Manuale dei Processi di Conservazione Elettronica per lo Studio Odontoiatrico

Versione 0.1

Elite Computer Italia S.r.l.
Sede legale: Via Padova 209 - 20127 - Milano
Sede operativa: Via Achille Grandi 19-21-23, 20090 Vimodrone (MI)
Tel. +39 02/27.40.95.21 – Fax +39 02/27.40.91.50
P.Iva/C.F 11654690152 - Cap. sociale Euro 100.000,00 i.v.
REA MI-1485870 www.orisline.com - info@orisline.com

Indice

Elite Computer Italia S.r.l.
Sede legale: Via Padova 209 - 20127 - Milano
Sede operativa: Via Achille Grandi 19-21-23, 20090 Vimodrone (MI)
Tel. +39 02/27.40.95.21 – Fax +39 02/27.40.91.50
P.Iva/C.F 11654690152 - Cap. sociale Euro 100.000,00 i.v.
REA MI-1485870 www.orisline.com - info@orisline.com

Scopo e campo di applicazione del documento

Il presente documento è il "Manuale dei processi di formazione e conservazione elettronica" (di seguito anche "Manuale della Conservazione") dei documenti di uno Studio Dentistico di seguito evidenziati, redatto da Elite Computer Italia Srl (da qui in avanti, "ECI") ai sensi dell'articolo 62 del Manuale Di Gestione Dei Documenti ex art. 5 DPCM 31 ottobre 2000.

Il Manuale ha lo scopo di raccogliere le diverse normative in materia e di documentare il processo di conservazione della documentazione oggetto di conservazione sostitutiva da parte degli Studi Dentistici. Inoltre, descrive tutte le procedure e le prassi seguite da ECI, in qualità di Responsabile della Conservazione e del trattamento dei dati personali, relativamente sia alla gestione sia alla sicurezza del servizio, dei documenti e delle informazioni trattate.

In particolare, 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 di Elite, e di conseguenza dello Studio Dentistico, al rispetto delle norme.

Il Manuale è organizzato per sezioni:

1. la prima sezione (capitoli 2-4) fornisce i profili e i riferimenti degli attori coinvolti, contiene una panoramica di tutte le leggi e i decreti che regolano la materia e introduce i documenti trattati con il loro ciclo di vita;
2. la seconda sezione (capitoli 5-6) descrive i sistemi utilizzati sia per la creazione e la gestione dei documenti sia per la loro conservazione (in modalità ASP presso il Data Center del partner tecnologico);
3. la terza sezione (capitoli 7-9) contiene il dettaglio del processo di conservazione, posto sotto la responsabilità di ECI, delle procedure di ricerca e di esibizione a norma dei documenti conservati e delle modalità per la loro modifica e cancellazione logica;
4. l'ultima sezione (capitoli 10-11) riporta infine le misure fisiche e logiche di sicurezza adottate e gli allegati che si è ritenuto opportuno rendere disponibili.

Principi di redazione

La redazione del presente Manuale della Conservazione 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.

Termini e definizioni

Termine	Definizione
Archiviazione	E' il processo di trattamento e gestione dei documenti di uso corrente e/o nel medio lungo periodo e costituisce il passo propedeutico alla conservazione, per il quale non sono previsti particolari obblighi di legge.
Application Service Provider	E' un modello architetturale per l'erogazione di servizi informatici che prevede che la tecnologia di elaborazione (hardware) e quella applicativa (software) vengono gestite centralmente da un Service Provider lasciando all'utente finale la scelta dei tempi e dei modi di fruizione del servizio.
Conservazione sostitutiva	Vedi conservazione.
Conservazione	Il processo che consente di conservare i documenti in modalità informatica a norma di legge e che risponde a quanto stabilito nella deliberazione CNIPA 11 del 19 febbraio 2004.
Documento analogico originale	Documento analogico che può essere unico oppure non unico se, in questo secondo caso, sia possibile risalire al suo contenuto attraverso altre scritture o documenti di cui sia obbligatoria la conservazione, anche se in possesso di terzi.
Documento informatico	E' la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Documento statico non modificabile	E' un documento informatico redatto in modo tale per cui il contenuto risulti non alterabile durante le fasi di accesso e di conservazione nonché immutabile nel tempo (non modificabilità) e non contenga macroistruzioni o codice eseguibile in grado di attivare funzionalità che ne possano modificare gli atti, i fatti o i dati nello stesso rappresentati (staticità).
Dati sensibili	Ai sensi dell'articolo 4, comma 1, lettera d) del Decreto Legislativo 30 giugno 2003 n. 196, sono 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 o organizzazioni a carattere filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

Termine	Definizione
Evidenza informatica	E' una sequenza di simboli binari (bit) che può essere elaborata da una procedura informatica (art. 1 comma 1 lettera r della Deliberazione CNIPA 11 del 19 febbraio 2004).
Extensible Markup Language	E' un linguaggio derivato dallo SGML (Standard Generalized Markup Language) - metalinguaggio che permette di creare altri linguaggi – che, a differenza del HTML, istanza specifica dell'SGML, costituisce a sua volta un metalinguaggio (più semplice dello SGML) largamente utilizzato per la descrizione di documenti sul Web. In particolare, l'XML viene utilizzato per definire le strutture dei dati invece che per descrivere come questi ultimi devono essere presentati, strutture che vengono definite utilizzando degli specifici marcatori (markup tag). Inoltre, diversamente dal HTML, l'XML consente all'utente di definire marcatori personalizzati e gli attributi dei singoli marcatori, dandogli il controllo completo sulla struttura di un documento.
Firma digitale	E' 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 del Decreto Legislativo del 7 marzo 2005 n. 82).
Firma elettronica	E' 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 del Decreto Legislativo del 7 marzo 2005 n. 82).
Firma elettronica qualificata	E' 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 del Decreto Legislativo del 7 marzo 2005 n. 82).
Firma elettronica avanzata	E' l'insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che: a) consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario; b) sono creati con mezzi sui quali il firmatario può conservare un controllo esclusivo; c) sono 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 del Decreto Legislativo del 7 marzo 2005 n. 82).

Termine	Definizione
Hardware security module	E' un dispositivo crittografico ad alte prestazioni utilizzato per apporre automaticamente la firma digitale e la validazione temporale a elevati volumi di documenti informatici.
Impronta di una sequenza di simboli binari (o hash)	E' la sequenza dei simboli binari (bit) di lunghezza predefinita generata mediante l'applicazione alla prima di una opportuna funzione di hash (art. 1 comma 1 lettera s della Deliberazione CNIPA 11 del 19 febbraio 2004).
Lotto di documenti	Costituisce l'insieme di documenti raggruppati secondo un criterio di aggregazione, aventi un file indice (file di chiusura del lotto) che attesta la conservazione con l'apposizione della firma del Responsabile della Conservazione e della marca temporale.
Marca temporale	E' il riferimento temporale, opponibile a terzi, che consente la validazione temporale, così come definita all'art. 1 comma 1 lettera i) DPCM del 30 marzo 2009.
PKCS #12	E' lo standard definito per lo scambio di informazioni personali combinando in un solo file protetto (con estensione .p12) la chiave privata e il certificato pubblico di un documento.
Portable Document Format	E' il formato di file creato da Adobe Systems nel 1993 per lo scambio di documenti. In particolare, 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. Inoltre, il PDF è uno standard aperto e 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	E' un sistema di posta elettronica nel quale è fornita al mittente documentazione elettronica attestante l'invio e la consegna di documenti informatici.
Responsabile della conservazione	E' il soggetto cui sono attribuite funzioni, adempimenti, attività e responsabilità relative al processo di conservazione ottica sostitutiva conformemente a quanto previsto all'art. 5 della Deliberazione Cnipa 11 del 19 febbraio 2004.
Riferimento temporale	E' un'informazione, contenente la data e l'ora, associata a uno o più documenti informatici, così come definito all'art. 1 comma 1 lettera m del DPCM del 30 marzo 2009.

Termine	Definizione
Web Services	E' un meccanismo software nato per supportare l'interoperabilità tra diverse applicazioni che operano sulla stessa rete. Caratteristica fondamentale di un Web Service è offrire un'interfaccia software a cui un'applicazione remota accede inviando a una specifica URL dei messaggi (basati su protocollo SOAP) formattati secondo lo standard XML.

Acronimi

Acronimo	Spiegazione
CA	Certification Authority
ASP	Application Service Provider
AID	Agenzia per l'Italia Digitale (ex Cnipa, ex Digit PA)
D.LGS	Decreto Legislativo
DPCM	Decreto del Presidente del Consiglio dei Ministri
GU	Gazzetta Ufficiale della Repubblica Italiana
HTTP	HyperText Transfer Protocol
HSM	Hardware Security Module
PDF	Portable Document Format
PEC	Posta Elettronica Certificata
PKCS	Public-Key Cryptography Standards
SOAP	Simple Object Access Protocol
SSL	Secure Socket Layer
TSA	Time Stamping Authority
TSS	Time Stamping Service
TU	Testo Unico
URL	Uniform Resource Locator
XML	Extensible Markup Language
FEA	Firma Elettronica Avanzata

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, gestione e conservazione del fascicolo tecnico, quale insieme di documenti oggetto di conservazione sostitutiva.

Studio Dentistico

Lo Studio Dentistico, nella pratica sia medica che amministrativa quotidiana, si trova a gestire una ingente mole di documenti obbligatori (di seguito meglio evidenziati), la cui conservazione fisica in un archivio cartaceo si presta a incombenze e problematiche di varia natura: costi di gestione, di conservazione, rischio di perdita del dato, ecc.. Il periodo di conservazione obbligatoria di tali documenti cartacei è variabile e arriva a una conservazione a tempo indeterminato per talune fattispecie (ad esempio dati clinici). Spesso anche l'archivio informatico (classico salvataggio dati sul proprio personal computer) non pone al sicuro la documentazione. Per ridurre i costi e i disagi riferiti a tale archivio, il servizio descritto in questo Manuale permette allo Studio Dentistico di creare la specifica documentazione obbligatoria per legge, in formato nativo digitale, grazie a una combinazione di firme elettroniche del paziente e/o dell'operatore sanitario e/o del soggetto giuridico di competenza, e di inviare tale documentazione via web in modalità protetta a un server esterno tramite il quale avverrà il processo di conservazione sostitutiva e di esibizione a norma.

La documentazione dello Studio pertanto sarà archiviata a norma di legge per tutto il tempo necessario, sarà ordinata per indici, sarà soggetta a back-up costanti e a misure di sicurezza e di aggiornamento informatico e sarà immediatamente consultabile in qualsiasi momento sia dallo Studio stesso sia dagli organi pubblici deputati al controllo di questo tipo di documentazione.

A tale scopo, mentre spetterà allo Studio Dentistico creare e gestire localmente la documentazione, l'intero processo di conservazione viene esternalizzato a ECI a cui, per competenza ed esperienza, saranno affidati il ruolo sia di Responsabile della Conservazione sia di Responsabile del trattamento dei dati personali, ai fini esclusivi della specifica documentazione sottoposta a conservazione e contrattualizzata fra le parti.

Elite Computer Italia (gruppo Orisline)

ECI nasce con l'obiettivo di condurre a termine un progetto di ampio respiro teso alla fornitura di specifici servizi informatici a tutti gli operatori del settore dentale e alle aziende di medie dimensioni. Dopo i primi anni rivolti principalmente allo sviluppo di soluzioni software d'avanguardia nei settori dell'odontotecnica e dell'odontoiatria e di soluzioni di outsourcing per le aziende pubbliche e private, dal 1994 Elite Computer Italia ha iniziato a diversificare maggiormente la gamma di prodotti offerti e oggi ha diverse linee di software utilizzate in oltre quindici Paesi da oltre undicimila utenti.

Denominazione sociale	**Elite Computer Italia Srl**
Sede Legale:	Via Padova, 209 – 20127 Milano Tel. +39.02.27409521 - Fax +39.02.26511579
Sito web:	http://www.orisline.com
e-mail	info@orisline.com
PEC	elitecomputer@orispec.it
Codice fiscale/Partita IVA	11654690152
Numero REA	MI-1485870

Ad ECI viene esternalizzata la gestione dell'intero processo di conservazione sostitutiva, incluso i ruoli di Responsabile della Conservazione e di Responsabile del trattamento dei dati personali attraverso un contratto di appalto di servizi del quale il presente Manuale è parte integrante.

Ciò significa che i compiti affidati a ECI attengono a qualunque operazione o complesso di operazioni, eseguiti eventualmente 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 dei dati oggetto di conservazione, e, non ultimo, il loro trattamento secondo quanto stabilito dal D.Lgs n. 196/2003 in materia di protezione dei dati personali.

Data Center

ECI, avvalendosi della facoltà prevista dalla Deliberazione CNIPA 11/2004, articolo 5, commi 2 e 3, ha a sua volta affidato lo svolgimento delle attività di conservazione, con l'esclusione di quelle di firma dei lotti, a un Data Center che, per competenza ed esperienza, ne garantisce la corretta esecuzione così come definito dalle norme vigenti.

L'introduzione di un Data Center che, in modalità ASP, sia di supporto all'intero processo di conservazione sostitutiva, massimizza l'affidabilità del servizio offerto da ECI garantendo non solo l'archiviazione in sicurezza dei documenti conservati, ma anche la loro leggibilità nonché la tracciatura delle esibizioni effettuate (quale ulteriore prova di leggibilità).

All'interno del Data Center, lo svolgimento delle attività di conservazione è affidato a una o più persone che, per competenza ed esperienza, garantiscono la corretta esecuzione di tutti i processi e procedure di conservazione secondo quanto previsto dalle norme e nella documentazione interna di organizzazione e gestione del servizio di conservazione.

E' inoltre presente una struttura di Service Desk la quale, composta da team specializzati su tutti gli ambiti tecnologici (sistemi di base e storage, network, middleware e database) e munita di console operativa per

monitorare tutte le informazioni raccolte dagli agenti software, agisce come SPOC (Single Point Of Contact) per problemi relativi all'erogazione dei servizi.

Fondamenti normativi

Le realtà aziendali e di Pubblica Amministrazione avvertono in maniera sempre crescente la necessità di ottenere e gestire informazioni corrette, tempestive, aggiornate, autentiche, integre, logicamente accessibili, protette e disponibili nel tempo. Riuscire a garantire queste caratteristiche permette al management di rispondere in maniera adeguata alle richieste aziendali interne o esterne e di trasformarle in un reale vantaggio competitivo.

Al crescere dei volumi della documentazione prodotta, il costo per archiviare e conservare nel tempo le informazioni in modo organizzato è ingente e può creare inutili processi di burocratizzazione. Per questi motivi una ben organizzata adozione del documento digitale consente di ridurre i costi e supportare efficacemente l'attività aziendale.

E' stato così introdotto il processo di conservazione sostitutiva col fine ultimo di rendere un documento inalterabile e immodificabile, in modo che possa essere disponibile nel tempo nella propria autenticità e integrità.

Il quadro normativo

Il contesto normativo in cui si inquadra la conservazione sostitutiva risale al 1994, ma è solo dall'anno 2004 che interventi più significativi hanno reso possibile la conservazione dei documenti in formato digitale valevole anche ai fini fiscali. Senza ripercorrere in dettaglio tutto l'excursus legislativo, se ne fornisce di seguito una panoramica per una più agevole comprensione dell'intero quadro normativo.

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 a 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 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.

Infine, il Codice è stato recentemente rivisto dal D.Lgs. n. 235 del 30 dicembre 2010 e dall'emissione delle Regole Tecniche ad esso relative (pubblicazione Gazzetta Ufficiale maggio 2013), allo scopo di rendere il quadro normativo più coerente alle innovazioni tecnologiche occorse negli ultimi anni.

Elementi in ambito conservazione sostitutiva

L'implementazione e la gestione dei processi di creazione e conservazione dei documenti elettronici sono operazioni che si avvalgono di numerosi strumenti ed elementi regolati da apposite discipline che vanno raccordate alla disciplina generale della conservazione.

In particolare, la norma fa riferimento agli strumenti e agli elementi qui di seguito riportati.

- ***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 richiede strumenti di validazione 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***: 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 e 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 e non ripudiabilità.
- ***Firma elettronica avanzata***: insieme di dati in forma elettronica, allegati oppure connessi ad un documenti 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.
- ***Attestazione temporale***: per stabilire il momento 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.

Allo scopo di chiarire ulteriormente la distinzione tra documenti cartacei e informatici (o elettronici), viene di seguito riportata una tabella sintetica che ne evidenzia le modalità di emissione e la loro conservabilità in modalità sostitutiva.

Tipologia	*Emissione*	*Conservabile in modalità sostitutiva*
Documento cartaceo "non unico"	Cartacea	Sì
Documento cartaceo "unico"	Cartacea	Sì, con l'intervento del Pubblico Ufficiale
Documento elettronico semplice	Nessuna condizione (la sua validità è sottoposta alla valutazione del giudice)	Sì
Documento elettronico con valenza di "forma scritta"	Documento "statico" con firma elettronica qualificata o firma digitale	Sì

Principali riferimenti normativi

Per completezza, viene qui di seguito presentato l'elenco dei principali riferimenti normativi su cui si basa il processo di conservazione sostitutiva e, di conseguenza, l'intero servizio Oris Paperless.

1. *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.
2. *Decreto Legislativo 30 giugno 2003, n. 196 e successive modifiche* – Codice in materia di Protezione dei Dati Personali.
3. *Decreto del 23 gennaio 2004 del Ministero dell'Economia e delle Finanze* – Modalità di assolvimento degli obblighi fiscali relativi ai documenti informatici e alla loro riproduzione in diversi tipi di supporto.
4. *Deliberazione CNIPA n. 11 del 19 febbraio 2004* – Regole tecniche per la riproduzione e conservazione su supporto ottico idoneo a garantire la conformità dei documenti agli originali.
5. *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.

6. *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.
7. *Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009* – Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
8. *Decreto Legislativo del 30 dicembre 2010* – Modifiche e 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; Norme Tecniche (maggio 2013).

La deliberazione CNIPA n. 11 del 19 febbraio 2004

La deliberazione CNIPA 11/2004 detta le regole valevoli, in generale, per le procedure per la riproduzione e conservazione dei documenti su supporto idoneo a garantire la conformità dei documenti agli originali.

La deliberazione, che sostituisce integralmente la precedente numero 42 del 2001, aggiorna le regole tecniche per la riproduzione e conservazione dei documenti su supporto ottico idoneo a garantire la conformità dei documenti agli originali, come previsto all'articolo 6, commi 1 e 2, del TU delle disposizioni legislative e regolamentari in materia di documentazione amministrativa di cui al DPR 28 dicembre 2000, n. 445.

Il provvedimento ridefinisce il quadro normativo di riferimento, mutato grazie al progresso tecnologico, adattandolo alle nuove situazioni.

Il Responsabile della Conservazione

Come già per la deliberazione AIPA n. 42/2001, la deliberazione CNIPA n. 11/2004 (art. 5) enfatizza 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.

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

Più in particolare dovrà provvedere a:

1. definire le caratteristiche e i requisiti del sistema di conservazione in funzione della tipologia dei documenti (analogici o informatici) da conservare;
2. organizzare conseguentemente il contenuto dei supporti ottici e gestire le procedure di sicurezza e di tracciabilità che ne garantiscono la corretta conservazione, anche al fine di consentire l'esibizione di ciascun documento conservato;
3. archiviare e rendere disponibili, con l'impiego di procedure elaborative e relativamente ad ogni supporto di memorizzazione utilizzato:
   - la descrizione del contenuto dell'insieme dei documenti;
   - gli estremi identificativi del Responsabile della Conservazione;
   - gli estremi identificativi delle persone eventualmente delegate dal Responsabile della Conservazione, con l'indicazione dei compiti alle stesse assegnati;
   - l'indicazione delle copie di sicurezza.
4. mantenere e rendere accessibile un archivio dei programmi in gestione nelle eventuali diverse versioni;
5. verificare la corretta funzionalità del sistema e dei programmi in gestione;
6. adottare le misure necessarie per la sicurezza fisica e logica del sistema preposto al processo di conservazione sostitutiva e delle copie di sicurezza dei supporti di memorizzazione;
7. richiedere la presenza di un pubblico ufficiale nei casi in cui sia previsto il suo intervento, assicurando allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività attribuitegli;
8. definire e documentare le procedure da rispettare per l'apposizione del riferimento temporale;
9. verificare periodicamente, con cadenza non superiore a cinque anni, l'effettiva leggibilità dei documenti conservati provvedendo, se necessario, al riversamento diretto o sostitutivo del contenuto dei supporti.

Al Responsabile della Conservazione sono attribuiti compiti cruciali in ragione del controllo e della supervisione che egli attua sull'intero procedimento di conservazione sostitutiva.

Gli adempimenti comprendono non solo attività di pianificazione, ma anche attività di tipo operativo/esecutivo, che può essere necessario svolgere in sedi diverse e magari distanti tra di loro. L'utilizzo degli strumenti telematici, infatti, consente di memorizzare documenti e scritture contabili con estrema facilità e a costi minori in sedi accentrate specializzate.

La deliberazione CNIPA 11/2004 ai commi 2 e 3 dell’art. 5 consente 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 a osservare le disposizioni contenute nella deliberazione stessa.

Parere legale / Aderenza di Oris Paperless alla normativa

Ai fini della valenza legale del procedimento, assume rilevanza il parere pro-veritate emesso dallo Studio Legale Finocchiaro, eccellenza nazionale in materia, in data 27/01/14. In estrema sintesi, da tale parere si evince che "**il sistema tecnologico di firma c.d. grafometrica che Elite Computer Italia Srl intende introdurre pare soddisfare i requisiti di cui all'art. 56 delle regole tecniche**" (Considerazioni conclusive, pag. 18).

Nello specifico, per quanto concerne l'aderenza di Oris Paperless alla normativa (e principalmente, alla data attuale, ai requisiti di cui agli articoli 56 e 57 delle Regole Tecniche del CAD del 22/02/13):

Lo stesso parere pro-veritate specifica inoltre quanto segue: "*Occorre tuttavia precisare che* ***alcuni dei requisiti citati dalle regole tecniche non possono essere soddisfatti da un sistema tecnologico di firma, per quanto sicuro, ma soltanto dall'organizzazione del soggetto che tale sistema adotta*** *(cioè ad esempio dallo Studio Odontoiatrico).*" (pag. 18). E' pertanto fondamentale che lo Studio Odontoiatrico si attenga scrupolosamente alla procedura tecnico-normativa in materia per evitare di inficiare in tutto o parte il delicato processo di firma e di conservazione. Si rimanda in tal senso al Manuale Operativo contenente gli obblighi di processo che lo Studio Odontoiatrico deve obbligatoriamente soddisfare e rispettare, sia ai fini contrattuali nei confronti di ECI, sia ai fini legali per il rispetto della normativa.

In linea generale, allo stato attuale tutte le leggi in materia confermano la correttezza del processo di Oris Paperless, e nessuna legge in materia vieta il processo di Oris Paperless, nella sua totalità e/o per specifiche parti di esso.

Cadenza di conservazione consigliata per l'utente.

La conservazione sostitutiva su supporto informatico, accompagnata da firma digitale, risponde pienamente ai requisiti della forma scritta ed equivale pertanto alla tradizionale conservazione in via cartacea, in ossequio al D. Lgs. 46/97. La firma digitale e/o la firma grafometrica sono in grado di collegare con certezza e univocamente i documenti prodotti e conservati al/ai responsabili e/o firmatari degli stessi.

La tempistica di invio in conservazione è ovviamente libera per l'utente, che quindi deve decidere in autonomia quando effettuarla, tramite apposita funzione di Orisdent. Ma, considerando una cadenza minima annuale dalla data di creazione del documento, incrociata ad una eventuale scadenza della firma digitale apposta dall'operatore (scadenza che renderebbe impossibile assegnare una data certa alla firma), **si consiglia allo Studio Odontoiatrico di inviare in conservazione i documenti firmati con cadenza almeno settimanale, al fine di evitare la possibile decadenza del valore legale degli stessi**. Difatti, se non viene chiuso il lotto e quindi se non viene apposta la marca temporale e la firma digitale del Responsabile della Conservazione, il processo non ha pieno valore legale. In tal senso, Oris Paperless prevede un preciso vincolo temporale: non viene consentita la firma di un documento entro sei mesi dalla scadenza del certificato di firma digitale dell'operatore eventualmente utilizzato. In tal modo si obbliga l'operatore a

richiedere l'intervento di un altro operatore dotato di token di firma regolare, o di richiedere un nuovo token di firma prima di poter procedere.

Le tipologie documentali trattate

Sulla base dei pareri sopra riportati e della normativa vigente, Oris Paperless prevede la dematerializzazione e la conservazione sostitutiva dei documenti indicati nell'Allegato 1 costituente parte integrante del presente Manuale, la cui versione aggiornata può essere scaricata in qualsiasi momento dal sito www.orisline.com.

Specifiche.

Per le specifiche legali e tecniche di cui ai documenti sopra menzionati, si rimanda alla specifica normativa in materia; per la gestione documentale, informatica e normativa degli stessi effettuata da Oris Paperless, si rimanda al Manuale Operativo, al parere legale pro-veritate sopra menzionato, e alla relazione finale di progetto della Fondazione Politecnico di Milano (ultima stesura aggiornata 19/07/13).

Ciclo di vita dei documenti

Allo scopo di inquadrare l'intero ciclo di vita dei documenti oggetto di conservazione, viene di seguito presentato sinteticamente l'intero ciclo di vita del documento, dal momento della sua creazione fino alla sua conservazione e custodia, mostrandone i responsabili e gli applicativi utilizzati.

Fase / Attività	***Soggetti incaricati***	***Afferenza / Applicativi***	***Descrizione***
Redazione	Studio Dentistico	Orisdent	Un utente abilitato può iniziare la creazione di un nuovo documento. Il documento è creato in formato PDF/A.
Memorizzazione e indicizzazione	Studio Dentistico	Orisdent	Il software gestionale Orisdent memorizza (solo) localmente e indicizza i documenti PDF/A.
Firma Elettronica Avanzata del Paziente	Paziente dello Studio	Oris Paperless	Il modulo Oris Paperless acquisisce la firma grafometrica del paziente, gestendola e memorizzandola a norma sia informaticamente che legalmente.

Fase / Attività	*Soggetti incaricati*	*Afferenza / Applicativi*	*Descrizione*
Apposizione certificato di firma aziendale	ECI	Oris Paperless	Alcuni fornitori di firma grafometrica possono richiedere, per proprie esigenze tecniche ininfluenti ai fini del processo, l'apposizione di un ulteriore certificato di firma aziendale, sul documento firmato grafometricamente. Se presente, trattasi di operazione ridondante, non obbligatoria, che rafforza ulteriormente il processo ma non ne inficia in alcun modo lo svolgimento.
Firma digitale	Studio Dentistico	Oris Paperless	Il documento viene firmato digitalmente da utente abilitato (operatore sanitario e/o amministrativo), conferendo valore legale e inalterabilità nel tempo. A seconda dei casi, il documento può o deve essere stampato su carta, e fornito in copia al paziente.
Invio in conservazione	Studio Dentistico	Oris Paperless	Il documento, correttamente firmato elettronicamente sia dal paziente sia, se necessario, dall'operatore di Studio, viene inviato via internet dal client locale di Orisdent allo spazio di conservazione online del Data Center. Se l'operazione va a buon fine, il file viene marchiato come "stato firmato e spedito" e viene fisicamente cancellato in locale; per talune categorie documentali (es. l'anamnesi) il documento elettronico nativo, privo di firme, è sempre visualizzabile nel database locale di Orisdent.
Elaborazione, chiusura e firma digitale del lotto	Data Center	Oris Paperless	Il documento informatico, insieme al suo file di controllo firmato elettronicamente, viene inserito nel lotto il quale viene chiuso al verificarsi di determinate casistiche, o in modo forzato dall'utente autorizzato dello Studio.

Fase / Attività	*Soggetti incaricati*	*Afferenza / Applicativi*	*Descrizione*
Completamento del processo di conservazione	Data Center	Oris Paperless	Il sistema di conservazione memorizza presso il Data Center il lotto firmato digitalmente e ne effettua le copie di sicurezza.
Ricerca ed esibizione	Studio Dentistico	Oris Paperless	L'utente può in qualsiasi momento e tramite il software Orisdent accedere a tutti i documenti firmati e inviati in conservazione, richiedendoli via Internet e visualizzandoli attraverso il proprio viewer; di tali documenti è possibile effettuare una stampa cartacea. In caso di crash del sistema locale, vengono applicati dei protocolli di sicurezza che garantiscono comunque l'accesso ai documenti, come più ampiamente riportato nel capitolo relativo alle misure di sicurezza.
Rettifica e cancellazione	Studio Dentistico	Oris Paperless	E' possibile inviare in conservazione un nuovo documento che ne rettifica uno già conservato a norma (che a sua volta rimane conservato con un diverso stato). Non è invece possibile effettuare la cancellazione fisica del documento conservato nel Data Center, a meno che non venga chiuso il rapporto tra ECI e lo Studio Dentistico, nel qual caso è facoltà di quest'ultimo chiedere copia di backup dei propri dati.

Il sistema Orisdent di creazione e gestione dei documenti

Orisdent è il programma di ECI per la gestione dello Studio Dentistico, nato dall'esperienza maturata in vent'anni di attività nel settore e divenuto leader di mercato grazie anche ai suggerimenti pervenuti dagli utenti rendendolo sempre più aderente a quelle che sono le reali esigenze di tutti gli operatori di odontoiatria italiani ed internazionali.

Rinviando al sito Internet http://www.orisline.com ogni ulteriore dettaglio, vengono di seguito brevemente descritte le principali funzionalità di Orisdent; si rimanda al manuale per eventuali approfondimenti.

Funzionalità	***Descrizione***
Pazienti	E' il cuore di Orisdent. Consente di gestire Anagrafiche, Cartelle Cliniche, Preventivi, Richiami, Foto/Immagini, Bilancio Pazienti, Diario Clinico, Gestione Testi.
Agenda	Suddiviso in Giornaliera, Settimanale, Mensile, Liste di Controllo, Volume di lavoro, Configura Agenda, Elenco Appuntamenti.
Studio	Suddiviso in Dati Studio, Operatori, Listini/Convenzioni, Compensi, Configura, Documenti, Backup, Statistiche.
Magazzino	Suddiviso in: Fornitori, Magazzino, Scadenze Prodotti, Movimenti, Fatture d'acquisto, Farmaci/Esami.
Contabilità	Suddiviso in: Banche/Casse, Prima nota, Gestione convenzioni, Sospesi di pagamento, Previsioni Entrate, Clienti, Fatturazione, Scadenziario.
Storico	Suddiviso in: Archivio Storico, Archivio Operatori, Archivio Listini.

Segue nei paragrafi seguenti una descrizione di alcune caratteristiche di dettaglio che si ritiene utile mettere in evidenza a fini della trasparenza e dell'accuratezza con cui viene descritto in questo Manuale l'intero processo di conservazione sostitutiva.

Requisiti tecnici minimi del software

Oris Paperless è un modulo software del programma gestionale Orisdent, entrambi installati localmente sui PC dello Studio Dentistico muniti di sistema operativo Windows XP / Vista / 7 con almeno 1024 MB di RAM, 800 MB di spazio su disco fisso, processore Intel Pentium IV 3 GHz e una risoluzione video 1024x768.

Per il corretto funzionamento di Oris Paperless sono requisiti obbligatori, fra gli altri, sia la presenza di una licenza di Orisdent installata sul PC locale, coperta da regolare contratto di assistenza, sia l'esistenza di un collegamento a internet attivo.

Indicizzazione dei documenti

L'indicizzazione dei documenti ai fini della conservazione (vedi il capitolo che ne descrive il processo) viene garantita dalle funzionalità messe a disposizione dal sistema di creazione e gestione dei documenti di Orisdent.

Controlli e gestione di eventuali anomalie

Ai sensi di legge, lo Studio Dentistico ed ECI, quale titolare del servizio di gestione documentale in uso, assicurano che i documenti inviati in conservazione sono statici e non modificabili, ovvero redatti senza macroistruzioni e codici eseguibili e in modo tale per cui il contenuto rimane immutabile nel tempo e, come tale, non possa essere alterato durante le fasi di conservazione ed esibizione (si veda il capitolo relativo al processo di rettifica e cancellazione).

In particolare la loro staticità è garantita dal formato PDF/A (standard ISO) mentre la loro non modificabilità è garantita dal fatto che gli stessi vengono firmati digitalmente prima di essere inviati in conservazione.

Formato dei documenti elettronici

La Deliberazione CNIPA numero 11/2004 non elenca 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.

Ad ogni modo il modulo Oris Paperless utilizza come formato dei documenti lo standard ISO PDF/A, rendendo così possibile la loro lettura nel tempo indipendentemente dall'evoluzione del formato PDF (e riducendo così la necessità di introdurre e applicare procedure di riversamento) e garantendone la loro staticità come già detto in precedenza e come richiesto dalla norma.

Oris Paperless comprende come funzione integrante un servizio di conservazione sostitutiva, oggetto del presente Manuale, che ECI rende disponibile per soddisfare le esigenze degli Studi Dentistici mantenendo e garantendo nel tempo l'integrità e la validità legale dei documenti, nel rispetto della normativa vigente.

Oris Paperless in tal senso consente di:

- conservare a norma di legge, per tutta la durata prevista dal contratto, i documenti in formato digitale statico non modificabile;

- visualizzare un documento conservato (*esibizione a norma*) richiamandolo via web dall'archivio del Data Center e fornendo le garanzie per la sua opponibilità a terzi (file di ricevuta e file di controllo del documento);
- rettificare un documento inviandone la versione modificata in conservazione senza però cancellare dall'archivio del Data Center il documento originario (quindi effettuando solo una "modifica logica"), nel pieno rispetto del principio di tracciabilità del documento;
- cancellare logicamente un documento conservato, allegando eventualmente la motivazione della cancellazione, mantenendo la sua copia fisica all'interno dell'archivio del Data Center e tracciandone adeguatamente la richiesta.

Oris Paperless integra pertanto il sistema di gestione documentale di Orisdent già in uso dallo Studio, e ne estende i servizi con funzionalità di firma digitale, firma elettronica avanzata e di conservazione a norma (solamente per i documenti che lo Studio decide di conservare e che sono compresi nell'elenco documentale che costituisce l'Allegato 1 del presente Manuale), organizzandone i supporti di memorizzazione e gestendo le fasi di raccolta, archiviazione ed esibizione nonché le procedure di sicurezza e di tracciabilità.

Il sistema supporta pertanto il Responsabile della Conservazione attraverso uno specifico cruscotto di monitoraggio (esportabile su foglio elettronico):

- nella supervisione delle informazioni relative a ogni supporto di memorizzazione utilizzato;
- nel controllo dell'effettiva leggibilità dei documenti conservati;
- nella tracciatura delle esibizioni effettuate, considerate un'ulteriore prova di leggibilità;
- nella verifica sull'utilizzo del servizio;
- nell'analisi delle quantità e dei volumi di informazioni movimentate specificandone il periodo e il livello di aggregazione.

Definizione di documento in Oris Paperless

In Oris Paperless il documento rappresenta l'unità minima di elaborazione, nel senso che viene memorizzato ed esibito come un tutt'uno senza la possibilità di estrarne solo una parte. In particolare, un documento conservato presso il sistema Oris Paperless, ha le seguenti caratteristiche:

- è costituito da uno o più file digitali, anche di diverse tipologie;
- è memorizzato sui supporti previsti dalla procedura di conservazione;
- è identificato in maniera univoca attraverso Oris Paperless;
- 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, firmati digitalmente dallo Studio Dentistico e inviati in conservazione, vengono archiviati presso il Data Center e resi disponibili per l'esibizione (e visualizzabili attraverso i viewer di Orisdent) ogni volta che lo Studio ne faccia esplicita richiesta.

Architettura e modalità di erogazione

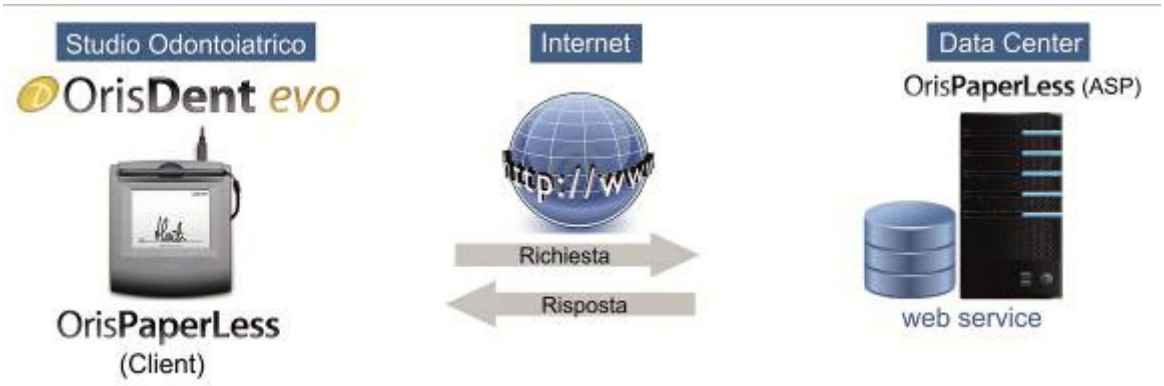
Il servizio di conservazione sostitutiva Oris Paperless si compone di un'applicazione software sviluppata a tale scopo e da una serie di servizi di interesse generalizzato condivisi con altre applicazioni (marca temporale, HSM, supporti di conservazione, viewer, ecc.).

Oris Paperless opera sia in locale sia in modalità ASP, e implementa le pre-esistenti funzioni di creazione e gestione documentale delle classi documentali ammesse, aggiungendo le fondamentali funzionalità di firma digitale, firma elettronica avanzata, conservazione sostitutiva ed esibizione a norma, in un processo del tutto integrato, atomizzato ove necessario, ed ergonomico per l'utente.

Parte dell'architettura del sistema Oris Paperless è di tipo distribuito, nel senso che i diversi servizi disponibili nel Data Center sono accessibili via web (sia per l'invio sia per l'esibizione dei documenti conservati) attraverso i diversi client installati localmente presso gli specifici Studi e integrati nel software Orisdent.

Tecnicamente l'accesso viene effettuato da un'applicazione (client) installata localmente sul PC dello Studio Dentistico e integrata con Orisdent che interagisce col Data Center accedendo via Internet (protocollo HTTP) ai web services disponibili remotamente ad una specifica URL di rete. L'invocazione dei web services deve avvenire dall'applicazione client (il cui database è criptato), fornendo apposite credenziali d'accesso e un certificato per l'autenticazione del servizio; il flusso dei dati avviene in modalità Soap.

La figura sottostante offre uno schema esemplificativo del dialogo tra l'applicazione presso lo Studio Dentistico e il Data Center, evidenziando l'integrazione con il software Orisdent.



In particolare, il Data Center è stato progettato seguendo alcuni principi fondamentali che permettono di erogare, con elevati standard di disponibilità e sicurezza i servizi di business:

- ampia adozione di tecnologie hardware contraddistinte da una scalabilità orizzontale (blade server) che permettono di contenere i consumi energetici senza alcuna penalizzazione prestazionale;
- ampia adozione di tecnologie di virtualizzazione contraddistinte da elevati standard di disponibilità dei sistemi, flessibilità in termini di gestione e costi scalabili (dimensionamento dei server virtuali allineate alle necessità del business).

I seguenti paragrafi descrivono brevemente i servizi condivisi o condivisibili con altre applicazioni e integrati nel modulo software Oris Paperless.

Marca temporale

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

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.

Firme elettroniche

La firma grafometrica (FEA) apposta dal paziente avviene su specifico hardware (tablet/tavoletta ottica e penna), e viene acquisita tramite software di firma grafometrica sviluppato e fornito da primari fornitori nazionali ed internazionali (vedasi documentazione di prodotto già citata per i dettagli). La firma digitale apposta dallo Studio Dentistico sui documenti firmati grafometricamente dal paziente, avviene attraverso l'utilizzo di una chiavetta USB a uso strettamente personale dell'utente o degli utenti dello Studio autorizzato/i alla firma, a seconda dei vari tipi di processo individuati. In tali casi, fra lo step di firma grafometrica del paziente e lo step di firma digitale dello Studio, potrebbe esserci l'apposizione di un certificato di firma aziendale di ECI, necessario per taluni software di firma grafometrica.

La firma digitale del file di chiusura lotto, invece, viene apposta mediante un sistema di firma automatica, erogato da una Certification Authority, che si avvale di un dispositivo crittografico per la firma digitale massiva (HSM). Questa tipologia di dispositivi, le cui caratteristiche sono conformi ai requisiti di sicurezza richiesti dalla normativa europea, permette di firmare remotamente e automaticamente più documenti contemporaneamente, garantendo non solo migliori prestazioni rispetto a una semplice smart card (o a un token USB), ma anche un utilizzo sicuro di chiavi crittografiche applicando elevatissimi standard di sicurezza informatica tanto da permettere di digitare il PIN una sola volta a fronte della sottoscrizione di più documenti.

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 ivi contenuti. L'apposizione della firma digitale del Responsabile della Conservazione e della marca temporale sul file di chiusura lotto attesta la conservazione del lotto stesso.

I lotti prodotti vengono archiviati mediante procedure e sistemi che consentono la memorizzazione permanente in più copie e la non-modificabilità di quanto memorizzato.

Inoltre, possono essere prodotte ulteriori copie di back-up su supporti ottici rimovibili, stoccati dal Data Center o inviati allo Studio Dentistico su espressa richiesta (come da contratto di servizi di cui il presente Manuale è parte integrante).

Controlli e gestione delle anomalie

Le procedure del servizio di conservazione sostitutiva previste da Oris Paperless sono fortemente automatizzate e, proprio per questa ragione, l'intero sistema di erogazione è dotato 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 preventivi;
- controlli di processo;
- controlli periodici.

Controlli preventivi

I controlli preventivi sono quelli che intervengono sui documenti prima del loro invio in conservazione e sono di due tipi: quelli che ne verificano la dimensione al fine di renderli accettabili dal Data Center e quelli che ne garantiscono le corrette tempistiche di conservazione.

I primi controlli verificano che la dimensione dei documenti da inviare non superi i 20 Mbyte, in quanto il sistema installato presso il Data Center è configurato in tal senso e, al venir meno di questa condizione, rifiuta il documento inviato.

Al fine invece di garantire le corrette tempistiche di conservazione, sono stati introdotti dei blocchi temporali in modo da impedire o quantomeno limitare fortemente eventuali errori in tal senso. In particolare:

- allo scopo di chiudere ogni lotto semestralmente, indipendentemente dalla quantità di dati contenuti, nelle direttive di conservazione la data di chiusura del lotto sarà impostata al 30/6 o al 31/12 di ogni anno;

- allo scopo di evitare la scadenza del certificato di firma, Oris Paperless non permette di firmare il documento entro sei mesi dalla scadenza di detto certificato, obbligando così l'utente a usare un nuovo certificato.

Controlli di processo

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

Oris Paperless è un sistema 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.

Controlli periodici

Presso il Data Center 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 (in termini di competenze) che utilizza strumentazioni di varia natura per la raccolta di dati relativi al funzionamento dei servizi e che si riunisce periodicamente per discutere dei malfunzionamenti registrati nel periodo e delle soluzioni adottate o potenziali per evitare il ripresentarsi dell'inconveniente.

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 del Data Center e di ECI 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.

Incident management

ECI, col supporto del Data Center di cui si avvale, è impegnata nel continuo affinamento e aggiornamento del sistema di conservazione documentale, al fine di individuare preventivamente ogni potenziale causa di incidente e provvedere alla sua rimozione, evitando il blocco del sistema o il danneggiamento dei file in esso contenuti.

I fornitori dei sistemi tecnologici utilizzati forniscono a ECI 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 (a cura della struttura di Service Desk) seguono le procedure definite e documentate secondo le raccomandazioni delle best practice ITIL; 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.

Il processo di conservazione attuato da ECI 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 eseguiti localmente presso lo Studio Dentistico (di front-end);
- processi eseguiti remotamente presso il Data Center (di back-end).

I processi di front-end sono finalizzati a mettere in comunicazione il software Orisdent installato e disponibile presso lo Studio Dentistico, con i servizi di Oris Paperless accessibili remotamente e richiamati attraverso una connessione Internet. 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;
- ottenimento per via telematica delle informazioni sullo stato di un documento o di un lotto;
- elaborazione e invio della richiesta di chiusura forzata del lotto;
- esibizione di un documento direttamente dal sistema Oris Paperless (vedi capitolo relativo alle procedure di ricerca ed esibizione);
- rettifica o cancellazione per via telematica di un documento già conservato in modalità sostitutiva (vedi capitolo relativo alle procedure di modifica dei documenti posti in conservazione).

I processi di back-end sono eseguiti dal sistema Oris Paperless in modalità differita e sono i processi che implementano la conservazione sostitutiva in conformità alle regole tecniche contenute nella deliberazione CNIPA 11/04.

Rinviando ai capitoli successivi le procedure di ricerca, esibizione e modifica o cancellazione dei documenti posti in conservazione, nei paragrafi successivi vengono dettagliate le due fasi principali del processo di conservazione:

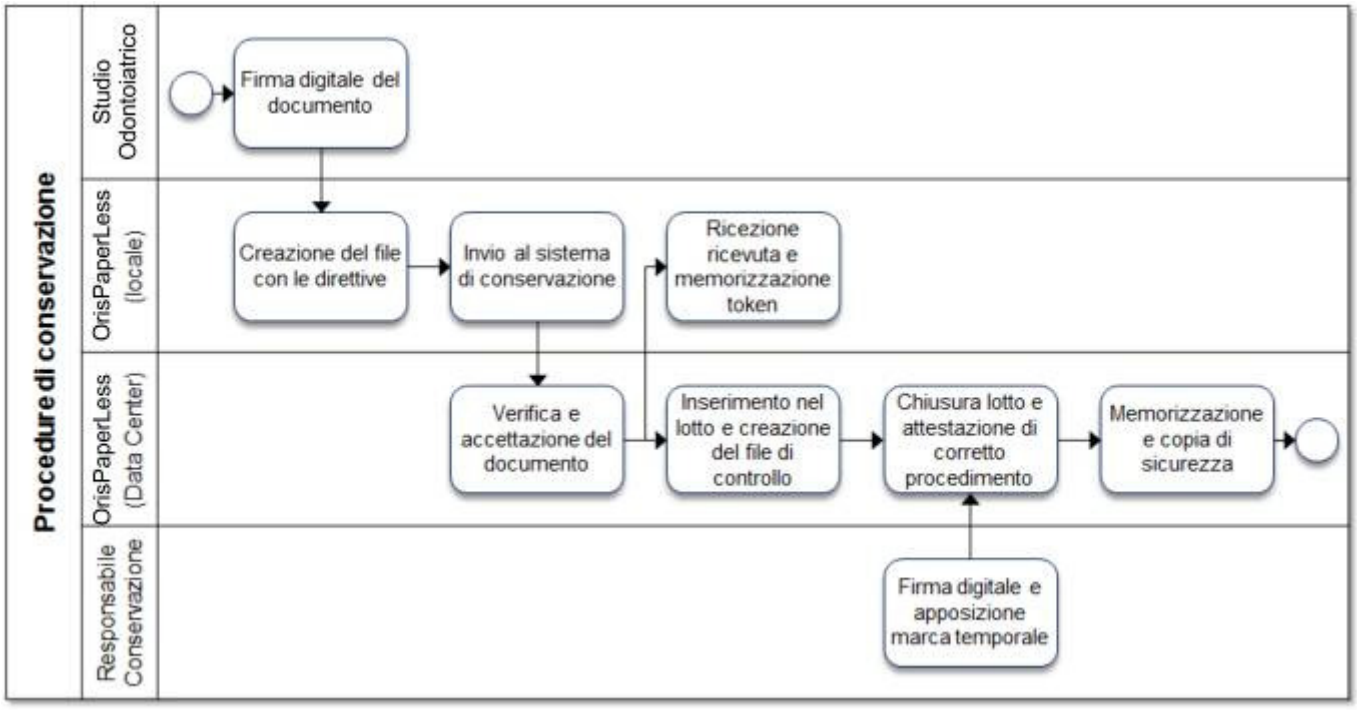
- elaborazione del singolo documento: in questa fase viene analizzato il singolo documento, che viene assegnato a un lotto di documenti. Il documento viene corredato da un file di controllo, firmato

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 – tokenLotto –, 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.

Fasi del processo di conservazione: schema generale e responsabilità

Segue una schematizzazione del processo di conservazione sostitutiva, opportunamente dettagliato nei paragrafi successivi.



La tabella seguente mostra invece le diverse responsabilità dei soggetti che intervengono nel processo di conservazione sostitutiva.

Responsabilità Attività	***Paziente***	***Studio Dentistico***	***Oris Paperless (locale)***	***Oris Paperless (Data Center)***	***Responsabile Conservazio-ne***
1. Firma elettronica avanzata del documento	**E - R**	**A**	**V**		
2. Firma digitale del documento		**E – R**	**V**		
3. Creazione del file con le direttive di conservazione			**R - E**		
4. Invio al sistema di conservazione		**R – E**	**V**		
5. Verifica e accettazione del documento e invio della ricevuta di accettazione dei documenti			**V**	**E**	**R**
6. Inserimento nel lotto e creazione del file di controllo				**E**	**R – V**
7. Chiusura e firma digitale del lotto e attestazione di corretto procedimento				**E**	**A – R – V**
8. Memorizzazione, creazione “copia di sicurezza” e chiusura del processo				**E**	**R – V**
	[**R**-responsabile; **E**-esegue; **V**-verifica; **A**-approva]				

Fasi del processo di conservazione: dettaglio

Viene di seguito dettagliata ogni singola fase del processo di conservazione evidenziandone i documenti in input e quelli in output così come ogni singola attività svolta con l’indicazione del relativo responsabile.

Firme digitali del documento

INPUT	*Categorie documentali di cui all'Allegato 1, sotto forma di documento informatico*	
Studio Dentistico	1.1	Accesso al sistema attraverso l'Id e la Password; è necessaria la chiave USB di protezione del software Orisdent.
	1.2	Apposizione firma grafometrica del paziente
	1.3	Eventuale apposizione di certificato di firma digitale aziendale di ECI, embedded in Oris Paperless.
	1.4	Apposizione firma digitale dello Studio (operatore amministrativo e/o sanitario) utilizzando un proprio certificato di firma digitale e il relativo pin (le condizioni del punto 1.1 persistono).
	1.5	Una volta firmato, il documento diventa un P7M e/o un PDF/A (a seconda del fornitore di software di firma grafometrica), e permane localmente sul disco in una cartella apposita fino al suo invio in conservazione al Data Center. Gli step 1.2, 1.3, 1.4, 1.5 sono atomizzati dal sistema e costituiscono un unico e indivisibile processo; il sistema non passa allo step successivo finchè non si è concluso con successo lo step precedente.
OUTPUT	*Fascicolo tecnico firmato digitalmente (in formato P7M o PDF/A)*	

Creazione del file delle direttive

INPUT	*Documenti di cui all'Allegato 1, firmati elettronicamente.*	
Oris Paperless (locale)	2.1	Predisposizione del file con le direttive di conservazione
	2.2	Calcolo delle impronte dei file costituenti il documento (hash)
	2.3	Inserimento delle impronte nel file delle direttive
	2.4	Apposizione della firma elettronica sul file delle direttive (p12 intestato al fornitore del service di conservazione sostitutiva)
	2.5	Costruzione del messaggio contenente i file che costituiscono il documento da inviare in conservazione
OUTPUT	*File delle direttive di conservazione predisposto e firmato elettronicamente*	

Elite Computer Italia S.r.l.
Sede legale: Via Padova 209 - 20127 - Milano
Sede operativa: Via Achille Grandi 19-21-23, 20090 Vimodrone (MI)
Tel. +39 02/27.40.95.21 – Fax +39 02/27.40.91.50
P.Iva/C.F 11654690152 - Cap. sociale Euro 100.000,00 i.v.
REA MI-1485870 www.orisline.com - info@orisline.com

Invio al sistema di conservazione

INPUT	*Documenti firmati elettronicamente, file delle direttive firmato elettronicamente e file degli indici di ricerca*	
Oris Paperless (locale)	3.1	Invio del documento, del file degli indici di ricerca e della relativa richiesta di conservazione tramite web, con protocollo “SOAP”, dal client locale di Orisdent allo spazio di conservazione online del Data Center.
	3.2	Il documento firmato elettronicamente (cioè il file p7m e/o il PDF/A) viene marchiato come “firmato e spedito” e quindi cancellato localmente. Alcuni documenti creati ma privi di firme (esempio: anamnesi) sono sempre visualizzabili in Orisdent, in locale.
OUTPUT	*Documento inviato al Data Center*	

Verifica, accettazione e invio della ricevuta di accettazione del documento

INPUT	*Documento da verificare*	
Oris Paperless (Data Center)	4.1	Acquisizione del documento.
	4.2	Sbustamento del messaggio e verifica della firma elettronica (p12) apposta sul file delle direttive di conservazione.
	4.3	Presa in carico dei file costituenti il documento da conservare.
	4.4	Esecuzione di una serie di verifiche sulla completezza e sulla correttezza delle informazioni contenute nel file delle direttive di conservazione.
	4.5	Generazione dell'impronta di ogni file del documento.
	4.6	Confronto dell'impronta generata con la corrispondente inviata dal Cliente per garantire l'integrità del documento ricevuto.
	4.7	Nel caso di esito negativo delle verifiche, il documento viene respinto con l'indicazione che descrive l'errore intercorso e il flusso termina.
	4.8	Generazione del file di ricevuta a partire dal file delle direttive.
	4.9	Generazione di un identificativo univoco per il documento (token Oris Paperless) e firma elettronica sul file di ricevuta.
	4.10	Invio al client locale di Oris Paperless del file di ricevuta di presa in carico della richiesta di conservazione.
Oris Paperless (locale)	4.11	Riceve il file di ricevuta di presa in carico della richiesta di conservazione, ne estrae il token e lo memorizza presso il proprio database, in associazione con gli indici di ricerca.
OUTPUT	*Documento verificato e ricevuta restituita al client locale*	

Elite Computer Italia S.r.l.
Sede legale: Via Padova 209 - 20127 - Milano
Sede operativa: Via Achille Grandi 19-21-23, 20090 Vimodrone (MI)
Tel. +39 02/27.40.95.21 – Fax +39 02/27.40.91.50
P.Iva/C.F 11654690152 - Cap. sociale Euro 100.000,00 i.v.
REA MI-1485870 www.orisline.com - info@orisline.com

Inserimento nel lotto e creazione del file di controllo

INPUT	*Documento da conservare*	
Oris Paperless (Data Center)	5.1	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.
	5.2	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 e gli estremi di identificazione del Responsabile della Conservazione.
	5.3	Apposizione della firma elettronica del Responsabile della Conservazione sul file di controllo.
	5.4	Inserimento del file di controllo e del relativo documento nel lotto di conservazione.
OUTPUT	*Documento inserito in un lotto di conservazione*	

Chiusura e firma digitale del lotto e attestazione di corretto procedimento

INPUT	*Lotto da chiudere*	
Oris Paperless (Data Center)	6.1	Chiusura del lotto al raggiungimento delle condizioni di chiusura lotto: • raggiungimento di 500 Mbyte; • raggiungimento del numero massimo di documenti per lotto gestibile dal sistema, fissato in 20.000 documenti; • raggiungimento della data massima di chiusura del lotto, impostata sulle due date 30/6 e 31/12 • raggiungimento di un anno solare dalla data di apertura del lotto Il lotto viene chiuso al verificarsi di uno o più dei precedenti eventi o in seguito alla ricezione della richiesta di chiusura forzata del lotto inviata dallo Studio Dentistico.
	6.2	Generazione del file di chiusura lotto e inserimento degli hash dei file di controllo del documento.
Responsabile Conservazione	6.3	Apposizione della firma digitale, necessaria ad attestare il corretto svolgimento del procedimento sul file di chiusura lotto.
	6.4	Apposizione della marca temporale sul file di chiusura lotto.
OUTPUT	*Lotto chiuso*	

Memorizzazione, creazione copia di sicurezza e chiusura della conservazione

INPUT	*Documenti da memorizzare*	
Oris Paperless (Data Center)	7.1	Memorizzazione del lotto su supporto magnetico per almeno quindici anni.
	7.2	Creazione della copia di sicurezza.
	7.3	Termine della procedura di conservazione.
OUTPUT	*Documenti conservati*	

Il processo di ricerca, esibizione ed erogazione

Ogni utente autorizzato può, in qualsiasi momento e tramite le funzioni di Orisdent e/o di Oris Paperless e/o di software terzi di visualizzazione, ricercare e accedere a tutti i documenti di cui al presente processo di conservazione, ancora presenti localmente e/o inviati in conservazione.

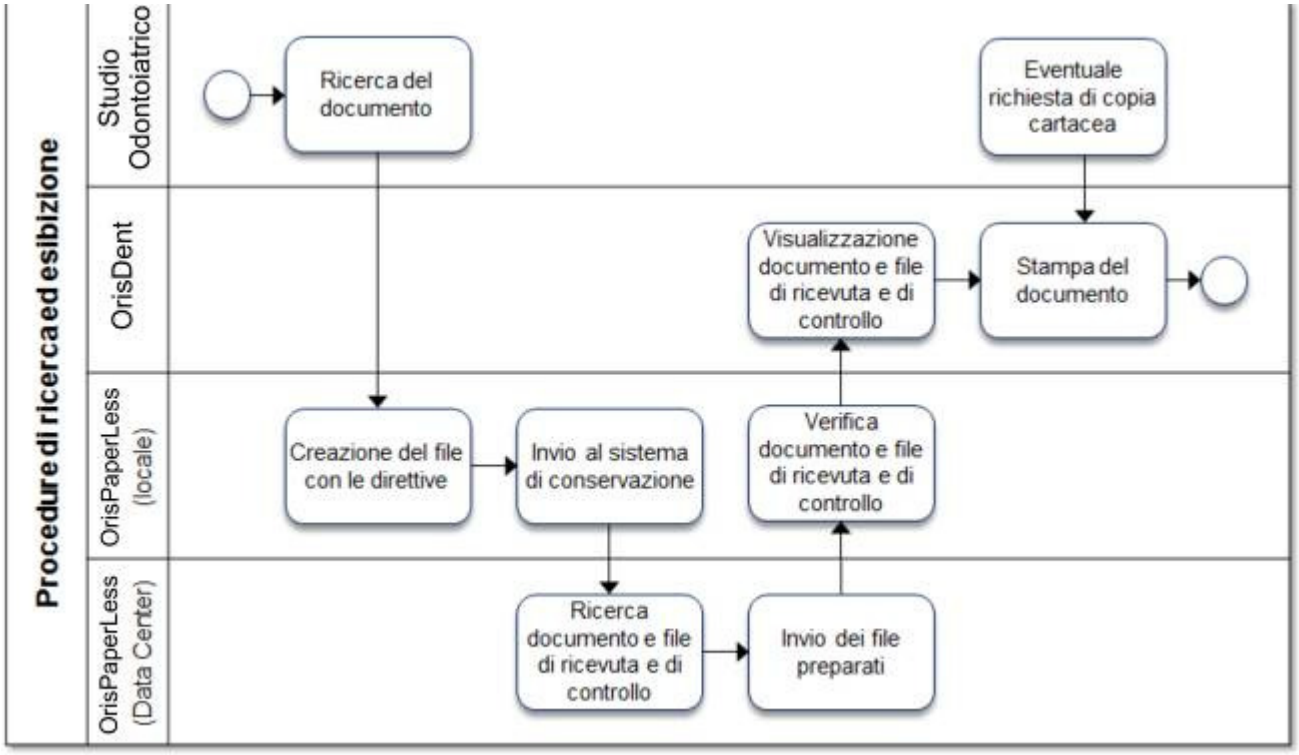
In particolare, le procedure di esibizione del documento integrate in Oris Paperless permettono di:

- estrarre dal Data Center ogni documento inviato in conservazione, sia in modalità erogazione (lotto aperto) sia in modalità esibizione (lotto chiuso, quindi con completamento della procedura di conservazione);
- 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;
- visualizzare il contenuto del documento;
- effettuare una copia cartacea del documento con o senza dicitura "la stampa su carta del presente documento costituisce copia analogica di documento informatico ai sensi dell'art. 23 comma 2 del D.Lgs. 82/2005", secondo la casistica.

In tal senso, l'esibizione del documento ottenuto tramite interrogazione al sistema Oris Paperless rappresenta un'esibizione completa, legalmente valida ai sensi del secondo comma dell'articolo 6 della deliberazione CNIPA 11/04.

Fasi del processo di ricerca ed esibizione: schema generale e responsabilità

Segue una schematizzazione del processo di ricerca e di esibizione, opportunamente dettagliato nei paragrafi successivi.



La tabella seguente mostra invece le diverse responsabilità dei soggetti che intervengono nelle procedure di ricerca ed esibizione.

Responsabilità ***Attività***	***Studio Dentistico***	***Orisdent***	***Oris Paperless (locale)***	***Oris Paperless (Data Center)***	***Responsabile Conservazione***
1. Ricerca del documento da esibire	**R**	**E**			
2. Invio della richiesta di esibizione	**V**		**R – E**		
3. Ricerca del documento nel sistema di conservazione ed esibizione				**E – V**	**R**
4. Verifica del documento			**R – E – V**		
5. Visualizzazione del documento	**R**	**E**			
[**R**-responsabile; **E**-esegue; **V**-verifica; **A**-approva; ***-se necessario]					

Fasi del processo di ricerca ed esibizione: dettaglio

Viene di seguito dettagliata ogni singola fase delle procedure di ricerca ed esibizione evidenziandone i documenti in input e quelli in output così come ogni singola attività svolta con l'indicazione del relativo responsabile.

Ricerca del documento da esibire

INPUT	*Lista di documenti*	
Studio Dentistico	1.1	Ricerca il documento da esibire utilizzando gli indici archiviati su Orisdent e recupero dei relativi indici.
OUTPUT	*Indici relativi al documento da esibire*	

Invio della richiesta di esibizione

INPUT	*Indici relativi al documento da esibire*	
Oris Paperless (locale)	2.1	Creazione del file delle direttive di esibizione, contenente gli indici relativi al documento da esibire, e sua sottoscrizione elettronica.
	2.2	Invio del file delle direttive di esibizione tramite web, con protocollo "SOAP", al sistema Oris Paperless del Data Center.
OUTPUT	*Richiesta di esibizione inviata al Data Center*	

Ricerca del documento nel sistema di conservazione ed esibizione

INPUT	*Richiesta di esibizione*	
Oris Paperless (Data Center)	3.1	Ricezione della richiesta di esibizione del documento.
	3.2	Controllo di corrispondenza tra gli indici di Oris Paperless ricevuti 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 dei file costituenti il documento e dei file attestanti il processo di conservazione, cioè di: • il file di controllo del documento firmato digitalmente che deve essere fornito in esibizione per poter, in combinazione con il file di chiusura del lotto, qualificare il processo stesso; • il file delle direttive di conservazione inviato con la richiesta di conservazione del documento, per poter verificarne la coerenza con quanto inviato dallo Studio Dentistico; • il file di ricevuta di presa in carico della conservazione fornito in risposta alla richiesta di conservazione; • il file di chiusura del lotto.
	3.4	Visualizzazione sul client locale di una lista di documenti disponibili sia in visualizzazione che in restituzione, sia singolarmente che globalmente.
OUTPUT	*Documento visualizzato e/o restituito al client locale insieme ai file che qualificano il processo di conservazione*	

Verifica del documento

INPUT	*Documento firmato digitalmente insieme ai file che qualificano il processo di conservazione*	
Oris Paperless (locale) tramite software terzi di visualizzazione e verifica certificati	4.1	Verifica la validità delle firme digitali e delle marche temporali apposte sul documento.
	4.2	Apertura del documento firmato digitalmente per renderlo leggibile e verifica della sua integrità.
	4.3	Verifica dei file che qualificano il processo di conservazione.
OUTPUT	*Documento e file che qualificano il processo di conservazione leggibili*	

Visualizzazione del documento

INPUT	*Documento e file che qualificano il processo di conservazione leggibili*	
Orisdent	5.1	Visualizzazione attraverso viewer terzi del documento e dei file che qualificano il processo di conservazione.
Studio Dentistico	5.2	Stampa su carta del documento con o senza dicitura "la stampa su carta del presente documento costituisce copia analogica di documento informatico ai sensi dell'art. 23 comma 2 del D.Lgs. 82/2005", a seconda della casistica.
OUTPUT	*Documento visualizzato ed eventualmente stampato*	

In caso di modifica dei documenti già posti in conservazione, lo Studio Dentistico provvede ad emanare ex novo un documento di rettifica e ad inviarlo al sistema di conservazione specificando quale tra i documenti conservati a norma viene rettificato (fornendo il suo token Oris Paperless).

La riconducibilità del documento modificante a quello modificato è resa possibile grazie agli indici predisposti nel sistema e all'univocità dei token Oris Paperless loro associati, che ne assicurano la sistematicità e la coerenza.

Essendo la procedura di modifica identica a quella di conservazione, a meno del recupero del token Oris Paperless relativo al documento da modificare che viene inserito nel file delle direttive e inviato al Data Center insieme al documento stesso appositamente firmato, si rimanda ogni ulteriore dettaglio a quanto descritto precedentemente nel capitolo relativo al processo di conservazione.

La cancellazione di un documento

Oris Paperless è configurato in modo da non consentire la cancellazione fisica di quanto conservato, nel rispetto dei principi normativi vigenti.

Misure di Sicurezza

Il sistema Oris Paperless è pienamente conforme ai requisiti di sicurezza prescritti dalla normativa. Nel seguito sono descritti i protocolli di sicurezza adottati da ECI in caso di crash del sistema locale dello Studio Dentistico e le modalità generali tecniche e il sistema di gestione della sicurezza informatica, certificato ISO 27001, adottato dal Data Center.

Per le misure relative al trattamento dei dati sensibili, si rimanda a quanto sopra descritto relativamente al modulo Oris Paperless.

Politiche d'accesso e gestione dei dati sensibili

Con Orisdent è possibile adempiere tutti gli obblighi richiesti dal nuovo Decreto in materia di tutela dei dati sensibili come descritto nel Documento Programmatico sulla Sicurezza stampabile attraverso Orisdent stesso. In particolare:

- in merito alle politiche d'accesso, viene inserita l'anagrafica di tutti gli operatori che lavorano in Studio definendo le loro "credenziali di autenticazione" (associando cioè a ognuno di loro un ID e una password), e viene scelto un supervisore che possa accedere a tutte le parti del programma e stabilire i permessi e i diversi livelli di accesso (visualizzazione, modifica o eliminazione dei dati) di tutti gli utenti;
- l'accesso al sistema Orisdent è pertanto possibile utilizzando le proprie credenziali d'accesso (ID e password) e inserendo la chiave hardware di protezione nella porta USB del pc (una chiave per ogni macchina);
- il database di Orisdent è criptato (con criptazione protetta da password), in modo da risultare inaccessibile dall'esterno del programma.

Con l'introduzione di Oris Paperless quale modulo integrato del software Orisdent, e atto a gestire la dematerializzazione e la conservazione a norma dei documenti di cui all'Allegato 1 del presente Manuale, sono state rafforzate le misure di sicurezza e sono state definite le seguenti ulteriori politiche d'accesso:

- per attivare il servizio Oris Paperless, è necessario che un utente autorizzato esegua la seguente procedura una tantum: accedere a Orisdent tramite ID e password, mantenendo sempre inserita la chiave USB di protezione; attivare il servizio Oris Paperless tramite il Codice Ente e la password ricevuti separatamente via mail (da Elite).
- Una volta attivato il servizio con procedura una tantum, l'accesso può essere effettuato dagli utenti autorizzati utilizzando le proprie credenziali d'accesso (ID e password), inserendo la chiave di protezione hardware nella porta USB, e, nel caso di firma digitale di un documento, inserendo la propria chiave di firma nella porta USB (in aggiunta alla chiave di protezione già inserita), e digitando il relativo pin di firma.
- il Responsabile della Conservazione viene identificato nel sistema grazie alla definizione di un particolare utente con il ruolo di "responsabile del procedimento di conservazione" i cui estremi identificativi (organizzazione di appartenenza, cognome, nome, codice fiscale) sono riportati anche nelle informazioni associate ai documenti conservati e nei file di chiusura dei lotti.

Protocolli di sicurezza in caso di crash del sistema locale

Nel caso in cui lo Studio Dentistico subisca un crash del sistema locale, sono stati predisposti tre livelli di sicurezza per garantire l'accesso ai documenti conservati a norma:

1. qualora sia disponibile l'accesso ad Internet, gli utenti autorizzati dello Studio Dentistico possono utilizzare l'applicativo java OrisDoc, disponibile nel setup di Oris Paperless, e fornendo ID, password, codice di controllo, ed eseguendo un'ulteriore autenticazione online. OrisDoc è in grado di interrogare direttamente l'area di conservazione remota di Oris Paperless;
2. In assenza di collegamento internet, lo Studio Dentistico può richiedere i documenti da esibire direttamente a ECI, la quale si collega al Data Center, estrae i documenti richiesti e li consegna allo Studio;
3. qualora le richieste di documenti siano molteplici e/o i livelli 1 e 2 non fossero sufficienti, ECI può richiedere al Data Center un ID e una password temporanei che fornisce a sua volta allo Studio Dentistico per permettere l'accesso diretto ai propri documenti utilizzando le funzionalità di esibizione a norma offerte dal modulo Oris Paperless.

I tre livelli di sicurezza sono sequenziali, quindi in caso di crash si inizia col protocollo (1) per poi passare al livello successivo solo se quello precedente non fosse applicabile e/o si dovesse rivelare manifestamente insufficiente a risolvere il problema contingente.

Sicurezza fisica del Data Center

I locali che ospitano il sistema remoto Oris Paperless sono siti in un immobile la cui zona d'ubicazione non presenta rischi ambientali dovuti alla vicinanza a installazioni pericolose. Inoltre, 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.

In particolare, l'accesso alla sala CED, cioè all'area all'interno dello stabile dove si trovano i dispositivi hardware e software dei diversi sistemi utilizzati, è accessibile solo alle persone autorizzate, ossia quelle con un ruolo operativo nell'erogazione del servizio e nella gestione dell'infrastruttura, mediante utilizzo di apposito badge.

All'interno della sala CED sono collocate le sale del locale CA, accessibili mediante badge autorizzato e PIN (Personal Identification Number) di accesso. Inoltre, per l'accesso alle singole sale del locale CA è necessario un ulteriore badge autorizzato.

Lo stabile è inoltre sorvegliato da personale specializzato 24 ore al giorno e tutte le porte sono dotate di allarme. In particolare 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.

Gruppi di continuità nel Data Center

Tutte le apparecchiature del Data Center 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.

Connessione a Internet e sicurezza delle reti del Data Center

Il Data Center è connesso alla rete Internet con due collegamenti Gigabit Ethernet in fibra ottica separati (gestiti da due diversi Provider), entrambi con velocità massima di 200 Mbit/sec. Tali collegamenti sono attestati su POP distinti, con percorsi fisici e apparati di interfaccia separati e completamente ridondati, garantendo così la continuità dei servizi nel caso di failure di uno dei due link (o di un failure all'interno della rete di uno dei due Provider).

In particolare, tra gli SLA del Data Center, vi è l'impegno di mantenere i tempi di attraversamento della rete inferiori a 20 ms tra il proprio centro servizi e i nodi d'interconnessione con i principali provider italiani e internazionali.

La connessione a Internet è controllata da sistemi firewall che ne consentono la suddivisione 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 prestabilite.

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 del sistema. 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).

Il Data Center provvede alla gestione e all'implementazione delle regole di sicurezza dei firewall i quali 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.

Sicurezza logica del Data Center

Il controllo dell'accesso alle informazioni avviene tramite credenziali di autenticazione rilasciate individualmente. Tali credenziali, personali e non cedibili, sono assegnate in base alla necessità di accedere ai dati o ai sistemi aziendali e sono gestite contemporaneamente alle abilitazioni, sulla base del principio del "minimo privilegio". In particolare, l'accesso da parte degli Amministratori di sistema, all'uopo nominati in conformità con quanto prescritto dalla normativa vigente, avviene tramite un'applicazione che permette l'utilizzo dei privilegi dell'utenza root solo previa autenticazione individuale (root on demand).

Alle password, con durata massima di sei mesi a meno di quelle degli Amministratori che hanno durata massima di tre mesi, sono imposte specifiche regole di robustezza (password guessing). Per i sistemi più critici è prevista l'autenticazione forte tramite token e certificati di autenticazione.

Tutti gli accessi sono tracciati, loggati e conservati per sei mesi.

Gestione dei backup e delle copie di sicurezza

L'architettura tecnologica a servizio del processo di Backup Management è costituita da prodotti all'avanguardia che controllano e gestiscono l'esecuzione dei salvataggi e la loro archiviazione su sottosistemi storage dedicati di tipo Disk Library (con Data Deduplication) e Tape Library. Il backup dei dati viene eseguito con modalità e pianificazione differenti secondo la tipologia e della criticità del servizio e del dato secondo le seguenti due macro tipologie:

- Backup Database Oracle: backup a caldo della base dati tramite le integrazioni messe a disposizione da Oracle e il prodotto di backup. In particolare sono state definite per il database differenti politiche di backup: il salvataggio dell'intera istanza database senza la necessità di porla offline (modalità full hot) avviene con cadenza settimanale nelle ore in cui il carico di query è statisticamente più basso e in modalità cumulative incremental negli altri giorni della settimana (con una retention di quattro settimane); il salvataggio degli archive log avviene invece più volte durante la giornata (tipicamente con cadenza oraria).
- Backup File System: il backup dei file system riservati ai server avviene in modalità full settimanalmente e in maniera incrementale giornalmente, con una retention di quattro settimane.

I media contenenti i backup sono conservati in una sala adibita a tale compito e ricavata in spazi attigui alla sala macchine, con condizioni di temperatura, umidità e sicurezza costantemente monitorate.

Il sito di Disaster Recovery è invece ubicato a Milano ed è connesso alla sede operativa di Padova tramite un doppio collegamento dedicato Gigabit Ethernet in fibra ottica, come indicato in precedenza.

Elite Computer Italia S.r.l.
Sede legale: Via Padova 209 - 20127 - Milano
Sede operativa: Via Achille Grandi 19-21-23, 20090 Vimodrone (MI)
Tel. +39 02/27.40.95.21 – Fax +39 02/27.40.91.50
P.Iva/C.F 11654690152 - Cap. sociale Euro 100.000,00 i.v.
REA MI-1485870 www.orisline.com - info@orisline.com

ALLEGATO 1

ELENCO DELLE TIPOLOGIE DOCUMENTALI

PER LE QUALI ORIS PAPERLESS CONSENTE LA DEMATERIALIZZAZIONE E LA CONSERVAZIONE SOSTITUTIVA

(aggiornamento del 28/10/13)

- Consenso informato generico;
- Dichiarazione di ricevuta informazione e consenso ad anestesia;
- Dichiarazione di ricevuta informazione e consenso ad interventi di chirurgia implantare osteointegrata;
- Dichiarazione di ricevuta informazione e consenso ad interventi di chirurgia orale;
- Dichiarazione di ricevuta informazione e consenso ad interventi di protesi mobile;
- Dichiarazione di ricevuta informazione e consenso ad interventi di terapia conservativa ed endodontica;
- Dichiarazione di ricevuta informazione e consenso ad interventi di terapia protesica complessa;
- Dichiarazione di ricevuta informazione e consenso ad interventi di trattamento ortodontico;
- Dichiarazione di ricevuta informazione e consenso ad interventi di chirurgia orale;
- Dichiarazione di ricevuta informazione e consenso ad interventi di chirurgia orale;
- Scheda Anamnesi;
- Consenso al trattamento dei dati ed informative ai sensi del codice sulla privacy (D. Leg.vo 196/03).