale di conservazione dei documenti informatici di cui al D.P.C.M. del 03.12.2013 ad oggetto "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 D.Lgs. n. 82 del 2005".

NOTE TRASPARENZA: Con il presente provvedimento di adotta il manuale di conservazione dei documenti informatici di cui al D.P.C.M. del 03.12.2013 ad oggetto "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 D.Lgs. n. 82 del 2005".

Il Direttore della **UOC Affari Generali e Legali** riferisce:

Nell'ambito del processo generale di innovazione della Pubblica Amministrazione all'interno del quale si inserisce il "Sistema di gestione informatica dei documenti", con deliberazione n. 1505 del 30.10.2015, è stato approvato l'adeguamento, ai sensi del D.P.C.M. del 03.12.2013 ad oggetto "Regole Tecniche per il protocollo informatico ai sensi degli articoli 40-bis, 41, 47, 57-bis e 71, del Codice dell'Amministrazione Digitale di cui al D.Lgs. n. 82 del 2005", del Manuale per la gestione del protocollo informatico dell'Azienda Ospedaliera di Padova.
Con il medesimo provvedimento è stato, inoltre, individuato nel Direttore dell'UOC Affari Generali e Legali, il Responsabile della conservazione di cui all'art. 7 del D.P.C.M. del 03.12.2013 ad oggetto "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 D.Lgs. n. 82 del 2005".
L'art. 7, comma 1, lett. m) del D.P.C.M. del 03.12.2013 "Regole tecniche in materia di conservazione", prevede che il Responsabile della conservazione predisponga il Manuale della conservazione, il quale, secondo quanto stabilito dall'art. 8, comma 1, del medesimo D.P.C.M. *"illustra dettagliatamente l'organizzazione, i soggetti coinvolti ed i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate ed ogni altra informazione utile alla gestione ed alla verifica del funzionamento, nel tempo, del sistema*

di conservazione", curandone l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.
Il Manuale di conservazione risulta, quindi, funzionalmente collegato al Manuale di gestione documentale nell'ottica di realizzare un processo finalizzato all'adozione di idonee procedure che garantiscano la corretta conservazione nel tempo dei documenti aziendali dematerializzati e/o digitali, in modo da assicurarne l'integrità, la reperibilità e la conformità agli originali, con specifico riferimento sia alla documentazione sanitaria sia a quella amministrativa.
Le Pubbliche Amministrazioni, secondo quanto stabilito dall'art. 5 dal predetto D.P.C.M., possono attuare i processi di conservazione o all'interno della propria struttura organizzativa o affidandoli, in modo totale o parziale, ad altri soggetti pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale. Inoltre, ai sensi dell'art. 6, commi 6 e 7, del D.P.C.M. in argomento *"il Responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento del processo di conservazione o di parte di esso ad uno o più soggetti di specifica competenza ed esperienza in relazione alle attività ad essi delegate. Tale delega è formalizzata, esplicitando chiaramente il contenuto della stessa ed in particolare le specifiche funzioni e competenze affidate al delegato che, per competenza ed esperienza, garantiscano la corretta esecuzione delle operazioni delegate [...] e che preveda l'obbligo del rispetto del Manuale di conservazione predisposto dal Responsabile della stessa".*

Considerato che con deliberazione n. 1024 del 17.07.2015 è stata aggiudicata, mediante piattaforma MEPA, alla InfoCert S.p.A. di Roma, la fornitura del servizio di manutenzione per la conservazione sostitutiva ed esibizione a norma di documenti digitali (L-Care), per il periodo di 36 mesi, con decorrenza dal 01.09.2015, stipulando il relativo contratto nella forma commerciale mediante scambio di corrispondenza, secondo la normativa vigente, si propone di procedere all'adozione del Manuale di conservazione dei documenti informatici nel testo allegato e di delegare, contestualmente, ad InfoCert S.p.A. il processo di conservazione dei documenti informatici mediante sottoscrizione di apposito atto di affidamento che forma parte integrante e sostanziale della presente deliberazione.

IL COMMISSARIO

PRESO ATTO della suestesa proposta e accertato che il Direttore della **UOC Affari Generali e Legali** ha attestato l'avvenuta regolare istruttoria della pratica, anche in ordine alla conformità con la vigente legislazione statale e regionale, nonché la copertura della spesa prevista nel budget

assegnato per l'anno in corso;
RITENUTO di dover adottare in merito i provvedimenti necessari;
VISTO il Decreto Legislativo n. 502/92 e successive modifiche ed integrazioni e le leggi regionali n. 55 e n. 56 del 1994 e successive modifiche ed integrazioni;
ACQUISITO il parere favorevole del Direttore Amministrativo e del Direttore Sanitario per quanto di rispettiva competenza;
IN BASE ai poteri conferitigli dal D.P.G.R.nr.197 del 30.12.2015.

DELIBERA

1. di approvare, per le motivazioni esposte in premessa, il Manuale di conservazione dei documenti informatici ai sensi del D.P.C.M. del 03.12.2013 ad oggetto "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 D.Lgs. n. 82 del 2005", nel testo allegato che forma parte integrante e sostanziale della presente deliberazione;

2. di autorizzare il Responsabile della conservazione a delegare alla InfoCert S.p.A. di Roma, a cui con deliberazione n. 1024 del 17.07.2015, è stata aggiudicata, mediante piattaforma MEPA, la fornitura del servizio di manutenzione per la conservazione sostitutiva ed esibizione a norma di documenti digitali (L-Care), per il periodo di 36 mesi, con decorrenza dal 01.09.2015, il processo di conservazione dei documenti informatici mediante sottoscrizione di apposito atto di affidamento che forma parte integrante e sostanziale della presente deliberazione;

3. di prendere atto che sono conservati agli atti dell'UOC Affari Generali e Legali le Condizioni Generali del Contratto, l'Allegato Tecnico ed il Manuale Utente LegalDoc;

4. di dare mandato all'UOC Informatica di provvedere, per quanto di propria competenza, agli aggiornamenti relativi alle procedure informatiche;

5. di dare atto che il presente Manuale potrà essere oggetto di aggiornamento e/o revisione qualora lo rendessero necessario il mutato quadro normativo o l'acquisizione di nuove tecnologie;

6. di delegare il Responsabile della conservazione all'adozione dei provvedimenti necessari per l'integrazione e la modifica del Manuale di conservazione dei documenti informatici;

7. di delegare il Direttore dell'UOC Affari Generali e Legali alla firma di tutti gli atti inerenti e conseguenti all'esecuzione della presente deliberazione;

8. di pubblicare il Manuale di conservazione dei documenti informatici nell'area "Amministrazione Trasparente" del sito Web aziendale.

Il Commissario
Dott. Luciano Flor

Manuale dei processi di formazione e conservazione dei documenti elettronici dell'Azienda Ospedaliera di Padova

INDICE

Versione/Release n° *:*	1	***Data Versione/Release*** *:*	maggio 2016
Descrizione modifiche:	nessuna		
Motivazioni:	prima emissione		

1 Introduzione al documento

1.1 Scopo e campo di applicazione del documento

Il presente documento è il Manuale dei processi di formazione e conservazione elettronica dei documenti (di seguito anche "Manuale della Conservazione") redatto dall'Azienda Ospedaliera di Padova.

Il Manuale ha lo scopo di raccogliere le diverse normative in materia e di documentare il processo di conservazione dei documenti elettronici.

Nel dettaglio il Manuale illustra l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Inoltre, descrive tutte le procedure e le prassi seguite dall'Azienda Ospedaliera di Padova (di seguito denominata AO) e dai partner tecnologici GPI, CBT, Noemalife in materia di gestione della sicurezza del servizio, dei documenti e delle informazioni trattate: questa parte costituisce il regolamento operativo di tutti i processi di digitalizzazione dei documenti di conservazione digitale.

In caso di ispezione da parte delle Autorità di Vigilanza o di altri organismi a ciò deputati, il Manuale permette un agevole svolgimento di tutte le attività di controllo e costituisce una importante dimostrazione dell'impegno dell'Ente al rispetto delle norme.

Il documento si applica al servizio LegalDoc fornito in modalità ASP (Application Service Providing) da InfoCert SpA secondo uno schema di Business Process Outsourcing (BPO).

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 1-3) contiene una panoramica di tutte le leggi e i decreti che regolano la materia, fornisce il profilo dell' AO, il profilo di InfoCert e dettaglia la configurazione dei sistemi utilizzati per l'erogazione;
2. la seconda sezione (capitoli 4-9) descrive il servizio LegalDoc, i compiti del responsabile della conservazione, illustra i macro flussi operativi definiti per la gestione della documentazione elettronica. Inoltre, è dettagliato il procedimento di conservazione posto sotto la responsabilità di InfoCert in virtù della delega allo svolgimento delle attività di competenza del Responsabile della Conservazione, sottolineando input, output e responsabilità di ogni fase. Infine, vengono descritti i controlli effettuati e i processi ricerca e esibizione a norma dei documenti conservati.
3. la terza sezione (capitoli 10-12) riporta le misure fisiche e logiche di sicurezza adottate, cenni sui riversamenti, i riferimenti alla normativa e alla policy sulla protezione dei dati personali e gli allegati al Manuale.

1.2 Principi di redazione

La redazione del Manuale della Conservazione dell' AO è ispirata ai seguenti principi:

- **Principio di trasparenza**, il Manuale mira a fornire una chiara spiegazione del sistema di conservazione documentale e dei processi erogati.
- **Ottica di processo**, il documento mira a descrivere le fasi del processo, non il dettaglio tecnico degli strumenti utilizzati, ad uso interno e a fini ispettivi.
- **Principio di rilevanza**: nel Manuale sono contenute solamente le informazioni rilevanti, con un livello di dettaglio mirante ad agevolare le ispezioni, senza dettagli tecnici superflui.

- **Principio di accuratezza**: le informazioni sono state revisionate da più persone, poste ai diversi livelli della catena decisionale.

1.3 Termini e definizioni

ACCESSO	Operazione che consente a chi ne ha diritto di prendere visione ed estrarre copia dei documenti informatici.
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.
AFFIDABILITA'	Caratteristica che esprime il livello di fiducia che l'utente ripone nel documento informatico.
AGGREGAZIONE DOCUMENTALE INFORMATICA	Aggregazione di documenti informatici o di fascicoli informatici, riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
ARCHIVIAZIONE	Processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo. È passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
AGID	Agenzia per l'Italia Digitale
ARCHIVIO	Complesso organico di documenti, di fascicoli e di aggregazioni documentali di qualunque natura e formato, prodotti o comunque acquisiti da un Soggetto Produttore durante lo svolgimento dell'attività.
ARCHIVIO INFORMATICO	Archivio costituito da documenti informatici, fascicoli informatici nonché aggregazioni documentali informatiche gestiti e conservati in ambiente informatico.
AREA ORGANIZATIVA OMOGENEA	Insieme di funzioni e di strutture, individuate dall' amministrazione, che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell'articolo 50, comma 4, del D.P.R. 28 dicembre 2000, n. 445.
ASP	Application Service Provider.
ATTESTAZIONE DI CONFORMITA' DELLE COPIE PER IMMAGINE SU SUPPORTO INFORMATICO DI UN DOCUMENTO ANALOGICO	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
AUTENTICITA'	Caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche. L'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico.
BASE DATI	Collezione di dati registrati e correlati tra loro.
CA	Certification Authority
CAD	Codice Amministrazione Digitale D.lgs. 82 del 7 marzo 2005 e successive modifiche.

CAS	Content Addressed Storage.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività 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.
CICLO DI GESTIONE	Arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo.
CLASSIFICAZIONE	Attività di organizzazione logica di tutti i documenti secondo uno schema articolato in voci individuate attraverso specifici titoli e classi.
CODICE (DELL'AMMINISTRAZIONE DIGITALE)	Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
CODICE ESEGUIBILE	Insieme di istruzioni o comandi software direttamente elaborabili dai sistemi informatici.
CONSERVATORE ACCREDITATO	Soggetto, pubblico o privato, che svolge attività 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, dall'Agenzia per l'Italia Digitale.
CONSERVAZIONE	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato, descritto nel presente manuale di conservazione e che risponde a quanto stabilito nel DPCM del 03 dicembre 2013.
COPIA ANALOGICA DI UN DOCUMENTO INFORMATICO	Documento analogico avente contenuto identico a quello del documento informatico da cui è tratto.
COPIA DI SICUREZZA	Copia di backup degli archivi del sistema di conservazione prodotta ai sensi dell'articolo 12 del DPCM del 3 dicembre 2013.
DATI SENSIBILI	Ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003, n.196 e la seguente deliberazione del Consiglio dei Ministri del 25 maggio 2012, i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
D. LGS	Decreto Legislativo
DPCM	Decreto della Presidenza del Consiglio dei Ministri
DPR	Decreto del Presidente della Repubblica
DOCUMENTO ANALOGICO	Rappresentazione analogica di atti, fatti o dati giuridicamente rilevanti.
DOCUMENTO INFORMATICO	Rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
ESIBIZIONE	Operazione che consente di visualizzare un documento conservato e di ottenerne copia.
EVIDENZA INFORMATICA	Sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica.

EXTENSIBLE MARKUP LANGUAGE	Linguaggio derivato dall'SGML (Standard Generalized Markup Language), metalinguaggio che permette di creare altri linguaggi. L'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati. Tali strutture vengono definite utilizzando dei marcatori (markup tags).
FASCICOLO INFORMATICO	Aggregazione strutturata e univocamente identificata di atti, documenti o dati informatici, prodotti e funzionali all'esercizio di una specifica attività o di uno specifico procedimento. Nella pubblica amministrazione il fascicolo informatico collegato al procedimento amministrativo è creato e gestito secondo le disposizioni stabilite dall'articolo 41 del Codice.
FIRMA DIGITALE	Un particolare tipo di firma elettronica avanzata 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 (art. 1 comma 1 lettera s) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA	L'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di identificazione informatica (art. 1 comma 1 lettera q) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA QUALIFICATA	Un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma (art. 1 comma 1 lettera r) Decreto Legislativo del 7 marzo 2005 n. 82).
FIRMA ELETTRONICA AVANZATA	Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati (art. 1 comma 1 lettera q-bis) Decreto Legislativo del 7 marzo 2005 n. 82). Si vedano anche le regole tecniche, pubblicate nella G.U. il 21 maggio 2013.
FORMATO	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
GU	Gazzetta Ufficiale della Repubblica Italiana.
HSM	Hardware Security Module.
IDENTIFICATIVO UNIVOCO (di seguito detto Token)	Sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione. Detto anche token LegalDoc.
IMMODIFICABILITA'	Caratteristica che rende il contenuto del documento informatico non alterabile nella forma e nel contenuto durante l'intero ciclo di gestione e ne garantisce la staticità nella conservazione del documento stesso.

IMPRONTA DI UNA SEQUENZA DI SIMBOLI BINARI (o HASH)	Una funzione matematica che genera, a partire da una evidenza informatica, una impronta in modo tale che risulti di fatto impossibile, a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
I.N.RI.M.	Istituto Nazionale di Ricerca Metrologica
INSIEME MINIMO DI METADATI DEL DOCUMENTO INFORMATICO	Complesso dei metadati, la cui struttura è descritta nell'allegato 5 del DPCM del 3 dicembre 2013, da associare al documento informatico per identificarne provenienza e natura e per garantirne la tenuta.
INTEGRITA'	Insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato.
INTEROPERABILITA'	Capacità di un sistema informatico di interagire con altri sistemi informatici analoghi sulla base di requisiti minimi condivisi.
LEGALDOC	Servizio di conservazione digitale a norma di InfoCert.
LEGGIBILITA'	Insieme delle caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti.
MARCA TEMPORALE	Il riferimento temporale che consente la validazione temporale e che dimostra l'esistenza di un'evidenza informatica in un tempo certo (art. 1, lettera m del DPCM 22 febbraio 2013). La marca temporale emessa in conformità con quanto previsto dal DPCM 22 febbraio 2013, titolo IV è opponibile ai terzi ai sensi dell'art. 41 dello stesso decreto.
MEF	Ministero dell'Economia e delle Finanze
METADATI	Insieme di dati associati a un documento informatico, o a un fascicolo informatico, o ad un'aggregazione documentale informatica per identificarlo e descriverne il contesto, il contenuto e la struttura, nonché per permetterne la gestione nel tempo nel sistema di conservazione; tale insieme è descritto nell'allegato 5 del DPCM del 3 dicembre 2013.
NTP	Network Time Protocol
OAIS	Open Archival Information System: è lo standard ISO 14721:2003 e definisce concetti, modelli e funzionalità inerenti agli archivi digitali e gli aspetti di digitalpreservation.
PACCHETTO INFORMATIVO	Contenitore che racchiude uno o più oggetti da conservare (documenti informatici, fascicoli informatici, aggregazioni documentali informatiche), oppure anche i soli metadati riferiti agli oggetti da conservare.
PORTABLE DOCUMENT FORMAT	Formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. Il PDF è un formato a schema fisso basato su un linguaggio di descrizione di pagina che permette di rappresentare documenti in modo indipendente dall'hardware, dal software e dal sistema operativo; ogni PDF incapsula una descrizione completa del documento, che include testo, caratteri, immagini e grafica. PDF è uno standard aperto; recentemente la versione PDF/A (PDF Reference Version 1.4) è stata riconosciuta dall'International Organization for Standardization (ISO) con la norma ISO 19005:2005.

POSTA ELETTRONICA CERTIFICATA	Sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
PRESA IN CARICO	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione.
PRODUTTORE/ SOGGETTO PRODUTTORE/CLIENTE	Persona fisica o giuridica, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione.
PA	Pubblica Amministrazione.
PEC	Posta Elettronica Certificata.
PU	Pubblico Ufficiale.
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; in LegalDoc è l'insieme degli Indici del Pacchetto di Archiviazione associati ad ogni documento inviato in conservazione in un'unica sessione, che fanno parte del pacchetto di versamento.
REST	Representational State Transfer.
RESPONSABILE DELLA CONSERVAZIONE	Soggetto responsabile dell'insieme delle attività elencate nell'articolo 8, comma 1 del DPCM del 3 dicembre 2013.
RESPONSABILE DEL SERVIZIO DI CONSERVAZIONE	Risorsa di InfoCert, che, su delega del Responsabile della Conservazione, gestisce le politiche generali del sistema di conservazione, nel rispetto del modello organizzativo esplicitato nel presente Manuale e di quanto previsto nelle Specificità del Contratto.
RESPONSABILE DELLA GESTIONE DOCUMENTALE O RESPONSABILE DEL SERVIZIO PER LA TENUTA DEL PROTOCOLLO INFORMATICO, DELLA GESTIONE DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI	Dirigente o funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica, preposto al servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445, che produce il pacchetto di versamento ed effettua il trasferimento del suo contenuto nel sistema di conservazione.
RESPONSABILE DELLA SICUREZZA INFORMATICA	Soggetto al quale compete la definizione delle soluzioni tecniche ed organizzative in attuazione delle disposizioni in materia di sicurezza.
RESPONSABILE DEL TRATTAMENTO DEI DATI	Persona fisica o giuridica o pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.
RIFERIMENTO TEMPORALE	Evidenza informatica, contenente la data e l'ora, che viene associata ad uno o più documenti informatici (art. 1, lettera m del DPCM 22 febbraio 2013).
SaaS	Software as a Service.
SCARTO	Operazione con cui si eliminano, secondo quanto previsto dalla normativa vigente, i documenti ritenuti privi di valore amministrativo e/o di interesse storico culturale.

SISTEMA DI CLASSIFICAZIONE	Strumento che permette di organizzare tutti i documenti secondo un ordinamento logico con riferimento alle funzioni e alle attività dell'amministrazione interessata.
SISTEMA DI GESTIONE INFORMATICA DEI DOCUMENTI	Nell'ambito della Pubblica Amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445; per i privati è il sistema che consente la tenuta di un documento informatico.
STATICITA'	Caratteristica che garantisce l'assenza di tutti gli elementi dinamici, quali macroistruzioni, riferimenti esterni o codici eseguibili, e l'assenza delle informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione.
TSA	Time Stamping Authority.
TSS	Time Stamping Service.
TU	Testo Unico.
URL	Universal Resource Locator.
UTC	Universal Coordinated Time – Tempo Universale Coordinato.
UTENTE	Persona fisica, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
VERSAMENTO AGLI ARCHIVI DI STATO	Operazione con cui il responsabile della conservazione di un organo giudiziario o amministrativo dello Stato effettua l'invio agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.
WORM	Write Once Read Many

1.4 Acronimi

CA	Certification Authority
CNIPA	Centro Nazionale per l'Informatica nella Pubblica Amministrazione (exDigitPA) ora Agenzia per l'Italia Digitale
D. LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
GU	Gazzetta Ufficiale della Repubblica Italiana
HSM	Hardware Security Module
PDF	PortableDocument Format
PEC	Posta Elettronica Certificata
SG	Sistema di Gestione
SGD	Sistema di Gestione Documentale
SSL	SecureSocketLayer
TSA	Time Stamping Authority
TSS	Time Stamping Service

TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language

2 Nomine e individuazione dei compiti

In questo capitolo sono individuati i differenti soggetti che intervengono a vario titolo nelle diverse fasi del processo di creazione dei documenti elettronici, digitalizzazione dei documenti cartacei e conservazione elettronica documentale.

2.1 AO – Azienda Ospedaliera

Ente	Azienda Ospedaliera di Padova
Sede Amministrativa	Via Nicolò Giustiniani, 1 – 35128 PADOVA
Recapiti	P.E.C.: azosp.padova@legalmail.it
Sito web	www.sanita.padova.it
Partita IVA	c.f./p.iva 00349040287
Codice Fiscale	c.f./p.iva 00349040287

2.2 Referenti di processo

Nominativo dei soggetti dell'AO incaricati della gestione del sistema di creazione dei documenti e di invio dei documenti in conservazione.

Nome e Cognome	Responsabile interno della Conservazione – Dott.ssa Caterina Dalla Zuanna
Ente/Società	Azienda Ospedaliera di Padova
Data inizio incarico	DDG 1505 del 30/10/2015

Nome e Cognome	Responsabile del processo di compilazione della documentazione sanitaria prodotta in regime ambulatoriale – UOC Informatica
Ente/Società	Azienda Ospedaliera di Padova

Nome e Cognome	Responsabile del processo di compilazione della documentazione sanitaria prodotta in regime di ricovero – UOC Informatica
Ente/Società	Azienda Ospedaliera di Padova

2.3 Responsabile della conservazione

L'Azienda, Soggetto Produttore, avvalendosi della facoltà prevista dall'art. 5, comma 1, b) del DPCM del 3 dicembre 2013 e dalla precedente deliberazione CNIPA 11/2004, ha affidato lo svolgimento delle attività del Responsabile della Conservazione ad un soggetto terzo che, per competenza ed esperienza, garantisce lo svolgimento delle suddette attività (si veda in proposito l'allegato n° [2] Affidamento del procedimento di conservazione sostitutiva).

Le attività sono state affidate ad InfoCert SpA, gestore del servizio di conservazione sostitutiva in outsourcing LegalDoc.

InfoCert assume l'incarico di svolgere le attività delegate dal Responsabile della Conservazione in accordo con quanto previsto dal contratto, dagli allegati contrattuali.

InfoCert SpA provvede ad affidare lo svolgimento delle attività delegate dal Responsabile della Conservazione ad una o più persone che, per competenza ed esperienza, garantiscano la corretta esecuzione dei processi di conservazione definiti dalle norme, dal contratto e dagli allegati contrattuali.

L'atto di affidamento allo svolgimento delle attività del Responsabile della Conservazione viene conferito dal Soggetto Produttore ad InfoCert contestualmente alla sottoscrizione del contratto di adesione al servizio LegalDoc.

2.4 InfoCert SPA

Denominazione sociale	InfoCert SpA
Sede Legale:	Piazza Sallustio, 9, 00187 Roma Tel.+39 06 836691 Fax +39 06 44285255
Sedi Operative:	Via Franco Russoli 5, 20143 Milano Tel: +39 02 872.867.00
	Corso Stati Uniti 14bis, 35127 Padova Tel. +39 04982881 Fax +39 049 0978406
	Via Marco e Marcelliano 45, 00147 Roma Tel. +39 06 836691 Fax +39 06 44285255
Sito web	www.infocert.it
e-mail	info@infocert.it
PEC	infocert@legalmail.it
Codice Fiscale / Partita IVA	07945211006
Numero REA	RM - 1064345

InfoCert S.p.A. si pone sul mercato come un Partner altamente specializzato nei servizi di Certificazione Digitale e Gestione dei documenti in modalità elettronica, in grado di garantire ai propri clienti la piena innovazione

nei processi di gestione del patrimonio documentale. InfoCert S.p.A., con un capitale sociale di oltre 17 M€ ed un fatturato 2013 di oltre 32 M€, è il Primo Ente Certificatore per la Firma Digitale in Italia, leader di mercato per i processi di Conservazione dei documenti a norma di legge e per i servizi di Posta Elettronica Certificata.

InfoCert progetta e sviluppa soluzioni informatiche ad alto valore tecnologico di dematerializzazione dei processi documentali, attraverso componenti di Gestione Documentale, Conservazione, Firma Digitale e Posta Elettronica Certificata. I clienti vengono accompagnati nella scelta di servizi e soluzioni pienamente rispondenti alle esigenze organizzative, ai vincoli normativi generali e specifici di settore.

InfoCert, inoltre, nello svolgimento delle proprie attività, si è dotata delle seguenti certificazioni:

- ISO 14001:2013 (Sistema di Gestione Ambientale)
- UNI EN ISO 20000-1:2011 (Gestione dei Servizi Informatici)
- UNI EN ISO 9001:2008 (Sistemi di gestione per la qualità);
- UNI EN ISO 27001:2006 (Sistemi di gestione della sicurezza delle informazioni);

2.4.1 Identificazione nel sistema

Il Responsabile della Conservazione InfoCert viene identificato nel sistema LegalDoc grazie alla definizione di un particolare utente con il ruolo di "responsabile del procedimento di conservazione".

Gli estremi identificativi di questo utente (organizzazione di appartenenza, cognome, nome, codice fiscale) sono, inoltre, riportati anche nelle informazioni associate ai documenti conservati (nelle informazioni relative ad ogni documento e nel file di chiusura lotto).

2.4.2 Supporto offerto dal sistema

LegalDoc supporta il Responsabile della Conservazione InfoCert nel controllo dell'effettiva leggibilità dei documenti conservati e mantiene la tracciatura delle esibizioni effettuate, considerate una ulteriore prova di leggibilità.

Il sistema gestisce in maniera automatica i parametri di organizzazione del contenuto dei supporti di memorizzazione e le procedure di sicurezza e di tracciabilità, fondamentali per la corretta conservazione del documento conservato.

Il sistema supporta il Responsabile della Conservazione nell'archiviazione delle informazioni relative a ogni supporto di memorizzazione utilizzato attraverso specifiche funzionalità, sulle quali egli esercita l'attività di controllo e di supervisione.

LegalDoc, inoltre, fornisce al Responsabile della Conservazione InfoCert un set di funzionalità per il mantenimento dell'archivio delle diverse versioni del software in gestione e il monitoraggio sia del flusso di documenti elaborati dal sistema, sia dei serventi specializzati. Il sistema, infatti, segnala ogni anomalia riscontrata, consentendo un pronto intervento e assicurando un monitoraggio costante.

3 Fondamenti normativi

3.1 Il quadro normativo

Il contesto normativo in cui si inquadra la conservazione sostitutiva risale al 1994, ma è solo a partire dall'anno 2004 che interventi più significativi hanno reso possibile la conservazione dei documenti in formato digitale valevole anche ai fini fiscali. Per agevolarne la comprensione, di seguito si fornisce una panoramica del quadro normativo di riferimento.

La legge numero 537 del 24 dicembre 1993 "Interventi correttivi di finanza pubblica" (GU n. 303 del 28 dicembre 1993) affronta per la prima volta il tema di una modalità alternativa di conservare (e conseguentemente esibire) dei documenti a fini amministrativi. La norma introduce nell'ordinamento la possibilità di conservare scritture e documenti contabili "sotto forma di registrazioni su supporti di immagini" ed estende questa possibilità anche a tutte le scritture e i documenti rilevanti ai fini delle disposizioni tributarie.

Le relative modalità operative, tuttavia, sono rimandate ad un decreto del Ministero delle Finanze, emanato solamente dieci anni più tardi (23 gennaio del 2004) permettendo l'avvio concreto del processo.

Nel frattempo, è stato completato il quadro normativo relativo al documento informatico, alla firma digitale e alla fattura elettronica (a titolo non esaustivo si citano il Testo Unico sulla documentazione amministrativa – TU 445/2000, il Decreto del Presidente del Consiglio dei Ministri 8/02/1999 ora sostituito dal Decreto del Presidente del Consiglio dei Ministri del 13/01/2004, le numerose deliberazioni AIPA – poi divenuta CNIPA, ora DigitPA –, il Decreto Ministero Economia e Finanze 23 gennaio 2004 e il Decreto Legislativo 52 del 20 febbraio 2004, relativi a specifiche tipologie di documenti).

Inoltre, è stato emanato il "Codice Dell'Amministrazione digitale", il D.Lgs n. 82 del 7 marzo del 2005 (GU 16/05/2005 s.o. n. 93/L) entrato in vigore a partire dal 1 gennaio 2006, che vuole contribuire a rendere ancora più omogeneo il quadro di riferimento; da questa data tutte le disposizioni non riunite e coordinate all'interno del Codice sono state abrogate. Il Codice è stato recentemente rivisto dal D.Lgs. n. 235 del 30 dicembre 2010, allo scopo di rendere il quadro normativo più coerente alle innovazioni tecnologiche occorse negli ultimi anni.

Infine il DPCM 03/12/2013 (GU n. 59 del 12-03-2014) 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, traccia le regole per la conservazione a norma, andando ad abrogare la Deliberazione CNIPA 11/2004**.**

3.2 Principali riferimenti normativi

1) *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 ai sensi degli articoli 20, 22, 23 -bis, 23 -ter, 40, comma1, 41, e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.
2) *Decreto del 17 giugno 2014 del Ministero dell'Economia e delle Finanze* – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici ed alla loro riproduzione su diversi tipi di supporto.
3) *Decreto del Presidente del Consiglio dei Ministri del 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.

4) *Decreto del Presidente del Consiglio dei Ministri del 3 dicembre 2013* - Regole tecniche per il protocollo informatico ai sensi degli articoli 40 -bis, 41, 47, 57 -bis e 71, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005.

5) *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 sensidegli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 *(GU n.117 del 21-5-2013).*

6) *Decreto Legislativo del 30 dicembre 2010* – Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n. 69.

7) *Decreto-Legge 29 novembre 2008, n. 185, coordinato con la legge di conversione 28 gennaio 2009, n. 2 – Misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale* – Modifiche al CAD in materia di copie informatiche di documenti analogici, modifiche al Codice Civile in materia di documentazione informatica.

8) *Decreto Legislativo del 7 marzo 2005, n. 82 – Codice dell'amministrazione digitale* – Testo che rappresenta la base per tutti i successivi interventi che verranno in tema di uso dei documenti digitali. In dettaglio si definiscono nuovamente i ruoli e le caratteristiche dei documenti informatici e se ne amplia l'utilizzo; in particolare, la PA vede imporre un uso delle tecnologie informatiche e la pressoché totale dematerializzazione dei documenti nei rapporti tra cittadini, imprese e pubblica amministrazione.

9) *Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche* – Codice in materia di Protezione dei Dati Personali.

10) *Decreto del Presidente della Repubblica 28 dicembre 2000 n. 445* – Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. Testo coordinato con le modifiche apportate dal D.Lgs 23 gennaio 2002, n. 10 e dal DPR 7 aprile 2003, n. SQ01-00-02 Procedura per la gestione della documentazione. Questo DPR è stato per la maggior parte sostituito dal Codice dell'amministrazione digitale in vigore dal 1° gennaio 2006.

3.3 La normativa in ambiente clinico-sanitario

Testo normativo	Contenuto
Circolare Ministero della Sanità 19 dicembre 1986, n. 61	Prescrive il periodo minimo di conservazione della documentazione sanitaria presso le istituzioni sanitarie pubbliche e private di ricovero e cura, non andando ad impattare sulle modalità della conservazione stessa. In particolare richiama un periodo di conservazione illimitato per la cartella clinica e un periodo minimo di 20 anni per le radiografie e la documentazione diagnostica in genere. Il servizio di Conservazione Sostitutiva adempie certamente alla previsione se è in grado di garantire l'integrità, l'immodificabilità e sicurezza dei documenti in esso depositati per un periodo illimitato, pur prevedendo la possibilità di una cancellazione logica dei dati in un arco di tempo più limitato.
D.lgs 17 marzo 1995, n. 230 Attuazione nazionale delle Direttive Euratomnn. 80/836, 84/467, 84/466, 89/618, 90/641 e 92/3, in materia di radiazioni ionizzanti	Tratta di radiazioni ionizzanti, dei limiti di esposizione e delle modalità di smaltimento dei rifiuti radioattivi. Ai sensi dell'art. 62, il datore di lavoro assicura la tutela dei propri lavoratori da rischi da radiazioni ionizzanti, nel caso in cui lo svolgimento delle attività dovesse prevedere l'accesso in strutture esposte a rischio da radiazioni, in particolare garantendo di ottemperare agli obblighi informativi e di tutela nei confronti dei lavoratori.

DM 14.2.1997 Norma di attuazione del D.lgs n.230/95, "Determinazione delle modalità affinché i documenti radiologici e di medicina nucleare e i resoconti esistenti siano resi tempestivamente disponibili per successive esigenze mediche, ai sensi dell'art. 111, comma 10, del decreto legislativo 17 marzo 1995, n. 230"	Detta disposizioni per la disponibilità dei documenti radiologici (iconografie) per non meno di 10 anni e illimitata per i resoconti radiologici (referti), inoltre detta regole, all'art.6, per il contenuto del riferimento d'archivio. Il sistema di Conservazione Sostitutiva consente l'esibizione dei documenti conservati, ottemperando in pieno all'obbligo di disponibilità dei documenti per tutta la durata del processo di conservazione. I riferimenti d'archivio sono parte integrante dei metadati associati al singolo documento conservato.
L. 15 marzo 1997, n. 59 Art.15, co.2: "Gli atti, dati e documenti formati dalla pubblica amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e trasmissione con strumenti informatici, sono validi e rilevanti a tutti gli effetti di legge"	L'articolo citato stabilisce la validità dei documenti informatici ai fini di Legge, garantendo, di conseguenza, la validità dei documenti contenuti in un sistema di Conservazione Sostitutiva, sviluppato secondo le regole imposte dal D.Lgs 82/2005 e dalla normativa in materia di conservazione.
D.lgs 26 maggio 2000, n. 187 Attuazione della direttiva 97/43/Euratom in materia di protezione sanitaria delle persone contro i pericoli delle radiazioni ionizzanti connesse ad esposizioni mediche	Il nucleo della norma è rivolto alla protezione delle persone contro i pericoli delle radiazioni ionizzanti, pur individuando, in allegato 4, dei requisiti specifici per i sistemi di rilevamento delle immagini, nonché dello sviluppo di queste su pellicola. Se il sistema di Conservazione è integrato al REPOSITORY, il sistema di Conservazione accoglie al suo interno i medesimi documenti posti all'interno dei sistemi sanitari, non andando ad inficiare la qualità di essi ma anzi garantendo la loro sicurezza, immodificabilità e integrità.
D.lgs 30 giugno 2003, n. 196 Codice in materia di protezione dei dati personali	Il Codice in materia di protezione dei dati personali tutela i dati personali e sensibili con l'obbligo per il titolare, responsabile e incaricati al trattamento di utilizzare particolari accorgimenti allo scopo di impedire la diffusione dei dati stessi senza il consenso dell'interessato. Il servizio di Conservazione Sostitutiva offerto da InfoCert prevede assoluto controllo degli accessi al sistema e ai dati in esso contenuti, in linea con quanto stabilito dal Codice e dalle regole tecniche in materia di conservazione.
Allegato B del D.lgs n.196/03 Disciplinare tecnico in materia di misure minime di sicurezza	La norma, che stabilisce regole generali per il trattamento di dati personali con strumenti informatici, va rispettata a tutela dagli accessi non autorizzati al sistema di conservazione e ai dati in esso contenuti.
Deliberazione Garante per la protezione dei dati personali23 dicembre 2004, n. 14 Contributo spese in caso di esercizio dei diritti dell'interessato	La deliberazione stabilisce il carattere gratuito dell'accesso ai dati personali detenuti da società pubbliche o private, da parte dei cittadini. La finalità è quella di non imporre oneri aggiuntivi a carico cittadino nel caso di accesso ai dati che lo riguardano: la norma è pienamente rispettata da un sistema di Conservazione Sostitutiva nel momento in cui l'esibizione della documentazione sottoposta a conservazione è un processo che non ha costi aggiuntivi rispetto al servizio di conservazione
Newsletter Garante per la protezione dei dati personali 27 febbraio 2005, n. 246 Accesso alle banche di dati, esibizione e diritti dei cittadini	L'articolo della newsletter ricorda quanto stabilito dalla Deliberazione 14 del 23 dicembre 2004, in merito al carattere gratuito dell'accesso ai dati personali da parte dell'interessato, caratteristica assolta dal sistema di conservazione in quanto l'esibizione dei documenti non presenti oneri aggiuntivi rispetto al servizio di conservazione
Prontuario di selezione per gli archivi delle aziende sanitarie locali e delle aziende ospedaliere, 2005	Atto di indirizzo che reca indicazioni sui tempi di conservazione dei documenti generati e/o custoditi da Aziende Sanitarie pubbliche ed accreditate, redatto dal Ministero per i Beni e la Attività Culturali, raccogliendo quanto stabilito dalla normativa diffusa in tema. Come per la Circolare 61/86, è possibile mantenere i documenti all'interno del sistema di Conservazione sostitutiva anche a durata illimitata, grazie a controlli periodici della leggibilità di essi e della loro integrità.

3.4 La normativa sulla fatturazione elettronica

Con il Decreto del 3 aprile 2013 n. 55, emanato dal Consiglio dei Ministri, sono state individuate le regole

tecniche e le linee guida per la gestione dei processi di fatturazione elettronica verso la Pubblica Amministrazione. Questo passo rappresenta l'ultimo passaggio del lungo percorso legislativo attivato con la Legge Finanziaria 2008 (più in dettaglio, la Legge 244 del 2007, articolo 1, commi da 209 a 214).Le disposizioni di cui alla suddetta legge finanziaria del 2008 prevedono che, al fine di semplificare il procedimento di fatturazione e registrazione delle operazioni imponibili, l'emissione, la trasmissione, la conservazione e l'archiviazione delle fatture emesse nei rapporti con le pubbliche amministrazioni, anche ad ordinamento autonomo, e con gli enti pubblici nazionali, anche sotto forma di nota, conto, parcella e simili, deve essere effettuata esclusivamente in forma elettronica.
A livello normativo, quindi, tutte le PA destinatarie non potranno né accettare le fatture emesse o trasmesse in forma cartacea né procedere al pagamento, neppure parziale, sino all'invio del documento in forma elettronica.

I fornitori delle amministrazioni pubbliche dovranno invece gestire il proprio ciclo di fatturazione esclusivamente in modalità di fatturazione elettronica.
Ecco le principali novità:

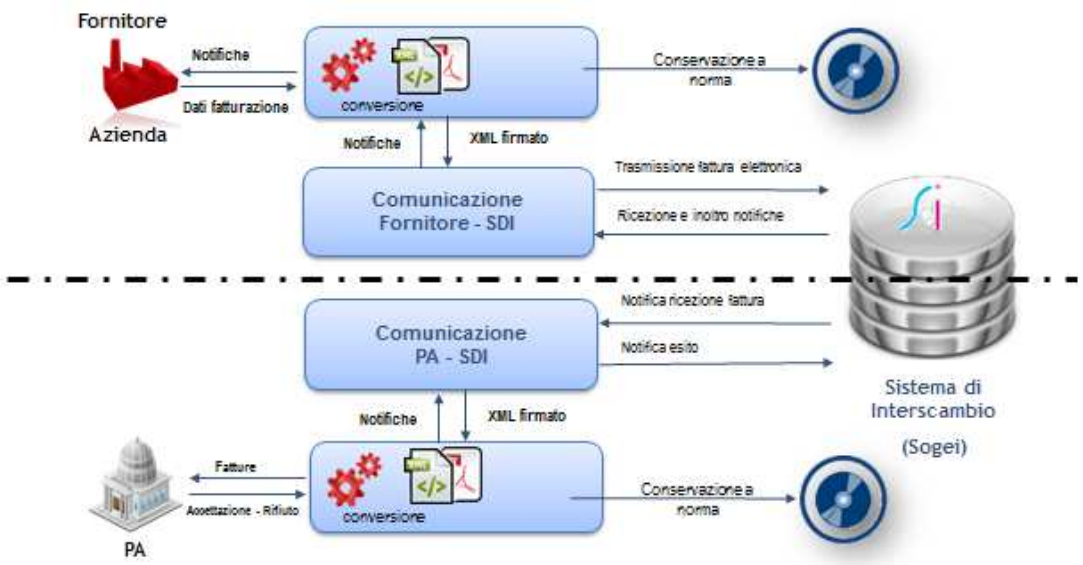
Decreto ministeriale 3 aprile 2013, numero 55
Art.2, comma 1. *Ai fini del presente regolamento,* ***la fattura elettronica reca i dati e le informazioni indicati e definiti nel documento recante «Formato della fattura elettronica» che costituisce l'allegato A del regolamento****.*
Art.2, comma 2. ***La fattura elettronica trasmessa*** *alle amministrazioni attraverso il Sistema di interscambio di cui al decreto del Ministro del'economia e delle finanze 7 marzo 2008* ***riporta obbligatoriamente le informazioni di cui ai paragrafi 3 e 4 dell'allegato A al presente regolamento****.*
Art.2, comma 3 ***Le regole tecniche*** *relative alle modalità di emissione della fattura elettronica, nonché alla trasmissione e al ricevimento della stessa attraverso il Sistema di interscambio,* ***sono quelle del documento che costituisce l'allegato B del presente regolamento****.*
Art.2, comma 3 ***La fattura elettronica si considera trasmessa per via elettronica****, …,* ***e ricevuta dalle amministrazioni*** *di cui all'articolo 1, comma 2,* ***solo a fronte del rilascio della ricevuta di consegna****, di cui al paragrafo 4 del documento che costituisce l'allegato B del presente regolamento,* ***da parte del Sistema di interscambio****.*
Art.3, comma 1 ***Le amministrazioni identificano i propri uffici deputati in via esclusiva alla ricezione delle fatture elettroniche da parte del Sistema di interscambio e ne curano l'inserimento nell'Indice delle Pubbliche Amministrazioni (IPA)****, …, in tempo utile per garantirne l'utilizzo in sede di trasmissione delle fatture elettroniche; le stesse amministrazioni curano altresì, agli stessi fini, l'aggiornamento periodico dei propri uffici nel predetto Indice,* ***che provvede ad assegnare il codice in modo univoco****.*

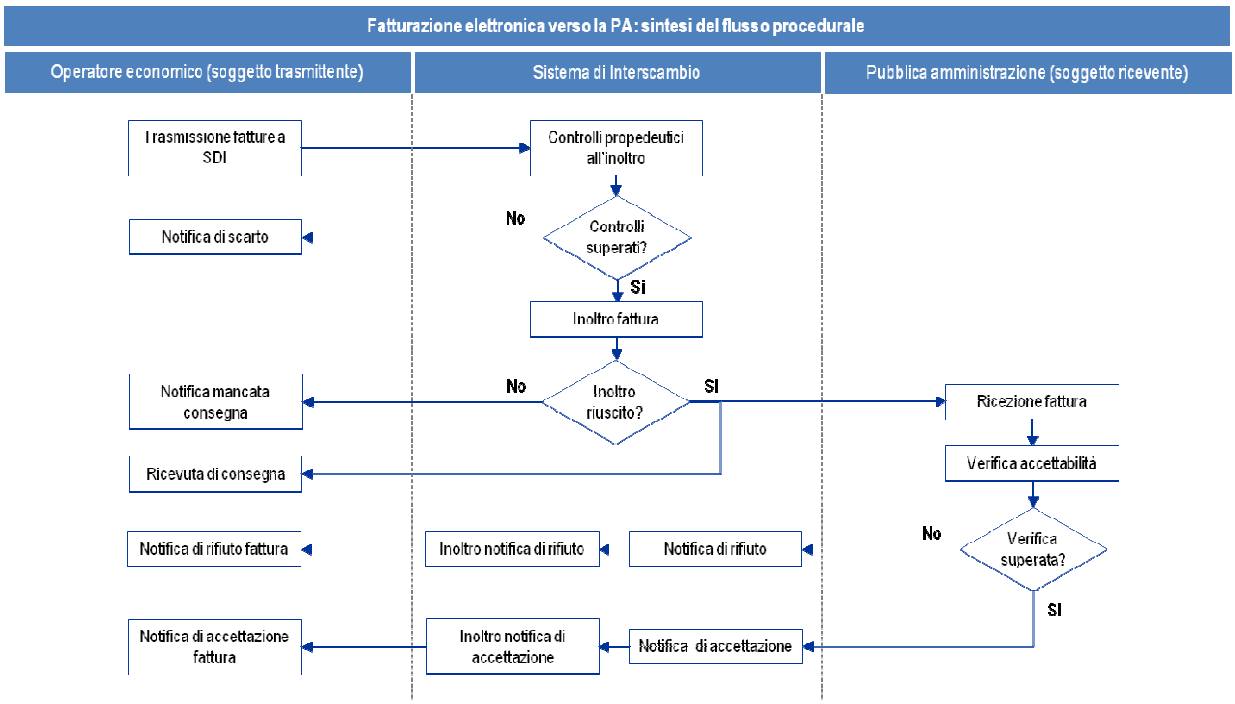
Obblighi e modalità di invio delle fatture elettroniche in conservazione digitale sono regolati dal Decreto MEF del 17 giugno 2014.

Articolo 1 commi dal 209 al 214 Legge numero 244 del 2007, Finanziaria 2008

- Emissione: esclusivamente in forma elettronica (XML) delle fatture, note, parcelle, conti e simili.
- Trasmissione: esclusivamente con strumenti elettronici, utilizzando il Sistema di Interscambio gestito dall'Agenzia delle Entrate, tramite il «braccio operativo» Sogei.
- Conservazione: esclusivamente e obbligatoriamente in forma elettronica, secondo le regole tecniche (Deliberazione CNIPA 11/2004, DPCM del 3 dicembre 2013 e DMEF del 17 giugno 2014).
- Pagamento: le PA destinatarie non potranno né accettare le fatture emesse o trasmesse in forma cartacea né procedere al pagamento, neppure parziale, sino all'invio del documento in forma elettronica.

Di seguito uno schema che descrive le attività previste per il processo di fatturazione elettronica verso la PA





Processo di Fatturazione Elettronica verso la PA

3.5 La conservazione sostitutiva dei documenti

L'implementazione e la gestione dei processi di creazione e conservazione dei documenti elettronici e di conservazione sostitutiva è una operazione che si avvale di numerosi strumenti ed elementi, regolata da apposite discipline che vanno raccordate alla disciplina generale della conservazione.

Di seguito si richiamano i principali strumenti ed elementi:

- ***Documento informatico***: è una realtà immateriale e il tipo di supporto fisico sul quale esso è registrato è irrilevante per la natura del documento stesso.
  Del documento informatico, a differenza di quello cartaceo, è possibile avere molteplici esemplari, tutti giuridicamente rilevanti e aventi identico valore legale. Per le sue caratteristiche, il documento informatico necessita di strumenti di validazione informatica efficaci e sicuri affinché ne siano garantite, in particolare, l'integrità e l'autenticità. Esemplificando, la gestione di un documento informatico non può prescindere dalla disponibilità di un elaboratore e dei relativi programmi necessari sia per "formare" il documento che per "leggerlo" e verificarne autenticità, integrità e paternità.
- ***Documento analogico***: in generale, è quello che per la sua formazione utilizza una grandezza fisica che assume valori continui come, ad esempio, le tracce continue su carta per il documento cartaceo o le immagini continue per il film. Il supporto fisico su cui si può formare il documento analogico non è necessariamente quello cartaceo, ma può essere film, lastra o pellicola radiologica, microfiche e microfilm, nastro audio e video. Il documento analogico può essere originale, a sua volta distinto in originale unico e non unico, o copia.
- ***Supporto di memorizzazione***: il supporto può essere ottico o non ottico, in quanto il documento esiste a prescindere dal supporto su cui è memorizzato. La deliberazione CNIPA 11/2004 autorizza l'utilizzo di un qualsiasi tipo di supporto di memorizzazione che consenta la registrazione mediante tecnologia laser (dischi ottici WORM e CD-R, dischi magneto-ottici o DVD). È data, inoltre, la possibilità di utilizzare un qualsiasi altro supporto di memorizzazione, oltre a quelli a tecnologia laser, nel rispetto delle regole tecniche previste ed in mancanza di altri motivi ostativi.
  Si è, infatti, raggiunta la consapevolezza del fatto che gli strumenti di firma digitale e di marca temporale garantiscono idoneamente l'integrità del documento nel processo di conservazione, indipendentemente dal supporto scelto. Gli stessi strumenti garantiscono anche la possibilità di trasmissione telematica dei documenti, senza che questo processo di trasmissione possa portare ad alterazioni di sorta.
- ***Firma digitale***: è l'elemento principale che interviene nella gestione elettronica del documento informatico dalla formazione, alla trasmissione, fino alla conservazione, poiché conferisce piena validità legale al documento cui è apposta, assicurando autenticità, integrità, non ripudiabilità.
- ***Attestazione temporale***: per stabilire il momento temporale in cui un documento informatico è stato formato è necessario attribuirgli una "validazione temporale", definita come il risultato di una procedura informatica in grado di offrire un riferimento temporale opponibile ai terzi. Lo strumento per ottenere questo risultato è la marca temporale, una particolare firma elettronica che contiene l'ora e la data in cui è stata generata ed è opponibile ai terzi.

Il fine ultimo del processo di conservazione è rendere un documento inalterabile ed immodificabile, in modo che possa essere disponibile nel tempo nella propria autenticità ed integrità.

In linea generale non sono previste autorizzazioni preventive per l'adozione di criteri operativi per effettuare la conservazione sostitutiva. Per effettuare la riproduzione e la conservazione dei documenti su supporti digitali, tuttavia, è necessario rispettare le regole previste da Codice dell'Amministrazione Digitale e dal DPCM 03/12/13.

3.6 La deliberazione CNIPA n. 11 del 19 febbraio 2004 e le Nuove Regole Tecniche (DPCM 03/12/2013)

Le Regole Tecniche del DPCM 03/12/2013 dettano le regole valevoli, in generale, per le procedure di riproduzione e conservazione dei documenti. Il Decreto ridefinisce il quadro normativo di riferimento, mutato grazie al progresso tecnologico, adattandolo alle nuove situazioni. Si precisa che i sistemi di conservazione già esistenti alla data di entrata in vigore del presente decreto sono adeguati entro e non oltre 36 mesi dall'entrata in vigore del decreto 03/12/13 secondo un piano dettagliato. Fino al completamento di tale processo restano validi i sistemi di conservazione realizzati ai sensi della deliberazione CNIPA n. 11/2004. Il Responsabile della Conservazione valuta l'opportunità di riversare nel nuovo sistema di conservazione gli archivi precedentemente formati o di mantenerli invariati fino al termine di scadenza di conservazione dei documenti in essi contenuti, così come previsto dall'Art. 14 del DPCM 03/12/13.

3.7 Il Responsabile della Conservazione

Come già per la deliberazione AIPA n. 42/2001, la Deliberazione CNIPA n. 11/2004 (art. 5) e le Regole Tecniche del DPCM 03/12/2013 enfatizzano il ruolo del Responsabile della Conservazione di documenti in formato digitale che assume un ruolo fondamentale all'interno del processo di conservazione sostitutiva, insieme ai suoi delegati o ai terzi affidatari. Il Responsabile della Conservazione in AO è la Dott.ssa Caterina Dalla Zuanna, designata con Deliberazione del Direttore Generale n. 1505 del 30/10/2015.

La presenza del Responsabile della Conservazione è necessaria sia in ambito privato sia in ambito pubblico e vi sono attributi compiti debitamente elencati, riguardanti le funzioni, gli adempimenti, le attività e le responsabilità. Il Responsabile della Conservazione è tenuto a gestire il processo in coerenza con quanto stabilito dalla normativa in vigore.

Uno dei obiettivi principali del Responsabile della Conservazione sostituiva è di definire ed impostare il processo per il trattamento della documentazione soggetta a conservazione sostituiva.

Più in particolare (art. 7 del DPCM 03/12/2013):

a) definisce le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti da conservare, della quale tiene evidenza, in conformità alla normativa vigente;

b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;

c) genera il rapporto di versamento, secondo le modalità previste dal Manuale di conservazione;

d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal Manuale di conservazione;

e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;

f) assicura la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità degli archivi e della leggibilità degli stessi;

g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;

h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal Manuale di conservazione;

i) adotta le misure necessarie per la sicurezza fisica e logica del sistema di conservazione ai sensi dell'art. 12;

j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;

k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;

l) provvede, per gli organi giudiziari e amministrativi dello Stato, al versamento dei documenti conservati all'archivio centrale dello Stato e agli archivi di Stato secondo quanto previsto dalle norme vigenti;

m) predispone il Manuale di conservazione di cui all'art. 8 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Le Regole Tecniche all'art. 5 consentono di delegare in tutto o in parte le attività previste ad altri soggetti interni alla struttura e/o di affidarle a soggetti terzi (pubblici o privati) i quali sono tenuti ad osservare le disposizioni contenute nella deliberazione stessa.

4 Il sistema di creazione e gestione dei documenti

Per la descrizione funzionale ed operativa del sistema di gestione informatica dei documenti dell'AO, si rimanda al Manuale di Gestione del Protocollo (Delibera del Direttore Generale n. 1505 del 30/10/2015 avente ad oggetto "Adeguamento del Manuale per la gestione del protocollo informatico dell'Azienda Ospedaliera di Padova ai sensi del D.P.C.M. del 03.12.2013).

4.1 Strumenti utilizzati

Per l'invio al sistema di conservazione LegalDoc, l'AO si avvale dell'infrastruttura informatica aziendale, l' UOC Informatica. Preliminarmente al processo di Conservazione dei documenti e delle immagini vi è quello di archiviazione, che è un processo mediante il quale i dati vengono univocamente identificati mediante un codice ed archiviati in appositi Database aziendali:

1. Repository di Noemalife (Galileo) per i referti di laboratorio, trasfusionali e anatomia patologica, ecc..
2. Gestionale contabile SCI di GPI
3. Protocollo informatico/Gestore documentale WebRainbow di CBT

Da questi Repository i documenti vengono estratti e inviati in conservazione attraverso LegalCare, come si specificherà in seguito.

4.2 Servizi di certificazione

Firma digitale

L'AO utilizza per l'apposizione di firme digitali smart card di InfoCert distribuite a medici e dirigenti amministrativi.

Firma automatica remota

Per firma automatica si intende una particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore, che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.

Per firma remota si intende una particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM (Hardware Security Module), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.

I certificati di firma digitale saranno rilasciati prevalentemente a medici che utilizzeranno il servizio per la firma dei documenti clinico sanitari e saranno rilasciati con il limite d'uso per la firma dei documenti prodotti dagli applicativi clinico sanitari presenti all'AO.

Il grande valore aggiunto per i medici firmatari è quello di poter apporre firme digitali senza dover ricorrere ad alcun dispositivo (smart card o token USB).

Il servizio si caratterizza per il disaccoppiamento tra la componente (L-Care - in locale presso l'AO) e la componente di firma vera e propria (LegalCert - in ASP e fisicamente posta nei locali di InfoCert). Il vantaggio della soluzione in ASP consiste nel fatto che l'AO è svincolata dalle problematiche di gestione sicura dei metadati e di controllo dei processi di apposizione della firma digitale su HSM (Hardware Security Module), poiché tali processi vengono svolti in remoto, sotto il presidio di InfoCert.

Il servizio è realizzato e gestito in partnership da InfoCert e LinkVerse.

Il Codice dell'Amministrazione Digitale (D.Lgs. n. 82/2005) all'art. 32 precisa, ovviamente, che il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

All'art. 35 comma 3 si precisa inoltre che la firma con procedura automatica è valida se apposta previo consenso del titolare all'adozione della procedura medesima.

L'attivazione del certificato tramite il portale di gestione rilasciato dalla Certification Authority di InfoCert avviene, di fatto, con Alias, PIN e OTP ricevuto via sms.

Successivamente il medico potrà gestire l'attivazione/disattivazione della propria firma sempre tramite il portale di gestione.

L'utilizzo del certificato per l'apposizione della firma avviene mediante autenticazione alla procedura informatica tramite credenziali di accesso e tramite credenziali di utilizzo del certificato (Alias e PIN) inserite a ogni sessione di lavoro (ogni turno o più volte in un turno).

Le Regole Tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, del DPCM del 22 febbraio 2013, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71 del Codice dell'Amministrazione Digitale all'art. 5 aggiungono che se il soggetto appone la sua firma elettronica qualificata o firma digitale per mezzo di una procedura automatica ai sensi dell'art. 35, comma 3 del Codice, deve utilizzare una coppia di chiavi destinata a tale scopo, diversa da tutte le altre in suo possesso.

L'utilizzo di tale procedura deve essere indicato esplicitamente nel certificato qualificato.

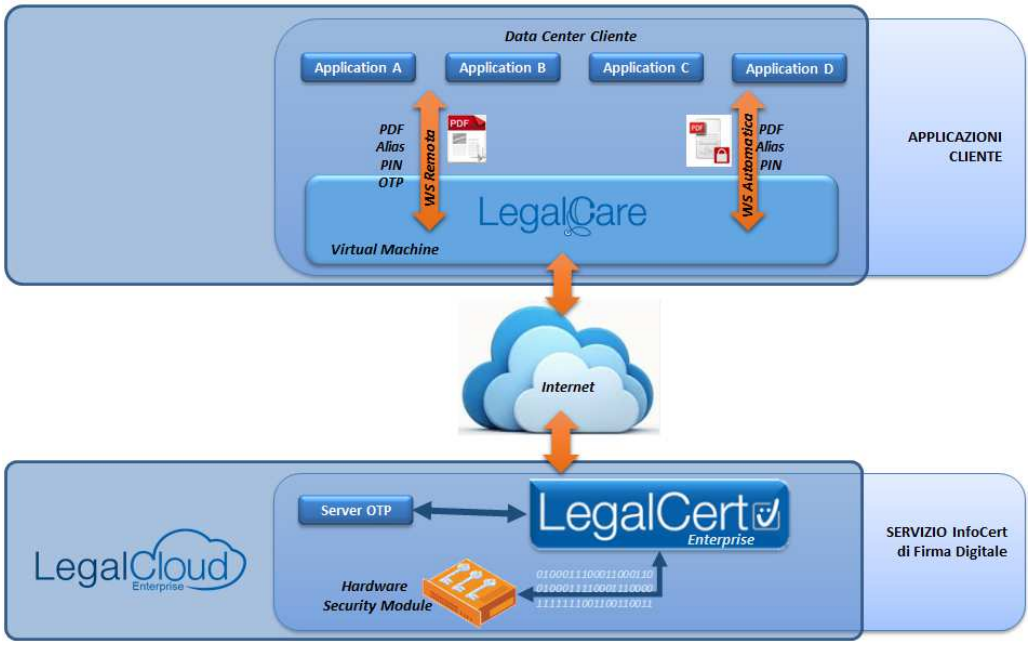
Se la procedura automatica fa uso di un insieme di dispositivi sicuri per la generazione della firma elettronica qualificata o firma digitale del medesimo soggetto, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

Quindi le condizioni normative essenziali sono:

- Consenso del titolare
- Generazione di una coppia di chiavi ad hoc e diversa dalle altre in possesso del titolare
- Generazione di una coppia di chiavi ad hoc e diversa per ciascun dispositivo utilizzato
- Dichiarazione di utilizzo inserita nel certificato qualificato
- Mantenimento del controllo da parte del titolare.

Lo strumento LegalCare Proxy Sign si basa su due servizi in modalità web service REST (uno per la firma remota e uno per la firma automatica) e questo sistema si interfaccia con l'HSM di InfoCert che contiene la chiave privata utilizzata per l'apposizione della firma sui documenti.

Di seguito uno schema dell'architettura predisposta:



Per ogni operazione che richieda l'accesso alle chiavi private delle credenziali di firma, LegalCare Proxy Sign invia le informazioni ai server InfoCert minimizzando la quantità di dati trasmessi e il carico sulla linea.

Tutte le operazioni sui dati vengono svolte localmente e nessuna informazioni riservata viene trasmessa all'esterno della rete dell'AO. L'accesso remoto viene usato solo per le attività che richiedono esplicitamente l'uso delle chiavi private massimizzando la sicurezza, la riservatezza e le prestazioni del sistema complessivo.

Il calcolo dell'impronta viene eseguito da LegalCare Proxy Sign e vengono inviati al server InfoCert solo l'impronta del documento da firmare e i dati di autenticazione della credenziale da usare per la firma.

Aver concentrato su una soluzione software centralizzata le logiche e la tecnologia di sicurezza legata alle operazioni di firma, comporta il significativo vantaggio della semplificazione delle componenti da implementare all'interno delle applicazioni.

Di seguito il dettaglio degli applicativi all'interno dell'AO che dialogano con il LegalCare Proxy Sign, delle tipologie documentali firmate e delle figure professionali coinvolte:

TIPOLOGIA DOCUMENTALE	APPLICATIVO	FIGURA PROFESSIONALE FIRMATARIA	DESCRIZIONE
Referti ambulatoriali e lettere di dimissioni	Galileo	Medici	I documenti (lettere di dimissione, referti ambulatoriali e di consulenze) prodotti direttamente da sistema ERP Aziendale (Galileo) vengono firmati dallo stesso con firma automatica.
Verbali di pronto soccorso	SSI (con Calamaio)	Medici	I verbali di pronto Soccorso prodotti direttamente dal sistema ERP Aziendale (SSI) vengono inviati al sistema di firma (Calamaio) e ivi firmati digitalmente con firma automatica.
Ordini	Iungo	Responsabili Ufficio Acquisti	Iungo è una piattaforma Web che consente l'invio informatico degli ordini di acquisto a fornitore tramite modalità multi-canale (email standard, email HTML strutturata, web

			service).Gli ordini d'acquisto vengono acquisiti direttamente dal sistema ERP Aziendale (SCI) e inviati al fornitore tramite la piattaforma e ivi firmati digitalmente con firma remota.
Cartellino ambulatoriale FKT	Arkimede	Medici	I referti vengono prodotii e firmati digitalmente con firma remota dal sistema aziendale Arkimede e inviati a Galileo per la conservazione.
Referti imaging diagnostici (Radiologici e Ambulatoriali)	Eris	Medici	I referti (testuali e strutturati) prodotti dal sistema RIS Aziendale (Eris) e Ivi firmati con firma automatica, vengono poi inviati a Galileo per la conservazione.

4.3 Controlli

Ai sensi di legge, l' AO, avvalendosi dei suoi fornitori, assicura che i documenti inviati in conservazione siano statici e non modificabili, ovvero redatti in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso ed è immutabile nel tempo.

4.4 Indicizzazione dei documenti

L'AO provvede all'indicizzazione dei documenti attraverso i sistemi Repository sopra elencati mediante l'utilizzo di apposite tabelle, descritte in seguito.

4.5 Gestione delle anomalie

Il sistema di conservazione LegalDoc è configurato per accettare solo documenti in formati prestabiliti e concordati con l'AO. Al venir meno di una di queste condizioni, sopraggiungendo l'impossibilità per LegalDoc di accettare il documento, L-care lascia in attesa il documento in entrata senza immetterlo nel sistema di conservazione e contestualmente segnala l'anomalia all'AO tramite la consolle di amministrazione, accessibile mediante autenticazione.

4.5.1 Descrizione generale del servizio LegalCare

LegalCare è composto da una componente locale (L-Care), installata presso l'AO, che si occupa del recupero dei documenti dai sistemi nativi e monitorizza i flussi documentali verso la componente remota (LegalDoc) che invece si occupa della conservazione a norma.

4.6 Formato dei documenti elettronici

Le nuove 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 (GU Serie Generale n.59 del 12-3-2014 - Suppl. Ordinario n. 20) elencano in modo specifico i formati documentali da adottare per la conservazione a lungo termine dei documenti, ovvero le modalità di organizzazione delle informazioni in un codice binario nel loro allegato.

AO ha deciso di inviare in conservazione i seguenti formati:

PDF – PDF/A

TIFF

JPG

Office Open XML (OOML)

Open Document Format

XML

TXT (dipende dalla codifica)

E-mail (Standard RFC 2822/MIME)

Eventualmente firmati digitalmente o marcati temporalmente.

5 Il sistema di conservazione documentale

5.1 Descrizione generale del servizio

LegalDoc è un servizio di conservazione dei documenti erogato in modalità ASP e sviluppato in base alle esigenze di imprese, professionisti, associazioni, Pubblica Amministrazione, che permette di mantenere e garantire nel tempo l'integrità e la validità legale di un documento informatico, nel rispetto della normativa vigente.

LegalDoc consente le funzionalità di:

- **conservazione** del documento, il documento, ricevuto negli Internet Data Center di InfoCert in formato digitale statico non modificabile, ovvero redatto in modo tale per cui il contenuto non possa essere alterabile durante le fasi di conservazione ed accesso, viene conservato a norma di legge per tutta la durata prevista dal contratto;
- **rettifica** di un documento conservato, un documento inviato in conservazione può essere rettificato dall'invio di un documento successivo. La rettifica non comporta la cancellazione del documento originario dall'archivio a norma ma è una modifica logica, nel pieno rispetto del principio di tracciabilità del documento;
- **cancellazione** di un documento conservato, un documento inviato in conservazione può essere cancellato, allegando eventualmente la motivazione della cancellazione. Il sistema terrà comunque traccia del documento all'interno dell'archivio a norma, nel rispetto del principio di tracciabilità del documento;
- **visualizzazione** di un documento conservato (esibizione a norma), il documento richiesto viene richiamato via web direttamente dal servizio di conservazione sostitutiva LegalDoc ed esibito con garanzia della sua opponibilità a terzi.

LegalDoc si integra con i sistemi installati presso l'AO, estendendone i servizi con funzionalità di stoccaggio digitale; il servizio LegalDoc, infatti, interviene solamente nella fase di conservazione ed esclusivamente per i documenti che l'Azienda sceglie di conservare.

5.2 Definizione di documento

In LegalDoc il documento è un insieme di uno o più file digitali, anche di diverse tipologie. Ad ogni documento è associato un file di controllo e un file delle direttive di conservazione, nonché un identificativo univoco generato da LegalDoc ("Token LegalDoc"). Il documento rappresenta l'unità minima di elaborazione nel senso che viene memorizzato ed esibito come un tutt'uno; non è possibile estrarre da LegalDoc parti di un documento.

Un documento conservato presso il sistema LegalDoc, quindi, ha le seguenti caratteristiche:

- è costituito da uno o più file;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso il token LegalDoc;
- appartiene a un lotto di documenti, a sua volta identificato univocamente nel sistema di conservazione;
- è conservato insieme al file delle direttive di conservazione, al file di ricevuta e al file di controllo del documento.

I documenti inviati nei formati standard, dettagliati nella documentazione contrattuale a disposizione dell'Azienda, sono visualizzabili mediante i relativi software definiti e messi a disposizione da InfoCert. Al momento dell'attivazione del servizio, l'AO verifica che i documenti inviati siano nel formato standard leggibile con il software definito da InfoCert.

5.3 Configurazione dei sistemi

5.3.1 Modalità di erogazione

Il servizio di conservazione sostitutiva LegalDoc è implementato da una applicazione software appositamente sviluppata a tale scopo (applicazione Java in architettura distribuita, ossia costituita da molteplici componenti) e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, PEC).

LegalDoc consente all' AO di accedere ai servizi di conservazione sostitutiva dei documenti informatici da un elaboratore elettronico, gestito da InfoCert e fisicamente posto nei locali di quest'ultima, in conformità a quanto descritto nel documento [1] *Condizioni Generali di Contratto* e nella relativa documentazione tecnica da questo referenziata.

Il servizio è accessibile dalla apposita URL di rete; AO richiama i servizi di LegalDoc secondo le modalità indicate da InfoCert nella documentazione contrattuale.

Figura 1 offre uno schema esemplificativo del dialogo tra l'applicazione di AO e LegalDoc.

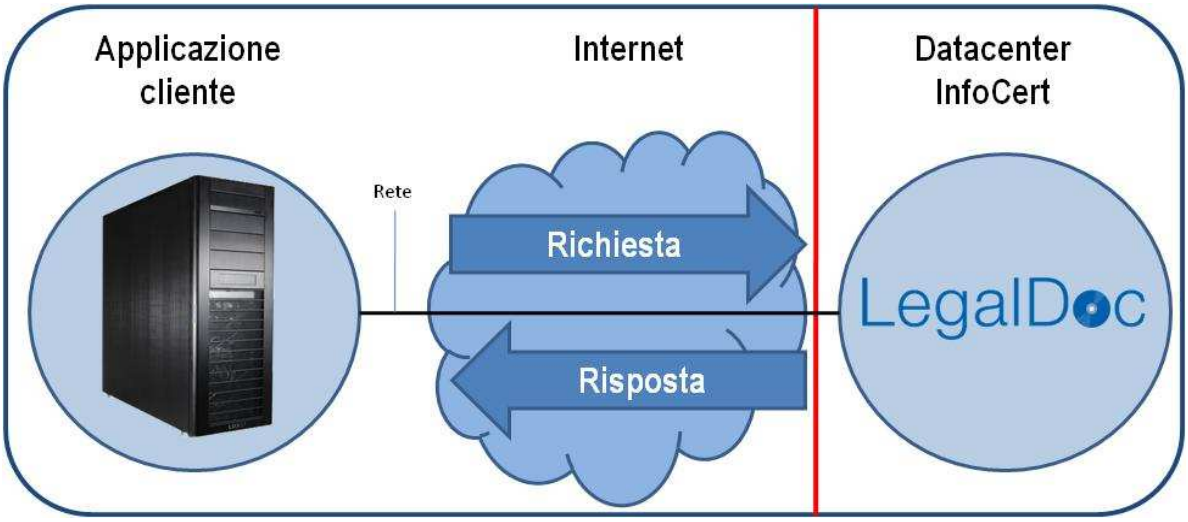


Figura - Dialogo tra il sistema di gestione dell'AO e il sistema di conservazione documentale LegalDoc

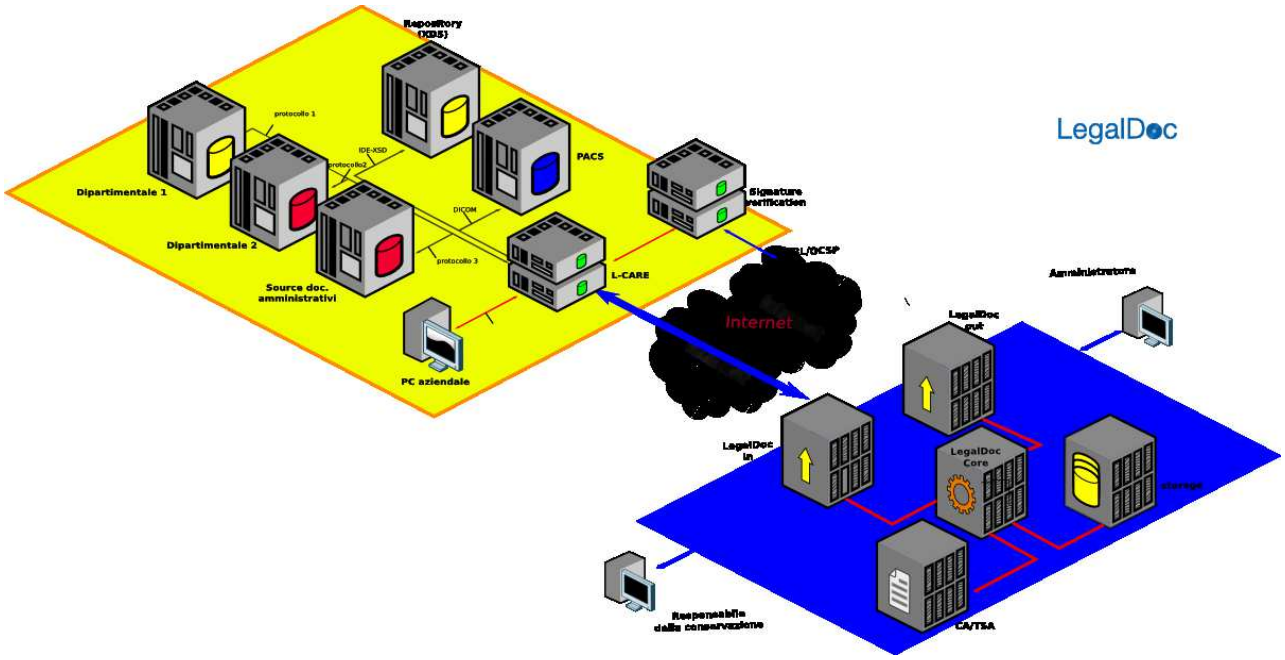
5.4 Componenti

5.4.1 Componente LegalCare

LegalCare è la soluzione integrata per la conservazione sostitutiva di documenti siano essi referti o immagini cliniche.

LegalCare è composto da una componente locale (L-Care), installata presso l'Azienda Ospedaliera che si occupa del recupero dei documenti dai sistemi nativi e monitorizza i flussi documentali verso la componente remota (LegalDoc) che invece si occupa della conservazione sostitutiva a norma.

L'architettura generale è schematizzata a titolo di esempio nella seguente figura:



Il servizio di conservazione si caratterizza per il disaccoppiamento tra la componente L-Care (in locale presso l'AO) e la componente di conservazione (LegalDoc - in ASP, descritta nei paragrafi precedenti). Il vantaggio dell'adozione di L -Care sta nel fatto di utilizzare una componente che risolve tutte le problematiche di acquisizione dei dati sollevando il cliente dalle incombenze dovute alla integrazione tra sistemi complessi.

5.4.2 Componente locale L-Care

La componente locale L-Care si configura come il punto di consolidamento prima delle operazioni di conservazione a norma in ASP. Questo elemento, è in grado di interfacciarsi con i flussi di lavoro sanitari per ricevere, prelevare o catturare documenti e metadati ad essi associati al fine di costituire l'insieme dei dati da sottoporre al flusso di conservazione.

Il ruolo di L-care è quello di mediare il più possibile la molteplicità e l'eterogeneità dei flussi informativi dell' AO con una piattaforma di conservazione stabile e general-purpose come LegalDoc.L-CARE è uno strumento dinamico e ricco di plug-in per la comunicazione con altri applicativi: HL7 (v2.x o v3, via socket, web-service, filesystem, etc.), DICOM (store e print), SOAP (programmabile, es. conforme AS-SEVO-SELG#04), supporto database multi-protocollo (JDBC, ODBC, Perl::DBI, etc.), network filesystem (es. SMB/CIFS, NFS, etc.), file transfer protocol (es. FTP, SFTP, etc.), HTTP/HTTPS, WebDAV, SMTP, JMS, sistemi di cattura del traffico (es. packetcapture) e diversi formati di file per i metadati (es. TXT, XML, XLS, CSV, MDB, etc.).

5.4.3 Marca temporale

Per l'emissione delle marche temporali LegalDoc si avvale del sistema di marcatura di InfoCert, Certification Authority accreditata. La marca temporale viene richiesta al TSS (Time Stamping Service) che la restituisce firmata con un certificato emesso dalla TSA (Time Stamping Authority) di InfoCert.

Il TSS è sincronizzato via radio con l'I.N.RI.M di Torino (*Istituto Nazionale di Ricerca Metrologica*, già *Istituto Elettrotecnico Nazionale "Galileo Ferraris"*) ed è protetto contro la manomissione della sincronizzazione mediante misure fisiche e logiche, nel pieno rispetto delle norme di legge.

5.4.4 Firma digitale con dispositivo HSM

Al buon esito del processo di conservazione, il Responsabile del servizio della Conservazione InfoCert appone la propria firma digitale sul file di chiusura lotto mediante un sistema di firma automatica erogato dalla CA InfoCert, che si avvale di un dispositivo crittografico ad altre prestazioni HSM.

5.4.5 Supporti di conservazione

Ai fini della conservazione i documenti vengono raggruppati in lotti e ciascun lotto è corredato da un file indice (file di chiusura lotto) che contiene gli hash dei documenti appartenenti al lotto.

L'apposizione della firma digitale del Responsabile del servizio della Conservazione e della marca temporale sul file di chiusura lotto attestano la conservazione del lotto.

I lotti prodotti vengono archiviati mediante procedure e sistemi che consentono la memorizzazione permanente in più copie e l'immodificabilità di quanto memorizzato.

Inoltre, possono essere prodotte ulteriori copie di back-up su supporti ottici rimovibili, stoccati da InfoCert o inviati al Cliente su espressa richiesta.

5.4.6 Posta Elettronica Certificata

Il servizio LegalDoc si avvale del servizio PEC di InfoCert: in sede di attivazione del servizio, è stata definita per il Cliente una casella di posta certificata tramite la quale richiedere attività di supporto e inviare messaggi in genere alla casella di amministrazione assistenza.legaldoc@legalmail.it.

5.5 Controlli

I processi del servizio di conservazione sostituiva LegalDoc sono fortemente automatizzati; i sistemi di erogazione sono dotati di molteplici funzioni di controllo in grado di rilevare e segnalare eventuali anomalie in essere o potenziali.

I controlli effettuati possono essere distinti secondo le seguenti tipologie:

- controlli di processo;
- controlli periodici.

5.5.1 Controlli di processo

I controlli di processo sono i controlli che hanno luogo durante l'elaborazione dei documenti soggetti al processo di conservazione.

LegalDoc è un processo complesso che movimenta una consistente mole di dati, dei quali è necessario garantire costantemente l'integrità e la coerenza: per questo motivo sono attivati numerosi controlli automatici, che richiedono l'intervento del Responsabile della Conservazione solo al verificarsi di eventuali eventi anomali non gestibili in modo automatico.

Oltre a questi, le procedure di gestione del sistema prevedono un elenco di controlli manuali effettuati direttamente dal Responsabile della Conservazione o da un suo delegato.

5.5.2 Controlli periodici

In InfoCert è attiva una struttura appositamente preposta alla supervisione e controllo della gestione dei problemi e del rispetto dei livelli di servizio per tutte le applicazioni.

La struttura si avvale di un gruppo di lavoro trasversale all'azienda e utilizza strumentazioni di varia natura per la raccolta di dati relativi al funzionamento dei servizi.

5.5.3 Ispezione del sistema da parte delle autorità competenti

In occasione delle ispezioni del sistema di conservazione da parte delle autorità competenti, gli esiti delle stesse e gli eventuali rilievi apposti sono registrati su appositi verbali.

Qualora dalle attività di ispezione e controllo emergessero punti critici o aree di miglioramento, è impegno di InfoCert l'attivazione delle strutture competenti per la tempestiva analisi della situazione e l'approntamento di tutte le misure necessarie al miglioramento del sistema e/o delle performance.

5.5.4 Incident management

InfoCert è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione documentale, al fine di individuare previamente ogni potenziale causa di incidente e provvedere alla sua rimozione, scongiurando il blocco del sistema o il danneggiamento dei file in esso contenuti.

I fornitori dei sistemi tecnologici utilizzati forniscono ad InfoCert tutte le opportune assicurazioni, rese per iscritto, contro il rischio di perdita dei documenti conservati.

Qualora si verificassero incidenti di sistema o di processo, le operazioni di ripristino della funzionalità seguono le procedure definite e documentate; per ogni incidente con impatti sul rispetto della normativa, è redatto un apposito verbale secondo la procedura definita.

Il Responsabile della Conservazione mantiene il verbale degli incidenti e delle contromisure attuate, che divengono oggetto di opportuni incontri di miglioramento.

6 Le tipologie documentali

Tipologia di documento	Referti di radiologia, laboratorio, trasfusionali, medicina nucleare e di anatomia patologica
Natura del documento	Originali digitali firmati digitalmente dal medico refertante
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite chiamate web service SOAP con attachment dai sistemi GALILEO di NoemaLife, con restituzione degli indici dei documenti alle tabelle.
Modalità di esibizione	I dati degli indici per i referti conservati nel modo descritto sono resi disponibili in una tabella L-Care per consentire l'esibizione tramite l'unico punto (Broker Console).
Data di decorrenza del processo di conservazione elettronica	Dal 2007 al 2015

Tipologia di documento	Referti di radiologia, laboratorio, trasfusionali, medicina nucleare e di anatomia patologica
Natura del documento	Originali digitali firmati digitalmente dal medico refertante
Modalità di caricamento	I documenti e gli indici vengono inviati al sistema di conservazione tramite chiamata HL7 verso LegalCare dai sistemi GALILEO di NoemaLife. Al termine della conservazione avviene la restituzione del token al sistema chiamante.
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Dal 2015

Tipologia di documento	Deliberazioni Decreti e Determinazioni
Natura del documento	Originali digitali firmati digitalmente da dirigenti dell'Amministrazione
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite connettore web service verso LegalCare dai sistemi WebRainbow di CBT, con indici su apposite tabelle db e restituzione del token. Anche gli indici vengono poi invianti in LegalDoc.
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Dal 2013

Tipologia di documento	Documenti Protocollati E/U/I
Natura del documento	Originali digitali e copie per immagini

Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite connettore web service verso LegalCare dai sistemi WebRainbow di CBT, con indici su apposite tabelle db e restituzione del token. Anche gli indici vengono poi invianti in LegalDoc. L'invio avviene a un anno di distanza dalla data di consolidamento al protocollo.
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Da implementarsi a breve

Tipologia di documento	Registri giornalieri di Protocollo
Natura del documento	Originali digitali firmati digitalmente da dirigenti dell'Amministrazione
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite connettore web service verso LegalCare dai sistemi WebRainbow di CBT, con indici su apposite tabelle db e restituzione del token. Anche gli indici vengono poi invianti in LegalDoc.
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Da implementarsi a breve (con recupero del pregresso dal 12 ottobre 2015)

Tipologia di documento	Registri e Repertori (deliberazioni, decreti, albo on-line)
Natura del documento	Originali digitali firmati digitalmente da dirigenti dell'Amministrazione
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite connettore web service verso LegalCare dai sistemi WebRainbow di CBT, con indici su apposite tabelle db e restituzione del token. Anche gli indici vengono poi invianti in LegalDoc. L'invio avviene con cadenza annuale e a fine anno.
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Da implementarsi a breve

Tipologia di documento	FatturazionePA attiva
Natura del documento	Originali digitali XML firmati digitalmente
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite tabelle di frontiera GPI/Legal Care. I rapporti con il Sistema di Interscambio vengono gestiti direttamente da Digit_Go di GPI.
Modalità di esibizione	Broker Console

Data di decorrenza del processo di conservazione elettronica	Da 28 Dicembre 2015

Tipologia di documento	Fatturazione PA passiva e notifiche
Natura del documento	Documento digitale XML firmato digitalmente
Modalità di caricamento	I documenti vengono inviati al sistema di conservazione tramite tabelle di frontiera GPI/Legalcare. I rapporti con il Sistema di Interscambio vengono gestiti direttamente da Digit-Go di GPI
Modalità di esibizione	Broker Console
Data di decorrenza del processo di conservazione elettronica	Entro Dicembre 2016

7 Il processo di conservazione

Il processo di conservazione attuato da InfoCert prevede l'utilizzo di diversi strumenti e l'intervento di soggetti che concorrono a rendere l'erogazione del servizio affidabile e rispondente ai requisiti richiesti dalla legge.

Ai fini del trattamento dei documenti destinati alla conservazione, il servizio si divide in due categorie di processi:

- processi di front-end;
- processi di back-end.

7.1 Processi di front-end

I processi di front-end sono erogati in modalità batch da L- Care, e sono finalizzati a mettere in comunicazione i sistemi gestionali del Cliente con i servizi di LegalDoc e sono richiamati in modalità on-line.

Per ciascuno dei servizi indicati di seguito si eseguono opportuni controlli di autenticazione del soggetto chiamante e di correttezza e accettabilità delle richieste:

- invio di un documento informatico o di un documento analogico opportunamente digitalizzato in conservazione sostitutiva;
- rettifica o cancellazione per via telematica di un documento già conservato in modalità sostitutiva;
- esibizione di un documento direttamente dal sistema LegalDoc;
- elaborazione ed invio della richiesta di chiusura forzata del lotto;
- ottenimento per via telematica delle informazioni sullo stato di un documento o di un lotto.

7.2 Processi di back-end

I processi di back-end sono eseguiti dal sistema LegalDoc in modalità differita e sono i processi che, a partire dalle tabelle di frontiera connette L- Care ai sistemi dell'AO, implementano la conservazione in conformità alla normativa.

Il processo di conservazione si suddivide in due macro fasi:

- **elaborazione del singolo documento**. In questa fase viene analizzato il singolo documento, che viene assegnato a un lotto di documenti. Il documento viene corredato da un file di controllo, firmato digitalmente dal Responsabile della Conservazione, contenente informazioni sensibili ai fini della conservazione (indice del documento, impronte dei file che lo costituiscono, classificazione anagrafica dei firmatari, lotto di appartenenza);
- **elaborazione e chiusura del lotto**. Quando si raggiungono le condizioni per la chiusura del lotto, questo viene corredato da un file di chiusura lotto contenente informazioni sensibili ai fini della conservazione (identificativo univoco del lotto – token lotto –, criteri di omogeneità, hash del file di controllo). Al file di chiusura lotto viene apposta la firma digitale del Responsabile della Conservazione e la marca temporale; infine, l'insieme di documenti appartenenti al lotto, corredati dai rispettivi file di controllo e dal file di chiusura lotto, viene memorizzato nei supporti di conservazione e nelle copie di sicurezza.

7.3 Responsabilità del processo di conservazione

Nel processo di conservazione sostitutiva intervengono numerosi soggetti, a differenti livelli e con diverse responsabilità, sintetizzate nella tabella seguente e dettagliate per singola attività.

Responsabilità ⇘ *Attività* ⇙	*Responsabile della Conservazione AO*	*L- Care*	*LegalDoc*	*Responsabile del servizio di Conservazione (InfoCert)*
1. Formazione del documento	**R - E**			
2. Indicizzazione e archiviazione	**R - E**			
3. Acquisizione documento e creazione del file con le direttive di conservazione	**V**	**R - E**		
4. Invio al sistema di conservazione	**V**	**R - E**		
5.Verifica e accettazione del documento e invio della ricevuta di accettazione dei documenti			**E - V**	
6.Inserimento nel lotto e creazione del file di controllo			**E**	**R - V* - A**
7. Chiusura del lotto e attestazione di corretto procedimento			**E**	**R - V* - A**
8. Memorizzazione, creazione "copia di sicurezza" e chiusura del processo			**E**	**R - V* - A**
[**R**-responsabile; **E**-esegue; **V**-verifica; **A**-approva]				

(*)Tutte le verifiche in carico al Responsabile del servizio della Conservazione sono garantite anche dal servizio di auditing InfoCert.

7.4 Fasi del processo di conservazione: dettaglio generale

7.4.1 Formazione del documento

INPUT	*Documento da generare*	
AO	1.1	AO genera i documenti secondo le procedure descritte precedentemente
OUTPUT	*Documento generato*	

7.4.2 Indicizzazione e archiviazione

INPUT	*Documento da archiviare*	
AO	2.1	I sistemi Repositorye di Gestione documentale indicizzano i documenti corredati dei relativi metadati e li rendono disponibili tramite chiamate HL7 o tabelle db.
OUTPUT	*Documento indicizzato e archiviato*	

7.4.3 Acquisizione documento e creazione del file delle direttive con L-Care

INPUT	*File delle direttive da predisporre*	
L- Care	3.1	L- Care acquisisce i documenti informatici tramite le chiamate HL7di AO e li prepara alla conservazione.
	3.2	Il servizio L- Care esegue le seguenti operazioni: • Predisposizione del file con le direttive di conservazione; • Calcolo delle impronte dei file costituenti il documento; • Inserimento delle impronte nel file delle direttive; • Apposizione della firma elettronica sul file delle direttive; • Costruzione del messaggio contenente i file che costituiscono il documento.
OUTPUT	*File delle direttive predisposto*	

7.4.5 Invio al sistema di conservazione

INPUT	*Documento da inviare a LegalDoc*	
L- Care	4.1	Invoca i servizi di LegalDoc e invia il documento, il file degli indici di ricerca e la relativa richiesta di conservazione.
OUTPUT	*Documento inviato a LegalDoc*	

7.4.6 Verifica, accettazione e invio della ricevuta di accettazione del documento

INPUT	*Documento da verificare*	
LegalDoc	5.1	Acquisizione del documento.
	5.2	Sbustamento del messaggio e verifica della firma elettronica apposta sul file delle direttive di conservazione
	5.3	Presa in carico dei file costituenti il documento.
	5.4	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione.
	5.5	Generazione dell'impronta di ogni file del documento.
	5.6	Confronto dell'impronta generata con la corrispondente inviata dal Cliente per garantire l'integrità del documento ricevuto.
	5.7	Nel caso di esito negativo delle verifiche, il documento viene respinto con l'indicazione che descrive l'errore intercorso. In questo caso il flusso termina.
	5.8	Generazione del file di ricevuta a partire dal file delle direttive.
	5.9	Generazione di un identificativo univoco per il documento (token LegalDoc) e firma elettronica sul file di ricevuta.
	5.10	Invio a L- Care del file di ricevuta di presa in carico della richiesta di conservazione

L- Care	5.11	Riceve il file di ricevuta di presa in carico della richiesta di conservazione, ne estrae il token LegalDoc e lo memorizza presso i propri archivi, in associazione con gli indici di ricerca. Restituisce il token tramite il Sistema di NoemaLife.
OUTPUT	*Documento verificato*	

7.4.7 Inserimento nel lotto e creazione del file di controllo

INPUT	*Documento da conservare*	
LegalDoc	6.1	Verifica per ogni documento se esiste già un lotto di documenti aperto che possiede le caratteristiche specificate dal file delle direttive in cui inserire il documento; in caso contrario si predispone un nuovo lotto.
	6.2	Predisposizione del file di controllo del documento contenente l'indice del documento, le impronte dei file che lo costituiscono, la classificazione anagrafica del documento, il lotto di appartenenza, gli estremi di identificazione del Responsabile della Conservazione.
	6.3	Apposizione della firma elettronica del Responsabile della Conservazione sul file di controllo.
	6.4	Inserimento del file di controllo e del relativo documento nel lotto di conservazione.
OUTPUT	*Documento inserito in un lotto di conservazione*	

7.4.8 Chiusura del lotto e attestazione di corretto procedimento

INPUT	*Lotto da chiudere*	
LegalDoc	7.1	Chiusura del lotto dopo il raggiungimento delle condizioni di chiusura lotto: • raggiungimento della dimensione fisica del supporto disponibile definita in fase contrattuale; • raggiungimento del numero massimo di documenti per lotto gestibile dal sistema, fissato in 20.000 documenti; • raggiungimento della data massima di chiusura del lotto. Il lotto viene chiuso al verificarsi del primo dei precedenti eventi o in seguito alla ricezione della richiesta di chiusura forzata del lotto inviata dal Cliente.
	7.2	Generazione del file di chiusura lotto e inserimento degli hash dei file di controllo del documento.
Responsabile del servizio della Conservazione	7.3	Apposizione della firma digitale, necessaria ad attestare il corretto svolgimento del procedimento sul file di chiusura lotto.
	7.4	Apposizione della marca temporale sul file di chiusura lotto.
OUTPUT	*Lotto chiuso*	

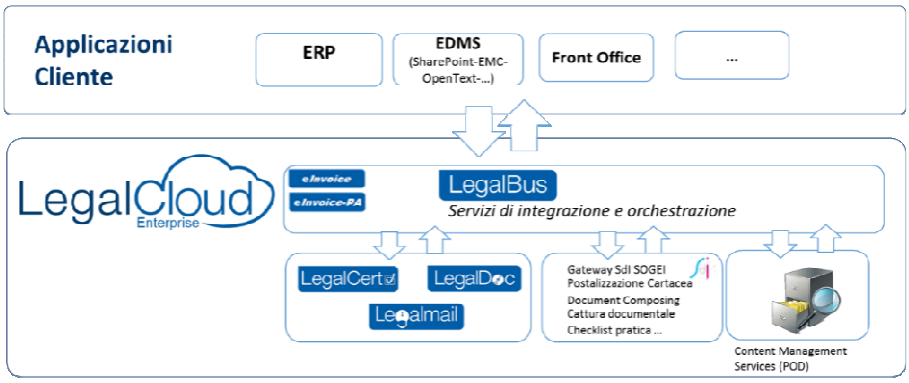
7.4.9 Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

INPUT	*Documenti da memorizzare*	
LegalDoc	8.1	Memorizzazione del lotto su supporto magnetico.
	8.2	Creazione della copia di sicurezza.
	8.3	Termine della procedura di conservazione.
OUTPUT	*Documenti conservati*	

7.5 Fasi del processo di conservazione: dettaglio sulle Fatture PA

Le componenti applicative interessate nel processo di gestione delle fatture PA sono le seguenti:

- LegalCare, installata presso la AO per la gestione del flusso di conservazione dei documenti XML di fatturazione e di notifica prodotti; LegalCare è composto da una componente locale (L-Care), installata presso l'AO, che si occupa del recupero dei documenti dai sistemi nativi e monitorizza i flussi documentali verso la componente remota (LegalDoc) che invece si occupa della conservazione digitale a norma.
- LegalBus, un middleware applicativo, facilmente integrabile, capace di orchestrare i vari servizi InfoCert. Di base integra, espone e richiama i servizi di firma digitale automatica massiva, di conservazione a norma e di posta elettronica certificata, così come rappresentato in figura.



Architettura di LegalCloud

- Servizio di Firma Digitale Automatica, che permette l'apposizione di firme digitali attraverso procedure automatiche, su un grande numero di documenti in breve tempo.
- Servizio di conservazione a norma LegalDoc, già utilizzato dall'AO per la tenuta dei documenti sanitari.
- Servizio di Posta Elettronica Certificata Legalmail, impiegato per le comunicazioni con il Sistema d'Interscambio tramite due caselle appositamente create.

7.5.1 Ciclo attivo

L'AO produce le FatturePA del suo ciclo attivo mediante il gestionale di contabilità e in formato XML, come previsto dalla normativa.

L'invio al Sistema di interscambio avviene mediante Legal-Care, il middleware di integrazione precedentemente descritto.

Le FatturePA, quindi, generate dal sistema di contabilità in uso, vengono inviate a L-Care,tramite Network File System, e conseguentemente a LegalBus, che si occupa:

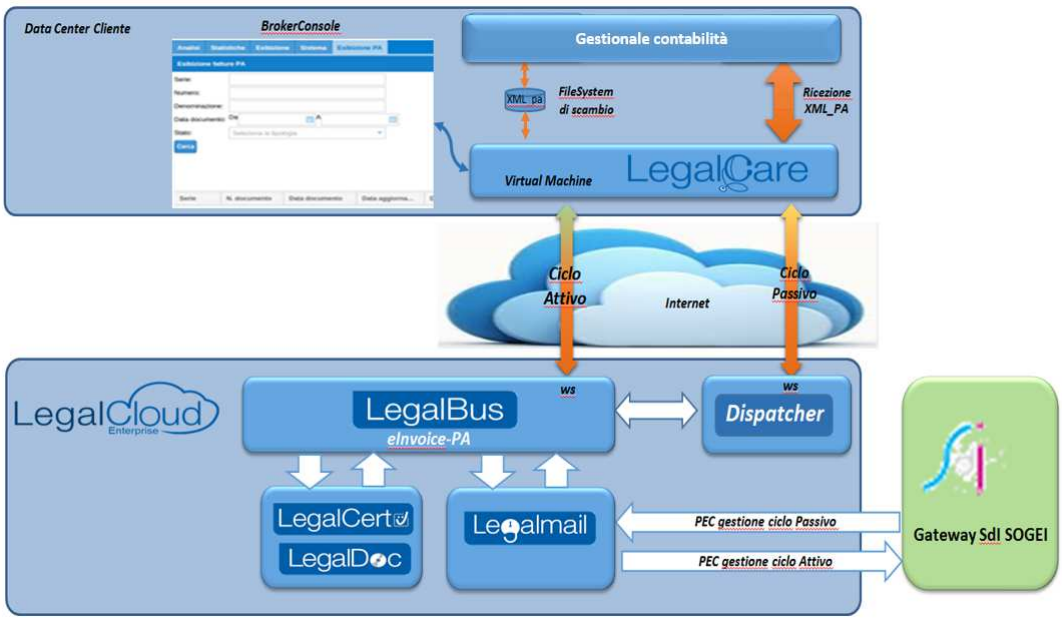
- dell'apposizione della firma digitale sulle fatture
- dell'invio tramite PEC dedicata al Sistema di Interscambio (di seguito SdI)
- della ricezione delle notifiche dal SdI
- dell'indicizzazione delle fatture e delle notifiche
- dell'invio in conservazione LegalDoc.

7.5.2 Ciclo passivo

L'AO riceve le FatturePA del suo ciclo passivo dal SdI in una PEC dedicata.

La componente LegalBus si occupa di colloquiare con il SdI di Sogei mediante l'utilizzo della casella PEC, ne sbusta il contenuto ed effettua le opportune verifiche di integrità e validità dei file XML firmati ricevuti in allegato alla PEC. LegalBus li rende disponibili al sistema LegalCare che, a sua volta, li trasmette al sistema di gestione documentale e contabile in uso presso l'AO.

Contemporaneamente LegalBus si occupa dell'invio al sistema di conservazione LegalDoc delle FatturePA e delle notifiche.



Architettura del processo

8 Procedure di ricerca ed esibizione

Le procedure di esibizione del documento integrate in LegalDoc permettono, a partire dalla funzione di ricerca in L-Care, di estrarre dal sistema un documento di cui sia completata la procedura di conservazione.

L'esibitore L-care (attraverso la Broker Console) è un'applicazione web, che permette ad un utente, in possesso delle credenziali, di accedere al sistema di conservazione LegalDoc da una qualsiasi postazione di lavoro.

L'interfaccia è organizzata a schede, ognuna delle quali tratta un aspetto relativo alla conservazione del documento.

Visualizzando il contenuto di ciascuna scheda diventa possibile:

- estrarre un documento e visualizzarlo a video
- produrre copia cartacea o su altro supporto informatico del documento
- estrarre i visualizzatori memorizzati nel sistema di conservazione permettendone l'installazione sulla stazione dove si sta svolgendo l'esibizione
- prendere visione dei file a corredo che qualificano il processo di conservazione attestandone il corretto svolgimento
- verificare la validità delle firme digitali e delle marche temporali apposte nel processo di conservazione
- verificare l'integrità del documento

L'esibizione del documento ottenuto tramite interrogazione al sistema LegalDoc rappresenta un'esibizione completa, legalmente valida ai sensi della deliberazione CNIPA 11 del 2004 e del DPCM del 3 dicembre 2013.

Di seguito si descrivono le fasi della procedura di ricerca ed esibizione.

8.1 Procedura di esibizione: dettaglio

8.1.1 Ricerca del documento da esibire

INPUT	*Lista di documenti*	
AO	1.1	Attraverso L- Care utilizzando gli indici archiviati nei propri Repository, ricerca il documento da esibire
OUTPUT	*Token relativo al documento da esibire*	

8.1.2 Invio della richiesta a LegalDoc

INPUT	*Richiesta di esibizione da preparare*	
L-Care	2.1	L-Care seleziona il token relativo al documento da esibire.
	2.2	Creazione del file delle direttive di esibizione, contenente il token LegalDoc relativo al documento da esibire, e sua sottoscrizione digitale.
	2.3	Chiamata al servizio LegalDoc.
OUTPUT	*Richiesta di esibizione presa in carico da LegalDoc*	

8.1.3 Ricerca del documento nel sistema ed esibizione

INPUT	*Richiesta di esibizione acquisita*

LegalDoc	3.1	Ricezione della richiesta di esibizione del documento.
	3.2	Controllo di corrispondenza tra il token LegalDoc inviato dall'AO e quelli dei documenti conservati; effettuazione della copia dei file costituenti il documento e dei file attestanti il processo di conservazione.
	3.3	Predisposizione delle copie di: • file costituenti il documento conservato • file di ricevuta • file di controllo del documento.
	3.4	Passaggio del pacchetto di file all'Esibitore L-care
OUTPUT	*Documento passato all'Esibitore L-care*	

8.1.4 Verifica del documento

INPUT	*Documento ricevuto dal sistema di conservazione*	
Esibitore L-care	4.1	Visualizzazione del pacchetto di file ed effettuazione di tutte le verifiche.
OUTPUT	*Documento esibito*	

8.1.5 Verifica del documento

INPUT	*Documento esibito*	
Esibitore L-care	5.1	Download del documento e memorizzazione dello stesso in locale
OUTPUT	*Documento salvato*	

Per maggiori dettagli operativi si rimanda al Manuale Utente dell'Esibitore in allegato.

9 Modifica dei documenti posti in conservazione

In caso di modifica dei documenti già posti in conservazione, l'AO provvede ad emanare ex novo un documento di rettifica che verrà a sua volta conservato a norma; la riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti dai sistemi Repository, che ne assicura la sistematicità e la coerenza.

9.1 La cancellazione di un documento

LegalDoc è configurato in modo da non consentire la cancellazione fisica di quanto conservato: il servizio di cancellazione consiste nella cancellazione logica del documento dal database.

La cancellazione può essere richiesta solo dal sistema di interfaccia a LegalDoc che ha fatto la richiesta di invio in conservazione del documento da cancellare.

10 Misure di sicurezza

10.1 Azienda Ospedaliera

Per le misure di sicurezza dei Repository nel trattamento dei documenti dell' AO si rimanda al Documento Programmatico per la Sicurezza approvato con Deliberazione del Direttore Generale n. 1810 del 31/12/2015.

Tutte le trasmissioni di dati tra l'AO ed InfoCert avvengono attraverso il canale sicuro HTTPS, nel pieno rispetto della normativa italiana ed europea sulla gestione della sicurezza dei dati sensibili e sanitari.

10.2 InfoCert

Il sistema LegalDoc è pienamente conforme ai requisiti di sicurezza prescritti dalle norme. Nel seguito sono descritte le modalità generali tecniche e le infrastrutture che InfoCert utilizza all'interno del proprio Data Center di Padova, in quanto fornitore del servizio di conservazione.

10.2.1 Sicurezza fisica

I locali che ospitano il sistema LegalDoc sono in un immobile la cui zona d'ubicazione non presenta rischi ambientali dovuti alla vicinanza ad installazioni pericolose. Durante la progettazione dello stabile sono stati presi opportuni accorgimenti per isolare i locali potenzialmente pericolosi, quali quelli contenenti il gruppo elettrogeno e la centrale termica. Per questi locali sono presenti le apparecchiature e gli accessori di controllo e di sicurezza previsti dalle norme in vigore. Lo stabile è inoltre sorvegliato da personale specializzato 24 ore al giorno.

La sala CED è l'area protetta all'interno dello stabile, accessibile mediante utilizzo del badge autorizzato, dove si trovano i dispositivi hardware e software dei diversi sistemi InfoCert.

L'accesso alla sala CED è consentito solamente alle persone autorizzate, ossia quelle con un ruolo operativo nell'erogazione del servizio e nella gestione dell'infrastruttura.

All'interno della sala CED sono collocate le sale denominate locale CA, accessibili mediante badge autorizzato e PIN (Personal IdentificationNumber) di accesso. L'accesso ai singoli locali del locale CA necessita di un ulteriore badge autorizzato.

La sala CED è dotata di telecamere a circuito chiuso, rilevatori combinati microonde e infrarossi, rilevatori ottici di fumo sul soffitto e nel sottopavimento, avvisatori manuali di allarme, avvisatori ottici acustici d'allarme per avviso locale, sensori piezodinamici per la rilevazione della rottura dei vetri. Tutte le porte sono dotate di allarme.

10.1.2 Gruppi di continuità

Tutte le apparecchiature del centro dati di InfoCert a Padova sono collegate alla rete elettrica attraverso gruppi di continuità che consentono di mantenere l'alimentazione alle apparecchiature in caso di interruzione dell'energia elettrica da parte del fornitore. In caso di assenza dell'alimentazione per pochi cicli, intervengono automaticamente delle batterie tampone in grado di mantenere la continuità elettrica. Qualora l'assenza di alimentazione si protragga per più di pochi secondi, vengono automaticamente avviati dei gruppi elettrogeni che iniziano a fornire l'alimentazione al gruppo di continuità.

10.1.3 Connessione a Internet

Il centro dati di InfoCert è connesso alla rete Internet con due collegamenti ATM separati, entrambi con velocità massima di 155 Mbit/sec.

Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati di interfaccia separati e completamente ridondati.

InfoCert è impegnata a mantenere tempi di attraversamento rete inferiori a 20 ms tra il proprio Centro Servizi e i nodi d'interconnessione con i principali provider italiani e internazionali.

10.1.4 Sicurezza delle reti: protezione da intrusioni

I sistemi e le reti di InfoCert sono connessi ad Internet in modo controllato da sistemi firewall che consentono di suddividere la connessione in aree a sicurezza progressivamente maggiore: rete Internet, reti DMZ (DeMilitarized Zone) o Perimetrali, Reti Interne. Tutto il traffico che fluisce tra le varie aree è sottoposto ad accettazione da parte del firewall, sulla base di un set di regole stabilite.

Le regole definite sui firewall vengono progettate in base a due principi: in primis il “default deny”, ossia quanto non è espressamente permesso è vietato di default ed è, quindi, consentito solo quanto è strettamente necessario al corretto funzionamento dell'applicazione. Il secondo principio consiste nel “defense in depht”, secondo il quale vengono organizzati livelli successivi di difesa, prima a livello di rete, tramite successive barriere firewall, poi a livello di sistema (hardening).

InfoCert provvede alla gestione e all'implementazione delle regole di sicurezza dei firewall. I sistemi firewall sono configurati in alta affidabilità (HA), ovvero sono formati da coppie di macchine indipendenti, collegate tra loro e gestite tramite appositi software in modo che, in caso di guasto di una delle macchine, il traffico venga dirottato sulla macchina di backup.

11 Note conclusive

11.1 Protezione dei dati personali

Nelle fasi di creazione, digitalizzazione, trattamento e invio in conservazione della documentazione cartacea e elettronica,l'AO pone la massima cura nel rispetto delle disposizioni stabilite dal D.Lgs n. 196/2003 "Codice in materia di protezione dei dati personali".

Ai sensi dell'articolo 29 Codice, l'AO ha nominato InfoCert SpA Responsabile dei trattamenti dei dati necessari all'esecuzione del servizio (allegato [2]).

In particolare, anche in considerazione del ruolo di Responsabile della Conservazione ricoperto, i compiti affidati ad InfoCert SpA attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati.

InfoCert opera quale Responsabile del trattamento applicando le misure di sicurezza in base alle disposizioni legislative e regolamentari in vigore.

12 Allegati

12.1 Documentazione contrattuale di riferimento

Si fornisce di seguito un elenco dei documenti contrattuali a cui il Manuale si riferisce e che vengono tenuti agli atti e disponibili alla richiesta di esibizione.

I documenti sotto riportati si intendono come riferimenti ufficiali: eventuali discrepanze fra quanto indicato nel Manuale e quanto presente nei documenti presenti nel seguente elenco si risolvono in favore di questi ultimi.

[1] Richiesta di attivazione con Condizioni Generali di Contratto – Regola il rapporto tra InfoCert e AO;

[2] Atto di Affidamento del procedimento di conservazione – formalizza l'affidamento ad InfoCert del processo di conservazione, delineandone l'ambito di applicazione;

[3] Allegato Tecnico– descrive le modalità di fornitura del servizio e l'infrastruttura utilizzata per la sua erogazione;

[4] Manuale Utente LegalDoc;

L'Atto di nomina del Responsabile della Conservazione Interno all'AO è contenuta all'interno del Manuale di gestione del protocollo (Delibera del Direttore Generale n. 1505 del 30/10/2015 avente ad oggetto "Adeguamento del Manuale per la gestione del protocollo informatico dell 'Azienda Ospedaliera di Padova ai sensi del D.P.C.M. del 03.12.2013), a cui si rimanda per ulteriori dettagli.

Rif. Contratto (a cura di InfoCert) _____

AFFIDAMENTO DEL PROCEDIMENTO
DI CONSERVAZIONE
(ART. 6, COMMA VI, D.P.C.M. 3.12.2013)
SERVIZIO LEGALDOC

Denominazione_____

Comune_____ **CAP** _____ **Sigla prov.**_____

Cod. Fisc._____ **Partita IVA**_____

Telefono/cellulare_____ **Fax**_____

Indirizzo *email* per comunicazioni (posta elettronica certificata)_____

Rappresentato da (Cognome/Nome)_____

Codice fiscale_____

nella qualità di legale rappresentante ovvero di incaricato alla sottoscrizione del presente atto ovvero in proprio, ai sensi dell'art. 6, D.P.C.M. 3.12.2013,

AFFIDA

ad InfoCert S.p.A, con sede legale in Roma, Piazza Sallustio 9, P. IVA 07945211006, il processo di conservazione di documenti informatici, secondo quanto previsto nelle Condizioni Generali di Contratto e nel presente documento, ad esclusione delle attività di riversamento dei documenti conservati da un supporto di memorizzazione ad un altro, che costituiscono un servizio a sé stante, effettuato dietro eventuale, espressa e separata richiesta. Sono inoltre escluse dalla responsabilità di InfoCert S.p.A. le attività che precedono l'invio dei documenti (ad es., la digitalizzazione dei documenti analogici, il rispetto dei tempi prescritti per l'invio in conservazione, l'idoneità del *software* realizzato dal Cliente/Produttore) ed il contenuto dei medesimi.

Data _____ Firma del Cliente/Produttore _____

1) La conservazione dei documenti informatici rilevanti a fini tributari, secondo le previsioni di cui al D.P.C.M. 3.12.2013, al D.M. Economia e Finanze del 17.06.2014, al D.Lgs. n. 52/2004 e ss. mm. ii., è assicurata mediante l'integrazione del Servizio reso da InfoCert S.p.A. con il Sistema di Gestione utilizzato dal Cliente/Produttore.

2) Ai fini della conservazione dei documenti analogici originali, il Cliente/Produttore dovrà provvedere autonomamente ad apporre la firma digitale ai documenti e, ove previsto, per particolari tipologie di documenti analogici originali unici, a far intervenire un pubblico ufficiale, che attesti la conformità tra il documento conservato e l'originale, ai sensi dell'art. 22, c. 4 e 5 del D. Lgs 7.03.2005, n. 82.

3) In base al presente atto di affidamento e ai sensi dell'art. 6, D.P.C.M. 3.12.2013, InfoCert S.p.A. opererà quale Responsabile del servizio di conservazione dei documenti informatici del Cliente/Produttore, provvedendo all'esecuzione dei compiti definiti nel provvedimento citato, secondo quanto previsto nelle Condizioni Generali di Contratto e nel Contratto ivi definito.

In particolare, InfoCert S.p.A. provvederà a:

- attestare il corretto svolgimento del processo di conservazione con l'apposizione di un firma elettronica qualificata di un proprio dipendente a ciò delegato;
- verificare la corretta funzionalità del sistema di conservazione e dei programmi utilizzati;
- predisporre le misure di sicurezza del sistema di conservazione, al fine di garantire la sua continua integrità;
- definire e documentare le procedure da rispettare per l'apposizione della marca temporale;
- verificare, con periodicità non superiore a cinque anni, che i documenti conservati siano leggibili, anche attraverso la verifica dell'integrità dei supporti utilizzati per la conservazione, adottando gli opportuni accorgimenti al fine di assicurare la leggibilità degli stessi.

Nomina ex D.Lgs. n. 196/2003

Ai sensi dell'art. 29 del D.Lgs. n. 196/2003, Codice in materia di protezione dei dati personali, il Cliente/Produttore, con la sottoscrizione del presente atto di affidamento, nomina InfoCert S.p.A. quale Responsabile dei trattamenti dei dati necessari all'esecuzione del Servizio.

In particolare, anche in considerazione del ruolo di responsabile del servizio di conservazione, così come previsto dall'art. 6, DPCM 3.12.2013 ovvero, ove applicabile, dalla Deliberazione CNIPA n. 11/2004, i compiti affidati alla InfoCert S.p.A. attengono a qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la selezione, l'estrazione, l'interconnessione, la comunicazione, la cancellazione e la distruzione di dati. InfoCert S.p.A., quale Responsabile del trattamento, applicherà le misure di sicurezza in base alle disposizioni legislative e regolamentari in vigore.

Come previsto dal Provvedimento del Garante per la protezione dei dati personali del 27.11.2008, modificato dal successivo provvedimento del 25.06.2009, nella veste di Responsabile del trattamento, InfoCert provvederà ad adempiere a tutte le prescrizioni relative alla selezione, nomina e verifica delle attività effettivamente svolte dagli amministratori di sistema, oltre a predisporre, mantenere aggiornati e conservare presso la propria sede gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite.

Informativa ai sensi dell'art. 13 del D.Lgs n. 196/2003

InfoCert S.p.A., in qualità di Titolare del trattamento dei dati forniti dal Cliente/Produttore informa lo stesso, ai sensi e per gli effetti di cui all'art. 13 del D.Lgs. n. 196/2003, che i predetti dati personali saranno trattati, con l'ausilio di archivi cartacei e di strumenti informatici e telematici idonei a garantire la massima sicurezza e riservatezza, per le finalità e con le modalità illustrate nell'Informativa sul trattamento dei dati personali disponibile nella pagina di documentazione sul Servizio presente sul sito *www.infocert.it*, di cui il Cliente dichiara di aver preso visione.

Consenso

Ai sensi del D.Lgs. 30.05.2003, n. 196, Codice in materia di protezione dei dati personali, il Cliente/Produttore dichiara di aver preso visione dell'informativa di cui sopra e, preso atto dell'utilizzo dei dati da parte di InfoCert S.p.A.,

☐ presta il consenso
☐ non presta il consenso

al trattamento dei dati personali indicati ai fini della corretta gestione ed erogazione del servizio da parte di InfoCert (consenso obbligatorio)

☐ presta il consenso
☐ non presta il consenso

al trattamento dei dati personali indicati a fini di vendita diretta di prodotti o servizi, a fini di *marketing*, promozione delle attività e presentazione delle iniziative InfoCert, con modalità di contatto automatizzate e tradizionali (consenso facoltativo)

☐presta il consenso
☐non presta il consenso

al trattamento dei dati personali sopra indicati a fini di vendita diretta di prodotti o servizi, a fini di *marketing*, promozione delle attività e presentazione delle iniziative di terzi, con i quali InfoCert abbia stipulato accordi commerciali, con modalità di contatto automatizzate e tradizionali (consenso facoltativo)

(Firma Cliente/Produttore)

_____

ATTESTAZIONE DI PUBBLICAZIONE

La presente deliberazione e' stata pubblicata in copia all Albo di questa Azienda Ospedaliera di Padova per 15 giorni consecutivi dal

Il Direttore
UOC AFFARI GENERALI E LEGALI
(Dott.ssa Caterina Dalla Zuanna)

CERTIFICAZIONE DI ESECUTIVITA'

La presente deliberazione e' divenuta esecutiva il 11/07/2016

Il Direttore
UOC AFFARI GENERALI E LEGALI
(Dott.ssa Caterina Dalla Zuanna)

Copia composta di n°58 fogli (incluso il presente) della delibera n. 735 del 11/07/2016 firmata digitalmente dal Commissario e conservata secondo la normativa vigente presso Infocert S.p.a.

Padova, li

Il Direttore
UOC AFFARI GENERALI E LEGALI
(Dott.ssa Caterina Dalla Zuanna)
